Avaya Aura™ Communication Manager Feature Description and Implementation

555-245-205
Issue 7
Release 5.2
May 2009

© 2009 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the website, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Contents

About this document 61
Overview 61
Intended audience 61
How to use this book 61
Organization 61
Summary 62
Detailed description 62
Administering 62
End-user procedures 62
Reports 63
Considerations 63
Interactions 63
Troubleshooting 63
Related resources 63
Conventions 65
Admonishments 66
Trademarks 67
How to obtain Avaya books on the Web 67
How to comment on this book 68
How to get help 68

AAA Services 71
Detailed description of AAA Services 71
Supported security configurations 72
Configuring external AAA servers 73
User authentication 73
User profiles 74
User profiles for SAT form access 75
SAT profiles 75
Extended profiles 77
User profiles for Communication Manager server Web page access 77
Profile access to restricted objects 80
User accounts 81
External accounts 81
Local host accounts 81
Administrative logins 82
Avaya services logins 82
CDR logins 82
BusinessPartner login: dadmin 83

Remote logins: remote 83
Linux groups 83
Upgrades from a release that does not support profiles 85
Upgrades from a release that supports profiles 86
Backup and restore 86
Backup and file sync for web access profiles 87
Administering AAA Services 87
Screens for administering AAA Services 88
Managing accounts using Communication Manager Web pages 88
Adding an administrator account (login) 89
Changing a login 90
Removing a login 90
Locking a login 91
Adding a login group 91
Removing a login group 91
Managing profiles using the Communication Manager SAT 92
Adding a user profile for using the SAT 92
Enabling a second craft login at the SAT 92
Managing passwords and Access Security Gateway 93
Administering Communication Manager web access profiles 93
Adding web access profiles 93
Recommended procedure for adding web profiles 93
Changing web profiles 94
Duplicating web profiles 94
Deleting web profiles 94
Changing the profile base 95
Displaying the profile base 96
Administering user profiles for Communication Manager SAT access 96
Adding SAT profiles 96
Adding extended profiles 97
Duplicating SAT profiles 97
Deleting user profiles 97
Exporting and importing SAT profiles 98
Displaying the profile base 98

Abbreviated Dialing 99
Abbreviated Dialing labeling 99
Abbreviated Dialing on-hook programming 100
Detailed description of Abbreviated Dialing 100
Administering Abbreviated Dialing 101

Prerequisites for Abbreviated Dialing . . . 101
Screens for administering Abbreviated Dialing . . . 102
Adding Abbreviated Dialing lists . . . 102
Assigning telephones for group lists . . . 103
End-user procedures for Abbreviated Dialing . . . 104
Programming the Abbreviated Dialing feature . . . 105
Considerations for Abbreviated Dialing . . . 105
Interactions for Abbreviated Dialing . . . 106
Troubleshooting Abbreviated Dialing . . . 107
Edit Dialing . . . 108
Feature interactions . . . 108
Edit Dialing System Parameters screen . . . 109
Edit Dialing on 96xx H.323 Terminals? . . . 109
Field description . . . 109

Access Security Gateway . . . 111
Detailed description of Access Security Gateway . . . 111
Administering Access Security Gateway . . . 111
Prerequisites for administering Access Security Gateway . . . 112
Screens for administering Access Security Gateway . . . 112
Setting up Access Security Gateway . . . 113
Disabling Access Security Gateway . . . 114
Restarting Access Security Gateway . . . 115
Modifying Access Security Gateway for a lost key . . . 115
Monitoring the Access Security Gateway history log . . . 116
Interactions for Access Security Gateway . . . 117

Administered Connections . . . 119
Detailed description of Administered Connections . . . 119
Access endpoints . . . 120
Typical applications . . . 120
Establishing Administered Connections . . . 120
Dropping Administered Connections . . . 121
Autorestoration and fast retry . . . 122
Administering Administered Connections . . . 122
Prerequisites for administering Administered Connections . . . 123
Screens for administering Administered Connections . . . 123
Setting up Administered Connections . . . 123
Interactions for Administered Connections . . . 125

Administrable Alternate Gatekeeper List for IP Phones 127
Load balancing of IP telephones during registration 128
Building the Alternate Gatekeeper Lists 129
Application scenarios 129
Example 1: Unwanted C-LANs in the AGL 130
Example 2: Unable to pool C-LANS because of Network Region Connectivity . 133
High-level capacities 136
Considerations 137
Interactions 137

Administrable Language Displays 139
Detailed description of Administrable Language Displays 139
Administering Unicode display 140
Obtaining and installing Phone Message files 141
Checking the status of Phone Message file loads 142
Unicode "Native Name" support 143
Administering Administrable Language Displays 143
Prerequisites for administering Administrable Language Displays 144
Screens for administering Administrable Language Displays 144
Setting the display language 145
Entering translations for a user-defined language 146
Considerations for Administrable Language Displays 146
Troubleshooting Administrable Language Displays 147
Making Standard Telephone Features easier to use 148

Administration Change Notification 151
Detailed description of Administration Change Notification 151
Administering Administration Change Notification 151
Prerequisites for administering Administration Change Notification 152
Screens for administering Administration Change Notification 152
Initiating Administration Change Notification 152

Administration Without Hardware 153
Detailed description of Administration Without Hardware 153
Physical characteristics of an AWOH telephone 153
User-activated features 154
Association and disassociation 154
Phantom extensions 154
Administering Administration Without Hardware 154
Screens for administering Administration Without Hardware 155

Assigning AWOH for a hunt group queue . . . 155
Assigning AWOH to a telephone . . . 157
Assigning AWOH to an attendant console . . . 157
Assigning AWOH to a data module . . . 158
Reports for Administration Without Hardware . . . 159
Considerations for Administration Without Hardware . . . 159
Interactions for Administration Without Hardware . . . 160

Alphanumeric Dialing . . . 169
Detailed description of Alphanumeric Dialing . . . 169
Administering Alphanumeric Dialing . . . 169
Screens for administering Alphanumeric Dialing . . . 170
Considerations for Alphanumeric Dialing . . . 170

Announcements . . . 171
Announcements enhancements in Communication Manager 4.0 . . . 171
Detailed description of Announcements . . . 172
Voice Announcements over LAN . . . 173
VAL Manager . . . 173
Local announcements on media gateways . . . 174
Announcement devices and types . . . 174
Analog line types . . . 175
DS1 types . . . 175
Auxiliary trunk types . . . 176
Integrated types . . . 176
Barge-in announcements . . . 177
Barge-in operation . . . 177
Non-barge-in operation . . . 177
Announcement sources in the G700, G350, and G250 Media Gateway . . . 178
Compression rates . . . 178
Announcement sessions . . . 178
Announcement recordings . . . 179
Announcement session process . . . 179
Locally Sourced Announcements and Music . . . 180
Administering Announcements . . . 180
Prerequisites for administering Announcements . . . 181
Screens for administering Announcements . . . 181
Adding/changing/displaying or removing announcement extensions . . . 183
Adding a TN2501AP VAL circuit pack . . . 186
Listing all administered circuit packs . . . 188

Setting up a media gateway for announcements . . . 189
Recording and changing announcements . . . 191
Deleting and erasing announcements . . . 192
Deleting an announcement extension . . . 193
Erasing an announcement source . . . 193
Setting up continuous-play announcements . . . 194
Recording VAL announcements . . . 194
Prerequisites . . . 194
Announcement file format requirements . . . 195
Converting announcement files to VAL format . . . 196
Converting announcements for Interactive Voice Response . . . 197
Deleting VAL announcements . . . 198
Using the SAT to delete individual VAL announcement files . . . 198
Using the SAT to delete all VAL announcements on a circuit pack . . . 198
Using FTP to Manage VAL announcements . . . 199
Setting up an FTP session . . . 200
Performing tasks in an FTP session . . . 201
Recording announcements for TTY callers . . . 205
Reports for Announcements . . . 205
Viewing the Event Report . . . 206
Viewing Voice Announcement Measures . . . 207
Interactions for Announcements . . . 208
Troubleshooting Announcements . . . 209
Announcement capacities and load balancing . . . 210
Non-volatile storage of announcements on VAL . . . 211

Attendant Auto Start and Don’t Split . . . 213
Detailed description of Attendant Auto Start and Don’t Split . . . 213
Auto Start. . . . 213
Don’t Split . . . 213
Administering Attendant Auto Start and Don’t Split . . . 214
Prerequisites for administering Attendant Auto Start and Don’t Split . . . 214
Screens for administering Attendant Auto Start and Don’t Split . . . 214
Assigning a Don’t Split button . . . 215
Reports for Attendant Auto Start and Don’t Split . . . 215
Considerations for Attendant Auto Start and Don’t Split . . . 216
Interactions for Attendant Auto Start and Don’t Split . . . 216

Attendant Auto-Manual Splitting . . . 217
Detailed description of Attendant Auto-Manual Splitting . . . 217

Administering Attendant Auto-Manual Splitting 217
Screens for administering Attendant Auto-Manual Splitting 218

Attendant Backup 219
Detailed description of Attendant Backup 219
Attendant Backup Alerting 220
Administering Attendant Backup 220
Prerequisites for administering Attendant Backup 221
Screens for administering Attendant Backup 221
Setting up Attendant Backup telephones 222
Configuring your system 222
Defining Class of Service console permissions 223
Assigning console permissions to backup telephones 224
Training designated users 226
End-user procedures for Attendant Backup 226
Considerations for Attendant Backup 226
Interactions for Attendant Backup 227

Attendant Call Waiting 229
Detailed description of Attendant Call Waiting 229
Administering Attendant Call Waiting 230
Prerequisites for administering Attendant Call Waiting 230
Screens for administering Attendant Call Waiting 230
Setting up single-line telephones 231
Changing the call-waiting signal 232
Modifying timed intervals 233
Considerations for Attendant Call Waiting 234
Interactions for Attendant Call Waiting 234

Attendant Calling of Inward Restricted Stations 237
Detailed description of Attendant Calling of Inward Restricted Stations 237
Administering Attendant Calling of Inward Restricted Stations 237
Prerequisites for administering Attendant Calling of Inward Restricted Stations 238
Screens for administering Attendant Calling of Inward Restricted Stations 238
Setting up Class of Restriction override 238

Attendant Conference 239
Detailed description of Attendant Conference 239
Administering Attendant Conference 239

Prerequisites for administering Attendant Conference 239
Screens for administering Attendant Conference 240
Setting up Attendant Conference 240
Considerations for Attendant Conference 242
Interactions for Attendant Conference 242

Attendant Control of Trunk Group Access 245
Detailed description of Attendant Control of Trunk Group Access 245
Administering Attendant Control of Trunk Group Access 246
Prerequisites for administering Attendant Control of Trunk Group Access 246
Screens for administering Attendant Control of Trunk Group Access 247
Setting the trunk group threshold 247
Assigning Attendant Control of Trunk Group Access buttons 247
Interactions for Attendant Control of Trunk Group Access 248

Attendant Direct Extension Selection 251
Detailed description of Attendant Direct Extension Selection 251
Standard DXS Tracking 252
Enhanced DXS Tracking 252
Group Display button 252
Administering Attendant Direct Extension Selection 253
Prerequisites for administering Attendant Direct Extension Selection 253
Screens for administering Attendant Direct Extension Selection 253
Considerations for Attendant Direct Extension Selection 253
Interactions for Attendant Direct Extension Selection 254

Attendant Direct Trunk Group Selection 255
Detailed description of Attendant Direct Trunk Group Selection 255
Administering Attendant Direct Trunk Group Selection 256
Prerequisites for administering Attendant Direct Trunk Group Selection 256
Screens for administering Attendant Direct Extension Selection 256
Considerations for Attendant Direct Trunk Group Selection 256
Interactions for Attendant Direct Trunk Group Selection 257

Attendant Intrusion 259
Detailed description of Attendant Intrusion 259
Administering Attendant Intrusion 259
Prerequisites for administering Attendant Intrusion 259
Screens for administering Attendant Intrusion 260
Assigning an intrusion button 260

Reports for Attendant Intrusion 261
Considerations for Attendant Intrusion 261
Interactions for Attendant Intrusion 261

Attendant Lockout - Privacy 263
Detailed description of Attendant Lockout - Privacy 263
Administering Attendant Lockout - Privacy 263
Prerequisites for administering Attendant Lockout - Privacy 263
Screens for administering Attendant Lockout - Privacy 264
Activating or deactivating the Attendant Lockout - Privacy feature 264
Interactions for Attendant Lockout - Privacy 265

Attendant Override of Diversion Features 267
Detailed description of Attendant Override of Diversion Features 267
Administering Attendant Override of Diversion Features 267
Prerequisites for administering Attendant Override of Diversion Features 267
Screens for administering Attendant Override of Diversion Features 268

Attendant Priority Queue 269
Detailed description of Attendant Priority Queue 269
Priority by Call Category 269
Priority by Call Type 271
Administering Attendant Priority Queue 271
Prerequisites for administering Attendant Priority Queue 271
Screens for administering Attendant Priority Queue 272
Setting category priorities 272
Setting the number of calls in the queue 273
Assigning a Call Type button 274
Translating the Call Type button into a user-defined language 275
Considerations for Attendant Priority Queue 276
Interactions for Attendant Priority Queue 276

Attendant Recall 277
Detailed description of Attendant Recall 277
Administering Attendant Recall 277
Prerequisites for administering Attendant Recall 278
Screens for administering Attendant Recall 278
End-user procedures for Attendant Recall 278
Considerations for Attendant Recall 278
Interactions for Attendant Recall 279

Attendant Serial Calling 281
Detailed description of Attendant Serial Calling 281
Administering Attendant Serial Calling 281
Prerequisites for administering Attendant Serial Calling 281
Screens for administering Attendant Serial Calling 282

Attendant Split Swap 283
Detailed description of Attendant Split Swap 283
Administering Attendant Split Swap 283
Prerequisites for administering Attendant Split Swap 283
Screens for administering Attendant Split Swap 284
Assigning a split-swap button 284

Attendant Timers 285
Detailed description of Attendant Timers 285
Administering Attendant Timers 286
Prerequisites for administering Attendant Timers 286
Screens for administering Attendant Timers 287
Setting up Attendant Timers 287
Interactions for Attendant Timers 288
Return Call to (same) Attendant 289
Attendant Overflow Timer 290

Attendant Trunk Identification 291
Detailed description of Attendant Trunk Identification 291
Administering Attendant Trunk Identification 291
Prerequisites for administering Attendant Trunk Identification 291
Screens for administering Attendant Trunk Identification 292

Attendant Vectoring 293
Detailed description of Attendant Vectoring 293
Administering Attendant Vectoring 293
Prerequisites for administering Attendant Vectoring 294
Screens for administering Attendant Vectoring 295
Creating a VDN extension for Attendant Vectoring 295
Assigning the VDN extension for Attendant Vectoring to a console 296
Assigning the VDN extension for Attendant Vectoring to a tenant 297
Considerations for Attendant Vectoring 298
Interactions for Attendant Vectoring 299

Audible Message Waiting 301
Detailed description of Audible Message Waiting 301
Administering Audible Message Waiting 301
Prerequisites for administering Audible Message Waiting 302
Screens for administering Audible Message Waiting 302
Administering Audible Message Waiting for a user 302
Considerations for Audible Message Waiting 303
Interactions for Audible Message Waiting 304

AUDIX One-Step Recording 305
Detailed description of AUDIX One-Step Recording 305
Feature button 306
Language options 306
Periodic alerting tone 306
Ready indication tone 306
Recording delay timer 307
Administering AUDIX One-Step Recording 307
Prerequisites for administering AUDIX One-Step Recording 307
Screens for administering AUDIX One-Step Recording 308
Assigning AUDIX One-Step Recording Parameters 308
Translating telephone feature buttons and labels 310
Translating the AUDIX One-Step Recording text that appears on a telephone display to a user-defined language 310
Translating the AUDIX One-Step Recording button label to a user-defined language 311
Assigning the feature button to a telephone 312
Changing the characteristics of the zip tone 313
End-user procedures for AUDIX One-Step Recording 316
Recording a conversation 316
Considerations for AUDIX One-Step Recording 317
Interactions for AUDIX One-Step Recording 318
Troubleshooting AUDIX One-Step Recording 321

Authorization Codes 323
Detailed description of Authorization Codes 323
Length of authorization codes 323
Using authorization codes 324
AAR and ARS calls 324
Administering Authorization Codes 325
Prerequisites for administering Authorization Codes 325

Screens for administering Authorization Codes 326
Setting up Authorization Codes 326
Creating Authorization Codes with a specific Class of Restriction 329
Considerations for Authorization Codes 330
Interactions for Authorization Codes 330

Automated Attendant 333
Detailed description of Automated Attendant 333
Administering Automated Attendant 333
Prerequisites for administering Automated Attendant 334
Screens for administering Automated Attendant 334
Setting the prompting timeout 335
Administering a vector directory number 336
Administering announcements 336
Controlling hunt groups by vector 336
Assigning a caller information button on a multiappearance telephone 337
Assigning a caller information button on an attendant console 338
Considerations for Automated Attendant 339
Interactions for Automated Attendant 339

Automatic Callback 341
Detailed description of Automatic Callback 341
Ringback Queuing 342
Called Party Queuing 343
Analog Busy Automatic Callback Without Flash 343
QSIG Call Completion - Administrable TSC Signaling Connection 344
ISDN CCBS Supplementary Service on Busy 344
CCBS for Incoming Calls 345
CCBS Call Flow Scenarios 346
CCBS Routing issue 346
Administering Automatic Callback 347
Screens for administering Automatic Callback 348
Assigning a FAC for Automatic Callback 348
Enabling Automatic Callback With Called Party Queuing 349
Setting the no-answer timeout interval 350
Assigning a feature button for Automatic Callback 351
Setting the queue length for Ringback Queuing 351
Enabling CCBS. 352
Considerations for Automatic Callback 353
Interactions for Automatic Callback 355

Automatic Circuit Assurance 359
Detailed description of Automatic Circuit Assurance 359
The referral call 359
The audit trail 360
Administering Automatic Circuit Assurance 360
Screens for administering Automatic Circuit Assurance 360
Reports for Automatic Circuit Assurance 361
Considerations for Automatic Circuit Assurance 361
Interactions for Automatic Circuit Assurance 361

Automatic Number Identification 365
Detailed description of Automatic Number Identification 365
Incoming Automatic Number Identification 365
Outgoing Automatic Number Identification 366
Administering Automatic Number Identification 366
Prerequisites for Automatic Number Identification 366
Screens for administering Automatic Number Identification 367
Setting up ANI on a multifrequency trunk 367
Displaying incoming ANI calling party information 368
Setting up outgoing ANI 369
Prerequisites 369
ANI Reqd 370
Setting up an ANI request button 371
Reports for Automatic Number Identification 372
Considerations for Automatic Number Identification 372
Interactions for Automatic Number Identification 373

Avaya Video Telephony Solution 375
Detailed description of Avaya Video Telephony Solution 375

Bridged Call Appearance 379
Detailed description of Bridged Call Appearance 379
Sample uses 380
Administrable buttons and lamps for multiappearance telephones 380
Administering Bridged Call Appearance 381
Prerequisites for administering Bridged Call Appearance 381
Screens for administering Bridged Call Appearance 382
Creating a bridged call appearance on a single-line telephone 382
Creating a bridged call appearance on a multiappearance telephone 384
Considerations for Bridged Call Appearance 387

Interactions for Bridged Call Appearance 388

Bulletin Board 399
Detailed description of Bulletin Board 399
Administering Bulletin Board 399
Screens for administering Bulletin Board 400
Setting user permissions 400
Changing bulletin board information 401
Considerations for Bulletin Board 404

Busy Indicator 405
Detailed description of Busy Indicator 405
Busy Tone Disconnect 405
Interactions for Busy Indicator 406

Busy Verification 407
Detailed description of Busy Verification 407
Administering Busy Verification 409
Prerequisites for administering Busy Verification 409
Screens for administering Busy Verification 410
Using Busy Verification 410
Considerations for Busy Verification 411
Interactions for Busy Verification 411

Call Charge Information 413
Detailed description of Call Charge Information 413
Advice of Charge 413
Periodic Pulse Metering 413
Charge Display 414
Charge Display at a user telephone 414
Charge Display on a CDR report 414
Administering Call Charge Information 415
Prerequisites for administering Call Charge Information 415
Defining CDR to support Call Charge Information 416
Specifying the frequency of the call charge displays 416
Translating the text "Call Charge" 417
Assigning a COR for charge displays 418
Screens for administering Call Charge Information 419
Administering the charge display 421
Administering a trunk group for call charge displays 421

Assigning a call charge display button for a user 423
Assigning a call charge display feature button for an attendant 424
Administering AOC for ISDN trunks 425
Administering PPM for non-ISDN trunks 427
Administering PPM for DS1 circuit packs 429
End-user procedures for Call Charge Information 432
Displaying call charge information 432
Considerations for Call Charge Information 433
Interactions for Call Charge Information 433

Call Coverage 437
Detailed description of Call Coverage 437
What is a Call Coverage path? 438
Multiple coverage paths 438
Time-of-Day Coverage 439
Off-network Call Coverage 441
Call Coverage changeable coverage paths 442
Extended User Administration of Redirected Calls 442
Call coverage criteria 442
Enhanced Redirection Notification 444
Description 444
Limitations 444
VDN in a call coverage path (VICP) 445
Coverage answer groups 445
Announcement in a coverage path 445
Hunt group in a coverage path 446
Subsequent redirection interval 446
Notifying users when the calls are redirected 446
Caller response interval 446
Consult 447
Limit number of Concurrent Calls 447
Enhancements to LNCC 448
Features that override Call Coverage 448
Conditions that override Call Coverage 449
Administering Call Coverage 450
Prerequisites for administering Call Coverage 451
Screens for administering Call Coverage 452
Creating a coverage path 454
Prerequisites 454
Assigning a coverage path to a user 457

Prerequisites . . . 457
Assigning a Consult button for a user . . . 460
Defining coverage redirected off-network calls . . . 461
Prerequisites . . . 461
Assigning the telephone numbers for the off-network coverage points . . . 461
Administering the coverage path for redirected off-network calls . . . 462
Assigning time-of-day coverage . . . 464
Prerequisites . . . 464
Creating a coverage answer group . . . 466
Assigning Internal Alerting . . . 466
Enabling enhanced Redirection Notification . . . 467
Reports for Call Coverage . . . 468
Considerations for Call Coverage . . . 468
Interactions for Call Coverage . . . 468
Interactions for Limit Number of Concurrent Calls . . . 472
Interaction for Enhanced Redirection Notification . . . 474
Troubleshooting Call Coverage . . . 475

Call Detail Recording . . . 477
Detailed description of Call Detail Recording . . . 477
Monitoring call detail records . . . 478
Legacy CDR and Survivable CDR . . . 478
Setting up Survivable CDR . . . 479
Files for Survivable CDR . . . 479
File naming conventions for Survivable CDR . . . 480
Removing Survivable CDR files. . . . 481
Accessing Survivable CDR files . . . 481
QSIG Supplementary Service - Advice of Charge . . . 481
Administering Charge Advice for QSIG trunks . . . 482
Answer Detection . . . 483
Call classification . . . 483
Network answer supervision . . . 483
Answer supervision by timeout . . . 484
Account Code Dialing . . . 484
Forced Entry of Account Codes . . . 484
Call Splitting . . . 485
Incoming trunk call splitting . . . 485
Examples . . . 486
Outgoing trunk call splitting . . . 488
Examples . . . 488

ITCS, OTCS, and attendant call recording 489
Examples 490
Intraswitch CDR 491
CDR Privacy 492
CDR output 492
CDR record formats 493
Customized CDR call record formats. 495
Standard CDR call record formats for Communication Manager 4.0. 495
Standard CDR call record formats for "legacy" CDR 520
Call detail record field descriptions 545
Administering Call Detail Recording 563
Prerequisites for administering Call Detail Recording 563
Assigning Forced Entry of Account Codes 565
Prerequisites 565
Assigning FEAC for all calls 565
Assigning FEAC to a COR. 566
Assigning FEAC to a user. 567
Assigning privacy digits for a user. 568
Prerequisites 568
Administering the CDR system parameters 570
Administering CDR for a trunk group 580
Administering CDR for a data module 582
Identifying the Inter Exchange Carrier 592
Administering CDR for the paging ports 594
Administering the Intra-Switch CDR 595
Administering Survivable CDR 596
Creating a new user account 596
Administering Survivable CDR for the main server 597
Administering Survivable CDR for an LSP or ESS server 598
End-user procedures for Call Detail Recording 599
Considerations for Call Detail Recording 600
Interactions for Call Detail Recording 601
Interactions for QSIG Supplementary Service - Advice of Charge 613

Call Forwarding 615
Detailed description of Call Forwarding 615
Call Forwarding All Calls 615
Call Forwarding and FAC 616
Call Forwarding and attendants 616
Call Forward Busy/Don’t Answer 616

Call Forwarding Off-Net 617
Call Forwarding Override 617
Notifying users when their calls are redirected 618
Coverage for unanswered forwarded calls 618
Security 618
Administering Call Forwarding 619
Prerequisites for administering the Call Forwarding feature 619
Screens for administering Call Forwarding 621
Viewing user extensions that have the Call Forwarding capabilities active 621
Assigning the Call Forwarding All Calls capability to a user 622
Removing the Call Forwarding All Calls capability for a user 622
Assigning the Call Forward Busy/Don't Answer capability to a user 623
Prerequisites 623
Removing the Call Forward Busy/Don't Answer capability for a user 624
Assigning the Call Forwarding Off-Net capability to a user 624
Prerequisites 624
Removing the Call Forwarding Off-Net capability for a user 626
Enabling the Call Forwarding Override capability for your system 627
Disabling the Call Forwarding Override capability for your system 628
End-user procedures for Call Forwarding 628
Changing the Call Forwarding All Calls destination from an internal telephone 628
Changing the Call Forward Busy/Don't Answer destination from an internal telephone 629
Changing the forwarding destination when a user is at an off-network location 629
Changing the Call Forward Busy/Don't Answer destination when a user is at an off-network location 630
Call Log Enhancements 630
Log Forwarded Calls 630
Considerations 632
Interactions 633

Call Park 637
Detailed description of Call Park 637
Administering Call Park 637
Prerequisites for administering the Call Park feature 638
Screens for administering Call Park 642
Assigning a call park button to a multiple-call appearance telephone 643
End-user procedures for Call Park 644
Using Call Park from a single-line telephone 645

Using Call Park from a multiple-call appearance telephone 645
Using Call Park from an attendant console 645
Retrieving a parked call 645
Considerations for Call Park 646
Interactions for Call Park 646

Call Pickup 649
Detailed description of Call Pickup 649
Call Pickup Alerting 649
Extended Call Pickup 651
Directed Call Pickup 652
Enhanced Call Pickup Alerting 652
Administering Call Pickup 653
Screens for administering Call Pickup 654
Setting up Call Pickup 655
Adding pickup groups 655
Enabling Call Pickup Alerting 656
Enabling Enhanced Call Pickup Alerting 657
Assigning a Call Pickup button to a user telephone 657
Assigning a Call Pickup Feature Access Code 658
Removing a user from a pickup group 659
Deleting pickup groups 660
Getting a list of extended pickup groups 660
Removing a pickup group from an extended pickup group 660
Deleting the pickup group 661
Changing a Call Pickup button on a user telephone 661
Removing a Call Pickup button from a user telephone 662
Setting up simple extended pickup groups 662
Creating simple extended pickup groups 663
Creating an extended pickup group Feature Access Code 663
Assigning pickup groups to a simple extended pickup group 665
Pickup Numbers 666
Setting up flexible extended pickup groups 666
Creating flexible extended pickup groups 667
Assigning pickup groups to a flexible extended pickup group 669
Changing extended pickup groups 670
Changing from simple to flexible 670
Changing from flexible to simple 671
Setting up Directed Call Pickup 671
Prerequisites 671

Creating Classes of Restriction for Directed Call Pickup 672
Assigning a Class of Restriction to a user 674
Assigning a Directed Call Pickup button 675
Assigning a Directed Call Pickup Feature Access Code 675
Removing Directed Call Pickup from a user 676
End-user procedures for Call Pickup 677
End-user procedures for Directed Call Pickup 677
Considerations for Call Pickup 678
Interactions for Call Pickup 678

Call Waiting Termination 681
Detailed description of Call Waiting Termination 681
Call Waiting tones 681
Administering Call Waiting Termination 682
Prerequisites for administering Call Waiting Termination 682
Screens for administering Call Waiting Termination 683
Assigning Call Waiting Termination 684
Considerations for Call Waiting Termination 685
Interactions for Call Waiting Termination 686

Call-by-Call Service Selection 687
Detailed description of Call-by-Call Service Selection 687
ISDN messages and information elements for usage allocation 688
Usage Allocation Plans 689
Incoming call-handling treatment. 690
Call Detail Recording 690
Administering Call-by-Call Service Selection 691
Prerequisites for administering Call-by-Call Service Selection 691
Screens for administering Call-by-Call Service Selection 692
Setting up a trunk group for CBC. 692
Administering incoming call handling treatment 693
Administering route patterns for the CBC trunk group 694
Administering network facilities 695
Interactions for Call-by-Call Service Selection 697

Caller ID 699
Detailed description of Caller ID 699
Caller ID on analog trunks 700
Caller ID on digital trunks 700
Administering Caller ID 700

Prerequisites for administering Caller ID 700
Screens for administering Caller ID 701
Displaying Caller ID information 701
Considerations for Caller ID 702
Interactions for Caller ID 702

Centralized Attendant Service 705
Detailed description of Centralized Attendant Service 705
Branch-generated call identification tones 706
Administering Centralized Attendant Service 707
Prerequisites for administering Centralized Attendant Service 707
Screens for administering Centralized Attendant Service 708
Reports for Centralized Attendant Service. 708
Considerations for Centralized Attendant Service 708
Interactions for Centralized Attendant Service 710

Class of Restriction 715
Detailed description of Class of Restriction 715
Mask CLI/Station Name for Internal Calls 716
Strategy for assigning CORs 717
Types of restrictions. 718
Calling party restrictions 718
Called party restrictions 719
Fully restricted service 720
COR-to-COR restrictions 720
Administering Class of Restriction 721
Screens for administering Class of Restriction 721
Displaying administered CORs 722
Setting up a COR 722
Allowing users to change their own COR 726
Assigning a FAC 726
Assigning a password. 727
End-user procedures for Class of Restriction 728
Reports for Class of Restriction 728
Interactions for Class of Restriction 729

Class of Service 733
Detailed description of Class of Service 733
Administering Class of Service. 733
Prerequisites for administering Class of Service 734

Screens for administering Class of Service 734
Defining COS for your system 734
Descriptions of the COS features 735
Assigning a COS 738
Considerations for Class of Service 739
Interactions for Class of Service 739

Conference 741
Detailed description of Conference 741
Conference and DCP, hybrid, IP, wireless, and ISDN-BRI telephones 741
Meet-me Conference 742
Conference/Transfer Toggle/Swap 742
No Dial Tone Conferencing 742
No Hold Conference 743
Select Line Appearance Conferencing 743
Selective Conference Party Display, Drop, and Mute 743
Click to Conference 744
Administering Conference 744
Prerequisites for administering the Conference feature 744
Screens for administering Conference 747
Assigning the togle-mute feature button 748
Assigning feature buttons 748
Prerequisites 748
Assigning feature buttons to a user 750
Assigning feature buttons to an attendant 751
End-user procedures for Conference 752
Displaying the participants on a conference call 752
Considerations for Conference 753
Interactions for Conference 753

Co-resident DEFINITY LAN Gateway 755
Detailed description of Co-resident DEFINITY LAN Gateway 755
Administering Co-resident DEFINITY LAN Gateway 756
Prerequisites for administering Co-resident DEFINITY LAN Gateway 756
With the TN799 C-LAN circuit pack as the Ethernet Interface 756
With the TN2314 circuit pack as the Ethernet Interface 757
Screens for administering Co-resident DEFINITY LAN Gateway 757
Considerations for Co-resident DEFINITY LAN Gateway 758

Co-residency of Communication

Manager and SIP Enablement Services 761
Detailed description of Co-residency of Communication Manager and SIP Enablement Services 761
Data Call Setup 763
Detailed description of Data Call Setup 763
Administering Data Call Setup 766
Prerequisites 767
Screens for administering Data Call Setup 768
Defining a data module 768
Specifying the port location 780
Assigning the data extension feature button 781
End-user procedures for Data Call Setup 782
Setting up and disconnecting data calls from a DCP data terminal 783
Setting up data calls from a DCP telephone 783
Setting up and disconnecting data calls from an ISDN-BRI data terminal. 784
Setting up data calls from an ISDN-BRI telephone 784
Considerations for Data Call Setup 785
Interactions for Data Call Setup 785
Default Dialing 787
Detailed description of Default Dialing 787
Administering Default Dialing 787
Screens for administering Default Dialing 788
Demand Print 789
Detailed description of Demand Print 789
Administering Demand Print 789
Screens for administering Demand Print 789
Dial Access to Attendant 791
Detailed description of Dial Access to Attendant 791
Administering Dial Access to Attendant 791
Prerequisites for administering Dial Access to Attendant 791
Screens for administering Dial Access to Attendant 792
Changing the attendant access code 792
Reports for Dial Access to Attendant 793
Interactions for Dial Access to Attendant 794

Dial Plan 795
Detailed Description of Dial Plan 795
Dial Plan enhancements for Communication Manager 795
Dial plan information 796
Multi-location dial plan 797
Short dialing 797
Location prefix 797
Location prefix example 798
Other options for the dial plan 798
AAR/ARS Internal Call Prefix 800
AAR/ARS Internal Call Total Length 801
ETA Node Number 801
ETA Routing Pattern 801
Local Node Number 802
UDP Extension Search Order 802
Retry ARS Analysis if All-Location Entry Inaccessible (ESS/LSP)? 802
Dial Plan Analysis Table 803
Dial Plan Parameters 805
Multi-Location Dial Plan 805
Other options for Dial Plan 806
Administering Dial Plan 806
Prerequisites for administering Dial Plan 807
Screens for administering Dial Plan 807
Defining your dial plan 807
Adding extension ranges 812
Defining a multi-location dial plan 813
Prerequisites 813
Considerations for Dial Plan 813
Interactions for Dial Plan 814

Dial Plan Transparency 821
Detailed Description of Dial Plan Transparency 821
Administering Dial Plan Transparency 821
Prerequisites for administering Dial Plan Transparency 822
Screens for administering Dial Plan Transparency 822
Setting up Dial Plan Transparency 822
Maintenance for Dial Plan Transparency 825
Alarms 825
Audits/Logging 826
Debugging/Diagnostic Tools 826

Considerations for Dial Plan Transparency 826
Fiber PNC with Remote PNs 827
Interactions for Dial Plan Transparency 827
Overview 827
AAR/ARS partitioning 827
Abbreviated Dialing 828
Alternate facilities restriction levels 828
Announcements 828
Attendants 828
Authorization Codes 828
Automatic Callback 828
ANI 828
ARS 828
Bridging 829
Busy Indicator 829
Call Detail Recording 829
Call Forwarding 829
Call Park 829
Call Pickup 830
Conference 830
Coverage 830
Crisis Alert 830
E911 830
EC500 831
Enterprise Mobility User 831
Group Paging 831
Hunt Groups 831
Intercom 831
IP Endpoints 831
Last Number Dialed 832
Leave Word Calling 832
Loudspeaker paging 832
Malicious Call Trace 832
Meet-me Conference 832
Message Retrieval 833
Multi-Level Precedence and Preemption 833
No-Hold Conferencing 833
Personal Station Access 833
Priority Calling 833
Service Observing 833

Station Lock 833
TTI 834
Transfer 834
Transfer into/out of Voice Mail 834
Voice Messaging 834
Whisper Paging 835

Distinctive Ringing 837
Detailed description of Distinctive Ringing 837
Administering Distinctive Ringing 837
Prerequisites for administering Distinctive Ringing 838
Screens for administering Distinctive Ringing 838
Defining Distinctive Ringing 838
Reports for Distinctive Ringing 840
Considerations for Distinctive Ringing 841
Interactions for Distinctive Ringing 841

Enhanced 911 843
Detailed description of Enhanced 911 843
Configurations with media gateways in different locations 845
Location Specific Routing 845
E911 for wired IP telephones 847
Emergency Extension Forwarding 848
Call Forwarding of dropped emergency calls 848
Crisis Alert 849
Cancelling an alert 850
Administering Enhanced 911 850
Prerequisites for administering Enhanced 911 851
Screens for administering Enhanced 911 851
Setting up Crisis Alert to an attendant or a display telephone 852
Setting up the emergency number 853
Setting up the attendant console to receive emergency notification 854
Setting up digital telephones to receive emergency notification 855
Setting which users must acknowledge the emergency alert 856
Setting up Crisis Alert to notify a digital pager 857
Prerequisites 857
Setting up emergency extension forwarding 859
Setting up CAMA numbering 861
Reports for Enhanced 911 863
Considerations for Enhanced 911 863

Interactions for Enhanced 911 864

Emergency Calls from Unnamed IP Endpoints 867
Detailed description of Emergency Calls from Unnamed IP Endpoints 867
Changed screens 868
Feature-Related System Parameters screen 869
Port Information screen 870
System Capacity screen 870
Changed commands 871
reset ip-stations command 871
Administering Emergency Calls from Unnamed IP Endpoints 871
Prerequisites for administering Emergency Calls from Unnamed IP Endpoints 872
Screens for administering Emergency Calls from Unnamed IP Endpoints 874
Reports for Emergency Calls from Unnamed IP Endpoints 874
Interactions for Emergency Calls from Unnamed IP Endpoints 876

Enterprise Mobility User 877
Detailed description of Enterprise Mobility User 877
EMU Enhancements for Communication Manager 4.0 877
Extension to Cellular Availability with EMU 878
A home station of a visitor can be visited 878
The EMU timer 878
System requirements for EMU 879
EMU use and activation 879
EMU supported telephone buttons 880
EMU call processing 881
EMU and the station lock feature 881
Traffic considerations 881
Message waiting indication 882
Administering Enterprise Mobility User 882
Prerequisites for administering Enterprise Mobility User 882
Screens for administering Enterprise Mobility User 883
Configuring your system for Enterprise Mobility User 883
Setting EMU options for stations 887
Defining options for calling party identification 888
End-user procedures for Enterprise Mobility User 889
EMU activation process 889
EMU deactivate process 890

Enbloc Dialing and Call Type Digit Analysis 891
Detailed description of Enbloc Dialing and Call Type Digit Analysis 891
Recovery strategy and behavior 892
High-level Capacities 892
Administering Enbloc Dialing and Log Type Digit Analysis 893
Prerequisites for administering Log Dialing Digit Analysis 893
Administering Call Type Digit Analysis 893
Example of Call Type Digit Analysis 894
Interactions for Enbloc Dialing and Call Type Digit Analysis 894
End User Procedures for Enbloc Dialing and Call Type Digit Analysis 895

Enhanced Call Forwarding 897
Detailed description of Enhanced Call Forwarding 897
Chained Call Forwarding 898
Feature Button 898
Administering Enhanced Call Forwarding 899
Viewing Station Status for Enhanced Call Forwarding 899
Enabling Feature Access Codes for Enhanced Call Forwarding 900
Enabling Chained Call Forwarding 901
Specifying a coverage path 902
End-user procedures for Enhanced Call Forwarding 902
Activating Enhanced Call Forwarding 903
Deactivating Enhanced Call Forwarding 904
Reactivating Enhanced Call Forwarding 905
Displaying Status 906
Activating and deactivating Enhanced Call Forwarding from an off-network phone 906
Activating and deactivating Enhanced Call Forwarding from a phone with console permission 907
Interactions for Enhanced Call Forwarding 908
Interactions for Chained Call Forwarding 911

Expanded Meet-me Conferencing 913
Detailed description of Expanded Meet-me Conferencing 913
Highlights of Expanded Meet-me Conferencing 913
Expanded Meet-me Conferencing vectors and VDNs 914
Expanded Meet-me Conferencing display updates 915
Status screens for Expanded Meet-me Conferencing 916
Administering Expanded Meet-me Conferencing 916

Prerequisites for administering Expanded Meet-me Conferencing 916
Screens for administering Expanded Meet-me Conferencing 917
Setting the maximum number of parties for each conference 918
Changing or creating a VDN for Expanded Meet-me Conferencing 919
Setting language translations. 921
End-user procedures for Expanded Meet-me Conferencing 921
Interactions for Expanded Meet-me Conferencing 922

Extended User Administration of Redirected Calls 923
Detailed description of Extended User Administration of Redirected Calls 923
Disabling the telecommuting access extension 924
Extended User Administration of Redirected Calls and DCS 924
Extended User Administration of Redirected Calls and Class of Service 924
Extended User Administration of Redirected Calls and COR 925
Extended User Administration of Redirected Calls from an off-site telephone . . . 925
Administering Extended User Administration of Redirected Calls 925
Prerequisites for administering Extended User Administration of Redirected Calls 926
Screens for administering Extended User Administration of Redirected Calls . . . 931
Assigning a Station Security Code to a user 931
End-user procedures for Extended User Administration of Redirected Calls 932
Changing Call Coverage or activating Call Forwarding from an onsite telephone that is not assigned to the user 933
Deactivating Call Forwarding from an onsite telephone that is not assigned to the user 933
Interactions for Extended User Administration of Redirected Calls 934

Extension to Cellular 937
Detailed description of Extension to Cellular 937
Overview 938
Conditional Call Extending Feature 940
Shared Voice Connections Feature 940
Sharing Mappings among CM PBXs 941
SPFMC OPTIM Application 941
one-X Mobile Server and Application Support. 941
Application RTUs for Fixed Mobile Convergence 941
ARS/AAR routing 942
Basic Extension to Cellular operation 943
Call Detail Recording 944
CDR Reports for Extension to Cellular Calls. 944
Call filtering 946

Caller ID from the cell phone . . . 947
Capacity limitations . . . 947
Configuration sets . . . 948
Extension to Cellular Feature Access Codes . . . 948
EC500 Activation/Deactivation . . . 948
Self Administration Feature Access Code . . . 949
Conditional Call Extending . . . 949
Feature buttons on the office telephone . . . 950
Feature Name Extensions . . . 950
Multiple sets of Feature Name Extensions . . . 951
Mobile Call (CTI) Extension . . . 951
Multiple applications . . . 951
one-X Mobile Server and Application Support . . . 952
R2MFC trunks . . . 954
Security features . . . 954
Security codes . . . 954
Security tones . . . 955
Shared Voice Connections . . . 955
Sharing Mappings among CM PBXs . . . 957
SPFMC OPTIM Application . . . 957
Telephones supported . . . 957
Voice mail . . . 958
Voice Mail Avoidance . . . 958
Use timing to route calls . . . 959
Prevent coverage by cellular voice mail . . . 959
Cellular Voice Mail Avoidance Using Confirmed Answer . . . 960
Administering Extension to Cellular . . . 960
Prerequisites for administering Extension to Cellular . . . 961
Plan extensions and codes . . . 961
Review customer options . . . 962
Screens for administering Extension to Cellular . . . 963
Mapping an office telephone to a cell phone . . . 964
Setting up Feature Access Codes . . . 966
Creating a telecommuting access number . . . 967
Setting up Feature Name Extensions set . . . 968
Creating a Self Administration Feature access code . . . 970
Administer the office extension . . . 970
Administer the Feature Access Code . . . 971
Creating FACs to enable/disable Extension to Cellular . . . 972
Creating a Station Security Code FAC . . . 972

Creating a system-wide SSC change FAC 973
Defining the Station Security Code length 973
Administering an enable/disable feature button 974
Changing the EC500 state on the station form 975
Administering the feature button 975
Setting the optional timer 976
Administering a feature button to extend a call 977
Reviewing feature button assignments 977
Sending 10-digit caller identification for locally originated calls 979
Administering Confirmed Answer for Cellular Voice Mail Avoidance 980
Administering call filtering 980
Administering voice mail coverage 981
Setting up a Cellular Voice Mail Avoidance timer 981
Using timing to route calls to voice mail 982
Setting up Call Detail Recording 983
Enable CDR for the outgoing trunk 984
Enable CDR for Extension to Cellular 985
Generating two CDR records 985
Changing configuration sets 986
Administering the barge-in tone 988
Displaying System Capacity 989
Administering Conditional Call Extending 990
Administering Sharing Mapping among CM PBXs 991
Administration for one-X Mobile Server and Application Support 993
End-user procedures for Extension to Cellular 995
Considerations for Extension to Cellular 995
Upgrades from prior versions 996
Upgrade from Extension to Cellular Version 5. 997
Upgrade from Extension to Cellular Version 4 997
Upgrade from Extension to Cellular Version 3 998
Upgrade from Extension to Cellular Version 2 999
Upgrade from Extension to Cellular Version 1 1000
Interactions for Extension to Cellular 1001
Attendant 1001
Call coverage. 1001
Call Detail Recording 1001
Cellular service provider voice mail 1001
Class of Restriction 1002
Distributed Communications System 1002
Distinctive alerting 1002

Extension to Cellular enable and disable . . . 1002
Feature Access Codes. . . . 1003
Feature Name Extensions . . . 1003
Message waiting indication . . . 1003
“Notify me” under Unified Messenger for MS Exchange . . . 1003
Office caller ID for another Extension to Cellular user . . . 1003
QSIG . . . 1004
Troubleshooting Extension to Cellular . . . 1004
Installation and administration test . . . 1004
Test procedures . . . 1004
Users cannot receive Extension to Cellular calls on their cell phones . . . 1014

Facility and Non-Facility Associated Signaling . . . 1017
Detailed description of Facility and Non-Facility Associated Signaling . . . 1017
D-channel backup with NFAS . . . 1017
D-channel backup activation . . . 1019
Administering Facility and Non-Facility Associated Signaling . . . 1019
Prerequisites for administering Facility and Non-Facility Associated Signaling. . . . 1019
Screens for administering Facility and Non-Facility Associated Signaling . . . 1020
Reviewing the guidelines for FAS and NFAS . . . 1020
Implementing FAS and NFAS . . . 1021
Administering the DS1 Circuit Pack screen . . . 1021
Administering the Interface Links and Processor Channels screens . . . 1022
Administering the ISDN-PRI Trunk Group, Signaling Group, and Trunk Group Members screens . . . 1022

Facility Restriction Levels . . . 1025
Detailed description of Facility Restriction Levels . . . 1025
AAR and ARS calls . . . 1025
Originators of AAR and ARS calls . . . 1025
Call termination points for AAR and ARS calls . . . 1026
AFRL . . . 1027
Alt-frl feature button . . . 1027
Authorization codes . . . 1027
Administering Facility Restriction Levels . . . 1028
Screens for administering Facility Restriction Levels . . . 1028
End-user procedures for Facility Restriction Levels . . . 1029
Reports for Facility Restriction Levels . . . 1029
Considerations for Facility Restriction Levels . . . 1030

Interactions for Facility Restriction Levels 1030

Facility Test Calls 1031
Detailed description of Facility Test Calls 1031
Security 1032
Administering Facility Test Calls 1032
Screens for administering Facility Test Calls 1033
Considerations for Facility Test Calls 1033
Interactions for Facility Test Calls 1033

Feature Access Codes 1035
Detailed description of Feature Access Codes 1035
Administering Feature Access Codes 1036
Prerequisites for administering Feature Access Codes 1036
Screens for administering Feature Access Codes 1036
Assigning Feature Access Codes 1037
Changing or deleting Feature Access Codes 1038
Troubleshooting Feature Access Codes 1039

Group Paging 1041
Detailed Description of Group Paging 1041
Restrictions 1041
Controlling access to paging groups 1041
Administering Group Paging 1042
Screens for administering Group Paging 1042
Creating a paging group 1042
Changing a paging group 1044
Viewing all paging groups 1044
Considerations for Group Paging 1045
Interactions for Group Paging 1045
Troubleshooting Group Paging 1047

Hold 1049
Detailed description of Hold 1049
Soft Hold 1049
Hard Hold 1049
Automatic Hold 1050
Administering Hold 1050
Prerequisites for administering Hold 1050
Screens for administering Hold 1051

Enabling Automatic Hold 1051
Assigning a FAC for CAS remote hold and answer 1052
Reports for Hold 1053
Considerations for Hold 1054
Interactions for Hold 1054

Hot Line Service 1057
Detailed description of Hot Line Service 1057
Administering Hot Line Service 1058
Screens for administering Hot Line Service 1058
Reports for Hot Line Service 1058
Considerations for Hot Line Service 1059
Interactions for Hot Line Service 1059

Hunt Groups 1061
Detailed description of Hunt Groups 1061
Announcements for hunt groups 1062
Delay announcement intervals for hunt groups 1062
Analog, aux-trunk, or integrated delay announcements for hunt groups 1063
Call Coverage for hunt groups 1063
Call Distribution methods for hunt group types 1064
Hunt group extension unavailability 1065
Hunt Group Busy option 1066
Using Send All Calls with hunt groups 1066
Using Call Forwarding All Calls with hunt groups 1066
Queues for hunt groups 1067
TTY hunt groups 1067
Administering Hunt Groups 1068
Screens for administering Hunt Groups 1068
Setting up hunt groups 1069
Changing hunt groups 1069
Setting up queues for hunt groups 1070
Adding hunt group announcements 1070
Setting up night service for hunt groups 1071
Considerations for Hunt Groups 1071
Interactions for Hunt Groups 1073

Individual Attendant Access 1075
Detailed description of Individual Attendant Access 1075
Administering Individual Attendant Access 1075

Prerequisites for administering Individual Attendant Access 1075
Screens for administering Individual Attendant Access 1076
Assigning an extension to an attendant console 1076

Intercom 1077
Detailed description of Intercom 1077
Intercom groups 1077
Telephones 1078
Administering Intercom 1078
Interactions for Intercom 1078

Internal Automatic Answer 1079
Detailed description of Internal Automatic Answer 1079
Administering Internal Automatic Answer 1080
Screens for administering Internal Automatic Answer 1080
Reports for Internal Automatic Answer 1080
Considerations for Internal Automatic Answer 1081
Interactions for Internal Automatic Answer 1081

Inter-PBX Attendant Service 1085
Detailed description of Inter-PBX Attendant Service 1085
Administering Inter-PBX Attendant Service 1085
Prerequisites for administering Inter-PBX Attendant Service 1085
Screens for administering Inter-PBX Attendant Service 1086
Enabling Inter-PBX Attendant Service 1086
Reports for Inter-PBX Attendant Service. 1087
Considerations for Inter-PBX Attendant Service 1087
Interactions for Inter-PBX Attendant Service 1088

ISDN Service 1089
Detailed description of ISDN Service 1089
Transmission rate and protocols 1090
AT&T Switched Network protocol 1091
Private network services 1093
ETN services 1093
DCS services 1094
QSIG services 1094
Wideband Switching (ISDN-PRI only) 1094
Call-by-Call Service Selection. 1094
Access to Software Defined Data Network. 1094

Access to Switched Digital International 1094
National ISDN-2 services 1095
Calling Line Identification 1095
Non-Facility Associated Signaling (ISDN-PRI only) 1095
D-Channel Backup (ISDN-PRI only) 1095
Wideband Switching (ISDN-PRI only) 1095
Call-by-Call Service Selection 1095
ISDN interworking 1096
Call Identification Display 1097
Displays for redirected calls 1098
Displays for conference calls 1099
Displays for calls to hunt groups 1099
Displays for calls to Terminating Extension Groups 1099
Caller Information Forwarding 1099
Facilities restriction level and traveling class mark 1099
Information Indicator Digits (II-digits) 1099
Malicious Call Trace 1099
Multiple Subscriber Number - Limited 1100
Overlap Sending 1100
Interworking between TGU/TGE trunks and ISDN (Italy) 1100
Administering ISDN Service 1100
Screens for administering ISDN Service 1100
Interactions for ISDN Service 1101

Last Number Dialed 1103
Detailed description of Last Number Dialed 1103
Administering Last Number Dialed 1103
Screens for administering Last Number Dialed 1103
Considerations for Last Number Dialed 1104
Interactions for Last Number Dialed 1104

Leave Word Calling 1105
Detailed description of Leave Word Calling 1105
Voice synthesis 1106
End-user procedures for Leave Word Calling 1106
Considerations for Leave Word Calling 1107
Interactions for Leave Word Calling 1107

Line Lockout 1109
Detailed description of Line Lockout 1109

Administering Line Lockout 1109
Screens for administering Line Lockout 1110
Reports for Line Lockout 1110
Considerations for Line Lockout 1110

Listed Directory Number 1113
Detailed description of Listed Directory Number 1113
Incoming DID trunk calls to the attendant group 1113
Incoming FX and CO trunk calls to the attendant group 1113
Administering Listed Directory Number 1114
Prerequisites for administering Listed Directory Number 1114
Screens for administering Listed Directory Number 1114
Assigning listed directory numbers 1115
Assigning an incoming destination to a trunk 1116
Reports for Listed Directory Number. 1117
Considerations for Listed Directory Number 1117
Interactions for Listed Directory Number 1117

Locally Sourced Announcements and Music 1119
Detailed description of Locally Sourced Announcements and Music 1119
Administering Locally Sourced Announcements and Music 1120
Screens for administering Locally Sourced Announcements and Music 1121
Adding an audio group 1122
Listing all audio groups 1123
Changing audio group extensions 1123
Listing audio group extensions. 1123
Adding a music-on-hold group 1124
Listing music-on-hold groups 1125
Changing music-on-hold source type 1126
Adding music sources to a tenant partition 1127
Displaying VAL board or vVAL group descriptions 1129
Displaying system capacities 1129
Reports for Locally Sourced Announcements and Music 1130
Considerations for Locally Sourced Announcements and Music 1130
Interactions for Locally Sourced Announcements and Music 1131

Loss Plans 1133
Detailed description of Loss Plans 1133
Administering Loss Plans. 1134
Prerequisites for administering Loss Plans 1134

Guidelines for using loss groups 1134
Screens for administering Loss Plans 1135

Loudspeaker Paging 1137
Detailed description of Loudspeaker Paging 1137
Types of Paging 1137
Deluxe paging 1137
Chime paging 1138
Auxiliary paging systems 1139
Restrictions on loudspeaker paging 1139
Administering Loudspeaker Paging 1139
Prerequisites for administering Loudspeaker Paging 1140
Screens for administering Loudspeaker Paging 1140
Setting up Voice Paging over loudspeakers 1141
Setting up Chime Paging over Loudspeakers 1142
Assigning a chime page code to an individual extension 1144
Interactions for Loudspeaker Paging 1145
Troubleshooting Loudspeaker Paging 1146

Malicious Call Trace 1147
Detailed description of Malicious Call Trace 1147
Activation 1147
Control 1147
Deactivation 1148
MCT voice recorder 1148
Administering Malicious Call Trace 1149
Prerequisites for administering Malicious Call Trace 1149
Screens for administering Malicious Call Trace 1150
Defining Malicious Call Trace on your system 1150
Assigning an MCT feature button for an attendant 1153
Assigning an MCT feature button for a user 1153
Administering MCT for ISDN notification 1154
End-user procedures for Malicious Call Trace 1157
Activating MCT with a feature button when you receive a malicious call 1157
Activating MCT with a FAC when you are active on a call 1157
Activating MCT with a FAC when you are not active on a call 1158
Requesting that an MCT controller on a tandemed server continue the trace . . . 1158
Displaying MCT information 1158
Deactivating MCT 1158
Reports for Malicious Call Trace 1159

Considerations for Malicious Call Trace 1159
Interactions for Malicious Call Trace 1160

Manual Message Waiting 1163
Detailed description of Manual Message Waiting 1163
Administering Manual Message Waiting 1163
Screens for administering Manual Message Waiting 1164
Assigning the Manual Message Waiting feature button 1164

Manual Signaling 1167
Detailed description of Manual Signaling 1167
Administering Manual Signaling 1167
Screens for administering Manual Signaling 1168
Assigning a manual signaling button for a multiple-call appearance telephone user 1168
End-user procedures for Manual Signaling 1169
Interactions for Manual Signaling 1169

Meet-me Conference 1171
Detailed description of Meet-me Conference 1171
Administering Meet-me Conference 1171
Prerequisites for administering Meet-me Conference 1172
Screens for administering Meet-me Conference 1172
Creating or changing a Meet-me Conference vector 1173
Options for creating vector steps 1175
How the vector processes a call 1176
Creating a Meet-me Conference VDN 1177
End-user procedures for Meet-me Conference 1179
Accessing a Meet-me Conference as an attendee 1179
Changing a Meet-me Conference access code 1180
Using Selective Conference Party Display, Drop, and Mute 1180
Considerations for Meet-me Conference 1181
Interactions for Meet-me Conference 1184
Troubleshooting Meet-me Conference 1185

Modem Pooling 1187
Detailed description of Modem Pooling 1187
Administering Modem Pooling 1188
Screens for administering Modem Pooling 1188
Considerations for Modem Pooling 1189

Interactions for Modem Pooling 1189

Multifrequency Signaling 1191
Detailed description of Multifrequency Signaling 1191
MFE 1192
MF Shuttle 1192
R2-MFC 1192
Guidelines for administering Multifrequency Signaling 1192
Administering Multifrequency Signaling 1194
Screens for administering Multifrequency Signaling 1194
Considerations for Multifrequency Signaling 1194
Interactions for Multifrequency Signaling 1195

Multiple Level Precedence and Preemption 1199
Detailed description of Multiple Level Precedence and Preemption 1199
Precedence Calling 1200
Precedence levels 1200
Format for dialed digits 1201
Access digits 1201
Address digits 1201
Precedence Calling diversion scenarios 1202
How service domains influence preemption and precedence 1204
Station-to-station calls on the same server 1205
Precedence calls to destinations over ISDN-PRI trunks 1206
Precedence calls to destinations over non-ISDN-PRI trunks 1207
Announcements for Precedence Calling 1209
Precedence Call Waiting 1210
Precedence Routing 1210
Dual Homing 1210
End Office Access Line Hunting 1211
Preemption 1211
Line Load Control 1212
Worldwide Numbering and Dialing Plan 1213
Feature Access Code 1214
Route Code 1214
Address Digits 1215
Administering Multiple Level Precedence and Preemption 1216
Prerequisites for administering Multiple Level Precedence and Preemption 1218
Screens for administering Multiple Level Precedence and Preemption 1218
Precedence Calling 1220

Assigning an MLPP Feature Access Code 1220
Assigning Precedence Calling system parameters 1221
Assigning a maximum precedence level 1222
Assigning trunks 1223
Assigning a hot line number 1224
Assigning attendant queue priorities 1227
Announcements for Precedence Calling 1228
Adding extensions 1228
Assigning announcement types 1229
Recording announcements 1229
Deleting announcements 1230
Saving announcements 1230
Precedence Call Waiting 1231
Enabling Precedence Call Waiting for a telephone 1231
Setting the Precedence Call timeout 1232
Assigning Feature Access Codes 1233
Precedence Routing 1234
Assigning digit analysis 1234
Assigning route patterns 1237
Assigning digit conversion 1238
Dual Homing 1239
End Office Access Line Hunting 1240
Preemption 1240
Assigning Preemption to a COR 1240
Assigning trunks for Preemption 1241
Setting the Precedence Call timeout 1241
Line Load Control 1241
Worldwide Numbering and Dialing Plan 1242
Assigning WNDP system parameters 1242
Assigning WNDP Feature Access Codes 1243
Assigning a hot line number 1243
Assigning attendant queue priorities 1244
Considerations for Multiple Level Precedence and Preemption 1245
Precedence Calling 1245
Announcements for Precedence Calling 1245
Precedence Call Waiting 1245
Precedence Routing 1246
Preemption 1246
Line Load Control 1246
Worldwide Numbering and Dialing Plan 1246

Interactions for Multiple Level Precedence and Preemption 1247
Precedence Calling 1247
Precedence Call Waiting 1250
Precedence Routing 1251
Preemption 1252
Line Load Control 1254
Worldwide Numbering and Dialing Plan (WNDP) 1256

Multi-Location Dial Plan 1259
Detailed description of Multi-Location Dial Plan 1260
Location prefix 1260
Feature Access Codes 1261
Announcements 1262
Invalid announcements 1262
Maintenance 1263
Administering Multi-Location Dial Plan 1263
Prerequisites for administering Multi-Location Dial Plan 1264
Screens for administering Multi-Location Dial Plan 1264
Changing extensions 1265
Function 1266
Exceptions 1266
Audits 1266
Prepending numbers to the dialed string 1267
Setting up announcements 1268
Setting up a local centralized answering point 1269
Setting up multiple Feature Access Codes for attendants 1270
Setting up multiple Feature Access Codes for ARS 1270
Interactions for Multi-Location Dial Plan 1270

Music-on-Hold 1273
Detailed description of Music-on-Hold 1273
Administering Music-on-Hold 1274
Prerequisites for administering Music-on-Hold 1274
Screens for administering Music-on-Hold 1274
Assigning music tones, music ports, and music for transferred trunks 1275
Defining a Class of Restriction for Music-on-Hold 1277
Connecting a music source to the server 1278
Assigning a source of music to a port 1278
Reports for Music-on-Hold 1279
Considerations for Music-on-Hold 1279

Interactions for Music-on-Hold 1280

Night Service 1281
Detailed description of Night Service 1281
Hunt Group Night Service 1281
Night Console Service 1281
Night Station Service 1282
Trunk Answer from Any Station 1282
Trunk Group Night Service 1283
Administering Night Service 1283
Screens for administering Night Service 1284
Setting up night station service to voice mail 1284
Setting up Night Console Service 1287
Setting up Night Station Service 1288
Setting up Trunk Answer from Any Station 1290
Setting up external alerting 1291
Setting up external alerting Night Service 1291
Setting up Night Service for trunk groups 1293
Setting up Night Service for hunt groups 1294
Considerations for Night Service 1295
Considerations for Hunt Group Night Service 1295
Considerations for Night Console Service 1295
Considerations for Night Station Service 1295
Considerations for TAAS 1296
Considerations for Trunk Group Night Service 1296
Interactions for Night Service 1297
Interactions for Hunt Group Night Service 1297
Interactions for Night Console Service 1298
Interactions for Night Station Service 1298
Interactions for TAAS 1299
Interactions for Trunk Group Night Service 1299

Off-Premises Station 1301
Detailed description of Off-Premises Station 1301
Administering Off-Premises Station 1302
Screens for administering Off-Premises Station 1302
Activating Off-Premises Station for a user 1302
Interactions for Off-Premises Station 1304

Overriding of SAC/CF 1305
Detailed description 1305

Administer overriding of SAC/CF 1305
Enabling SAC/CF Override by Dialing or Priority calling 1306
Enabling SAC/CF Override Protection 1307
Enabling SAC/CF Override for station with or without display 1307
Using SAC/CF Override 1307
Overriding of SAC/CF 1308
Asking for Overriding of SAC/CF 1310
No Overriding of SAC/CF 1313

Personal Station Access 1317
Detailed description of Personal Station Access 1317
Telecommuting 1317
Invalid attempts to use PSA 1317
Preferences and permissions 1318
Button mapping 1318
Unanswered calls 1318
Dissociated telephones 1319
Security 1320
Administering Personal Station Access 1320
Prerequisites for administering Personal Station Access 1320
Screens for administering Personal Station Access 1322
End-user procedures for Personal Station Access 1323
Using the PSA associate command 1323
Interrupting the PSA associate command sequence 1325
Using the PSA dissociate command 1325
Reports for Personal Station Access 1325
Considerations for Personal Station Access 1325
Interactions for Personal Station Access 1326
Hot Desking interaction with PSA 1327

Personalized Ringing 1329
Detailed description of Personalized Ringing 1329
Ringing patterns 1329
Power failures 1329
Administering Personalized Ringing 1330
Prerequisites for administering Personalized Ringing 1330
Screens for administering Personalized Ringing 1330
Assigning Personalized Ringing to a user telephone 1330
Interactions for Personalized Ringing 1332

PIN Checking for Private Calls 1333
Detailed description 1333
Three examples of Feature Access Codes 1333
PIN Codes 1334
Feature Access Code screen 1337
System parameters screen 1338
PIN Checking for Private Calls? 1339
Field description 1339
Feature interactions 1339
Call Detail Recording 1339

Port Network Recovery from Control Network Outages 1341
Detailed description 1341
Improved Port Network Recovery from Control Network Outages 1341
Configuration impacts on availability 1343
Survivability 1343

Posted Messages 1345
Detailed description of Posted Messages 1345
Language options 1345
Messages 1346
Fixed messages 1346
Custom messages 1347
QSIG support 1347
Administering Posted Messages 1348
Prerequisites for administering Posted Messages 1348
Screens for administering Posted Messages 1349
Defining a Feature Access Code 1350
Requiring a security code 1351
Setting up a security code for the telephone of a user 1352
Activating the Posted Messages security code 1352
Activating QSIG to send custom messages 1353
Translating Posted Messages 1354
Translating fixed messages to a user-defined language 1354
Creating custom messages 1355
Translating telephone feature buttons and labels 1357
Translating the Posted Messages feature display to a user-defined language 1358
Translating the Posted Messages softkey button label to a user-defined language 1358
Translating the Posted Messages button label to a

user-defined language 1359
End-user procedures for Posted Messages 1360
Activating the Posted Messages feature 1361
Using a Feature Access Code. 1361
Examples 1362
Using the Posted Messages feature button 1362
Deactivating the Posted Messages feature 1363
Using a Feature Access Code. 1363
Examples 1363
Using the Posted Messages feature button 1364
Considerations for Posted Messages 1364
Interactions for Posted Messages 1365

Priority Calling 1369
Detailed description of Priority Calling 1369
Administering Priority Calling 1370
Prerequisites for administering Priority Calling 1370
Screens for administering Priority Calling 1372
Assigning a priority feature button to an attendant console 1373
Assigning a priority feature button to a telephone 1374
End-user procedures for Priority Calling 1375
Considerations for Priority Calling 1375
Interactions for Priority Calling 1375

Privacy 1377
Detailed description of Privacy 1377
Data Privacy 1377
Data Restriction 1377
Privacy - Automatic Exclusion 1378
Privacy - Manual Exclusion 1378
Administering Privacy 1378
Prerequisites for administering Privacy 1378
Screens for administering Privacy 1379
Administering Privacy for a user 1379
Activating Data Restriction for a trunk group 1382
End-user procedures for Privacy 1383
Considerations for Privacy 1383
Interactions for Privacy 1383

Public Network Call Priority 1385
Detailed description of Public Network Call Priority 1385
China 1385
Forced disconnect 1385
Mode-of-release control 1385
Russia 1387
Intrusion 1387
Re-ring 1387
Spain 1387
Call retention 1387
Re-ring 1387
Administering Public Network Call Priority 1387
Screens for administering Public Network Call Priority 1388
Screens for China 1388
Screens for Russia. 1388
Screens for Spain 1389
Interactions for Public Network Call Priority 1389
China 1389
Forced disconnect 1389
Mode-of-release control 1390
Re-ring 1390
Russia 1391

Record on Messaging 1393
Detailed description of Record on Messaging 1393
Feature button 1393
Language options 1394
Periodic alerting tone 1394
Ready indication tone 1394
Recording delay timer 1395
Administering Record on Messaging 1395
Prerequisites for administering Record on Messaging 1395
Screens for administering Record on Messaging 1396
Assigning Record on Messaging Parameters 1396
Translating telephone feature buttons and labels 1398
Translating the Record on Messaging text that appears on a telephone display to a user-defined language 1398
Translating the Record on Messaging button label to a user-defined language 1399
Assigning the feature button to a telephone 1400
Changing the characteristics of the zip tone 1401

End-user procedures for Record on Messaging 1404
Recording a conversation 1404
Considerations for Record on Messaging 1405
Interactions for Record on Messaging 1406
Troubleshooting Record on Messaging 1408

Recorded Telephone Dictation Access 1411
Detailed description of Recorded Telephone Dictation Access 1411
Administering Recorded Telephone Dictation Access 1411
Screens for administering Recorded Telephone Dictation Access 1412
Assigning manual signaling button to a multiple-call appearance telephone user 1412
Interactions for Recorded Telephone Dictation Access 1413

Remote Access 1415
Detailed description of Remote Access 1415
Night Service 1416
Security 1416
Status remote-access 1416
Barrier codes 1417
Authorization codes 1418
Alternate Facility Restriction Levels 1418
Class of Restriction 1418
Logoff Notification 1418
Administering Remote Access 1419
Prerequisites for administering Remote Access 1419
Screens for administering Remote Access 1419
Administering the Remote Access screen 1420
Enabling Remote Access 1420
Disabling Remote Access 1423
Assigning authorization codes 1423
Prerequisites 1423
Administering Remote Access for Night Service 1426
End-user procedures for Remote Access 1427
Reports for Remote Access 1427
Considerations for Remote Access 1427
Interactions for Remote Access 1428

Restriction - Controlled 1429
Detailed description of Restriction - Controlled 1429

Administering Restriction - Controlled 1430
Screens for administering Restriction - Controlled 1430
End-user procedures for Restriction - Controlled 1430
Activating Restriction - Controlled 1431
Reports for Restriction - Controlled 1431
Considerations for Restriction - Controlled 1431
Interactions for Restriction - Controlled 1432

Ringing - Abbreviated and Delayed 1433
Detailed description of Ringing - Abbreviated and Delayed 1433
Administering Ringing - Abbreviated and Delayed 1434
Prerequisites for administering Ringing - Abbreviated and Delayed 1434
Screens for administering Ringing - Abbreviated and Delayed 1435
Assigning ring control to a user 1436
Assigning an abbreviated ringing button to a user 1437
Reports for Ringing - Abbreviated and Delayed 1438
Considerations for Ringing - Abbreviated and Delayed 1439
Interactions for Ringing - Abbreviated and Delayed 1439

Security Violation Notification 1441
Detailed description of Security Violation Notification 1441
Security violation thresholds and notification 1442
Sequence of events 1442
Reporting 1442
SVN - halt buttons 1443
SVN Referral Call with Announcement 1443
Dealing with Security Violations 1443
Disabling a login ID 1444
Enabling a login ID 1444
Enabling remote access 1444
Disabling remote access 1444
Administering Security Violation Notification 1444
Prerequisites for administering Security Violation Notification 1445
Screens for administering Security Violation Notification 1445
Setting up Security Violation Notification 1445
Reports for Security Violation Notification 1450
Considerations for Security Violation Notification 1450
Interactions for Security Violation Notification 1450

Separation of Bearer and Signaling 1453
Detailed description of Separation of Bearer and Signaling 1453
Typical Call Connections 1455
Typical Call Setup 1458
Tandem SBS calls 1460
Tandem SBS bearer call 1460
Tandem SBS signaling call 1461
Interworked SBS calls 1461
Administering Separation of Bearer and Signaling 1461
Prerequisites for administering Separation of Bearer and Signaling 1462
Screens for administering Separation of Bearer and Signaling 1463
Administering Local Country Code and International Access Code 1464
Administering SBS trunks and trunk groups 1465
Creating the SBS trunk group 1466
Creating a signaling group 1466
Adding trunk group members to SBS trunk group 1468
Administering routing for SBS 1468
Administering SBS extensions 1470
Administering SBS extensions 1471
Defining the dial plan 1471
Mapping SBS Extensions to complete numbers 1472
Verifying system capacities 1474
Considerations for Separation of Bearer and Signaling 1476
Interactions for Separation of Bearer and Signaling 1478
Overview of SBS interactions 1478
Understanding potential interactions 1479
General system features and SBS 1480
Attendant interactions with SBS 1481
Attendant features that do not work with SBS 1481
Attendant features that work with SBS 1481
Adjunct Switch Applications Interface interactions with SBS 1482
CM Messaging and Octel voice mail adjuncts interactions with SBS 1482
Call Center interactions with SBS 1483
Automatic Call Distribution interactions with SBS 1483
Best Service Routing interactions with SBS 1484
Vectors interactions with SBS 1484
Networking-related interactions with SBS 1484
Networking features or capabilities that do not work with SBS 1484
Networking features or capabilities that work with SBS 1486
Network interface interactions 1489

Service Observing 1491
Detailed description of Service Observing 1491
Listen and talk modes 1492
Service Observing with Multiple Observers 1492
Telephone displays 1493
Trunk calls 1493
Warning and conference tones 1493
Administering Service Observing 1493
Screens for administering Service Observing 1494
End-user procedures for Service Observing 1495
Reports for Service Observing 1495
Considerations for Service Observing 1495
Interactions for Service Observing 1496

Station Hunting 1499
Detailed description of Station Hunting 1499
Station Hunting and Call Coverage 1500
Removing a station from a Station Hunting chain 1500
Duplicating a station in a Station Hunt chain 1501
Administering Station Hunting 1501
Prerequisites for administering Station Hunting 1501
Screens for administering Station Hunting 1502
Assigning station hunting after coverage 1502
Assigning a hunt-to station to an extension 1503
Administering Station Hunting before Coverage 1504
Reports for Station Hunting 1505
Interactions for Station Hunting 1506

Station Lock 1511
Detailed description of Station Lock 1511
Station Lock by time of day 1512
Screens for administering Station Lock 1513
End-user procedures for Station Lock 1513
Activating or deactivating Station Lock from a remote telephone 1514
Interactions for Station Lock 1514
Hot Desking Enhancement 1514
Station Lock 1515
Telephones 1516

Station Security Code 1517
Detailed description of Station Security Code 1517
Administering Station Security Code 1517
Screens for administering Station Security Code 1518
Creating a Station Security Code 1518
Interactions for Station Security Code 1519
Station Security Code (Display Guidance) 1520
End-user administration 1520
Exception Handling 1521

Supporting TTY Callers 1523
Detailed description of Supporting TTY Callers 1523
Setting up announcements for TTY callers 1524
Setting up hunt groups for TTY callers 1525
Handling TTY calls with vectors 1525
Administering Supporting TTY Callers 1526
Screens for administering Supporting TTY Callers 1526
Reports for Supporting TTY Callers 1526

Team Button 1527
Detailed description of Team Button 1527
Audible Ringing and Call States for Team Button 1529
Administering Team Button 1530
Configuring the Team Button 1530
Viewing the status of Team Button usage 1531
Viewing system capacity for Team Button 1532
Administering audible ringing 1533
Administering Priority Ring for speed dialing 1534
Administering display of station name 1534
Administering Call Pickup by going off hook 1535
Team Button Override Send All Calls/Call Forward 1535
No Overriding of SAC/CFWD 1537
Unconditional Overriding of SAC/CFWD 1537
Overriding of SAC/CFWD by Asking 1538

Telephone Display 1539
Detailed description of Telephone Display 1539
Button display modes 1540
Enhancements for Communication Manager 4.0 1541
Integrated Directory: 1541

Integrated Directory Data Base: 1542
INTEGRATED DIRECTORY Mode Button: 1542
Call-related information display 1544
Message retrieval 1547
Feature information displays 1547
Unicode "Native Name" support 1548
Enhanced telephone display 1548
Mapping enhanced display characters 1566
US English to Russian characters 1566
US English to Japanese characters 1567
US English to European characters 1569
US English to Ukrainian characters 1571
Administering Telephone Display 1571
Screens for administering Telephone Display 1572
Reports for Telephone Display 1572
Considerations for Telephone Display 1572
Interactions for Telephone Display 1573
Temporary Bridged Appearance 1575
Detailed description of Temporary Bridged Appearance 1575
Administering Temporary Bridged Appearance 1575
Screens for administering Temporary Bridged Appearance 1576
Considerations for Temporary Bridged Appearance 1576
Interactions for Temporary Bridged Appearance 1577
Tenant Partitioning 1579
Detailed description of Tenant Partitioning 1579
Partitioning tenants 1580
Access control 1581
Attendant services 1581
Network route selection 1582
Tenant Partitioning examples 1582
Multiple Music-on-Hold 1583
Administering Tenant Partitioning 1584
Prerequisites for administering Tenant Partitioning 1585
Screens for administering Tenant Partitioning 1585
Defining a tenant partition 1586
Assigning a tenant partition number to an access telephone 1588
Assigning a tenant partition number to an agent login ID 1589
Assigning a tenant partition number to an announcement 1590

Assigning a tenant partition number to an attendant . . . 1591
Assigning a tenant partition number to a data module . . . 1592
Assigning a tenant partition number to a hunt group . . . 1593
Assigning a tenant partition number to a loudspeaker paging zone . . . 1594
Assigning a tenant partition number to the remote access extension . . . 1595
Assigning a tenant partition number to a user extension . . . 1596
Assigning a tenant partition number to a terminating extension group . . . 1597
Assigning a tenant partition number to a trunk group . . . 1598
Assigning a tenant partition number to a vector directory number . . . 1598
Assigning the sources of music for the tenant partitions . . . 1599
Reports for Tenant Partitioning . . . 1601
Considerations for Tenant Partitioning . . . 1601
Interactions for Tenant Partitioning . . . 1601

Terminal Translation Initialization . . . 1607
Detailed description of Terminal Translation Initialization . . . 1607
Attendant consoles . . . 1607
Data modules . . . 1608
Voice and data telephones . . . 1608
ISDN-BRI telephones . . . 1608
Analog queue warning ports and external alert ports . . . 1609
Security . . . 1610
Erase user data from DCP telephones . . . 1610
Administering Terminal Translation Initialization . . . 1611
Screens for administering Terminal Translation Initialization . . . 1611
Interactions for Terminal Translation Initialization . . . 1612

Terminating Extension Group . . . 1615
Detailed description of Terminating Extension Group . . . 1615
Administering Terminating Extension Group . . . 1615
Screens for administering Terminating Extension Group . . . 1616
Considerations for Terminating Extension Group . . . 1616
Interactions for Terminating Extension Group . . . 1616

Transfer . . . 1619
Detailed description of Transfer . . . 1619
Pull Transfer . . . 1619
Abort Transfer . . . 1620
Transfer Recall . . . 1620
Transfer Upon Hangup . . . 1620

Trunk-to-Trunk Transfer 1620
Outgoing Trunk to Outgoing Trunk Transfer 1621
Emergency Transfer 1621
Name Display on Unsupervised Transfer 1622
Administering Transfer 1622
Screens for administering Transfer 1623
Considerations for Transfer 1623
Interactions for Transfer 1625

Trunk Flash 1629
Detailed description of Trunk Flash 1629
Administering Trunk Flash 1630
Screens for administering Trunk Flash 1630
End-user procedures for Trunk Flash 1630
Considerations for Trunk Flash 1631

Uniform Dial Plan 1633
Detailed description of Uniform Dial Plan 1633
Uniform Dial Plan example 1635
Administering Uniform Dial Plan 1638
Prerequisites for administering Uniform Dial Plan 1639
Screens for administering Uniform Dial Plan 1640
Administering the Uniform Dial Plan table 1641
Administering the Node Number Routing Table 1643
Administering the AAR Digit Conversion Table 1644
Administering the ARS Digit Conversion Table 1645
Administering the AAR Digit Analysis Table 1647
Administering the ARS Digit Analysis Table 1650
Administering the extension number portability numbering plan 1653
Reports for Uniform Dial Plan 1654
Considerations for Uniform Dial Plan 1654
Interactions for Uniform Dial Plan 1655

Visually Impaired Attendant Service 1657
Detailed description of Visually Impaired Attendant Service 1657
Administering Visually Impaired Attendant Service 1658
Prerequisites for administering Visually Impaired Attendant Service 1658
Screens for administering Visually Impaired Attendant Service 1658
Interactions for Visually Impaired Attendant Service 1659

Voice Message Retrieval 1661
Detailed description of Voice Message Retrieval 1661
Administering Voice Message Retrieval 1661
Screens for administering Voice Message Retrieval 1662
Reports for Voice Message Retrieval 1662
Considerations for Voice Message Retrieval 1662
Interactions for Voice Message Retrieval 1663

Whisper Paging 1665
Detailed description of Whisper Paging 1665
Call redirection overrides 1665
Group answering environments 1666
Network restrictions 1666
Speakerphones 1666
Administering Whisper Paging 1666
Prerequisites for administering Whisper Paging 1666
Screens for administering Whisper Paging 1667
Making a whisper page 1667
Allowing users to answer whisper pages quickly 1667
Allowing users to block whisper pages 1667
End-user procedures for Whisper Paging 1668
Reports for Whisper Paging 1668
Considerations for Whisper Paging 1668
Interactions for Whisper Paging 1669

Wideband Switching 1673
Detailed description of Wideband Switching 1673
Channel allocation 1674
Typical uses 1674
Endpoint applications with signaling 1675
ISDN-PRI terminal adapters 1675
Line-side T1 or E1 ISDN-PRI facilities 1676
PRI endpoints 1676
Universal digital signal level 1 board 1676
Nonsignaling endpoint applications 1677
Data service unit/channel service unit 1677
Line-side T1 or E1 facility 1677
Wideband access endpoint 1677
Guidelines and examples 1678
High-speed video conferencing 1678

Data backup connection 1678
Scheduled batch processing 1678
Primary data connectivity 1679
Networking 1679
ISDN-PRI trunk groups and channel allocation 1679
Facility lists 1679
Direction of trunk hunting within facilities 1680
H11 channels 1680
H12 channels 1681
H0 channels 1682
N x DS0 channels 1682
Glare prevention and resolution 1683
Blocking prevention 1685
Administering Wideband Switching 1685
Screens for administering Wideband Switching 1686
Considerations for Wideband Switching 1686
Interactions for Wideband Switching 1686

World Class Routing 1689
Detailed description of World Class Routing 1689
Overview of automatic routing 1690
Understanding ARS analysis 1692
Examples of digit conversion 1692
ARS dialing without a FAC 1693
Extensions 1695
AAR and ARS partitioning 1695
Administering World Class Routing 1696
Screens for administering World Class Routing 1697
Using COR and FRL to manage calling privileges 1698
Assigning a FAC for ARS 1699
Setting up a location ARS FAC 1701
Prerequisites 1701
Displaying ARS analysis information 1702
Administering the route pattern 1704
Defining call types 1715
Defining operator-assisted calls 1715
Defining interexchange carrier calls 1716
Using restricted area codes and prefixes 1716
Using wildcards 1718
Defining local information calls 1719

Modifying call routing 1720
Adding a new area code 1720
Adding a new prefix 1722
Using ARS to restrict outgoing calls 1722
Defining ARS partitions 1724
Prerequisites 1724
Setting up partition groups 1724
Assigning a telephone to a partition group 1726
Setting up Time of Day Routing 1729
Prerequisites 1729
Reports for World Class Routing 1732
Considerations for World Class Routing 1732
Interactions for World Class Routing 1732
Index 1735

About this document

Overview

The *Avaya Aura™ Communication Manager Feature Description and Implementation* document describes the features that can be administered with the May 2009 release of Avaya Aura™ Communication Manager.

You might also want to see the *What's New in Avaya Aura™ Communication Manager, SIP Enablement Services, Avaya Servers and Media Gateways for Release 5.2* document to see what is new in a particular release.

Intended audience

This document is a useful reference for a large audience. However, this document is intended for the following audience:

- Communication Manager administrators and technical managers
- Users who want information about how to administer or use specific features
- Avaya personnel who plan, design, configure, sell, or support Avaya's converged solutions

How to use this book

Use this document both as a guide to administer and troubleshoot features, and as a reference document. If you are interested in information about a particular feature, use the index or table of contents to locate the page number where the document describes the information. To help you more easily locate a feature, this document presents the features in alphabetical order.

Organization

This document uses a framework to describe each feature. This framework includes the following sections:

- Summary
- Detailed description
- Administering
- End-user procedures
- Reports
- Considerations
- Interactions
- Troubleshooting

Summary

The Summary section provides a high-level description of the feature. For simple features, the Summary might be only one sentence. For more complex features, the Summary might be one or two paragraphs.

Detailed description

The Detailed Description section provides detailed information about the feature. Some features have more than one function. This document refers to these functions as capabilities. The Detailed Description lists these capabilities and provides a brief description of each of the capabilities.

Although the Detailed Description section provides a complete description of the feature, the section does not include procedural or administration information. The procedural and administration information is in the Administering section.

Administering

The Administering section provides the information that you need to administer and implement the feature. This section includes the following information:

Any prerequisites that you must complete before you administer the feature

- The screens that you use to administer the feature
- Complete administration procedures for the feature

End-user procedures

The End-user procedures section describes any procedures that might exist for a user to activate, deactivate, or otherwise modify administration of the feature, or a capability of the feature.

If a feature does not have end-user procedures, the feature description does not contain this section.

Reports

The Reports section lists the reports that provide information about the feature. If a feature does not have any reports, the feature description does not contain this section.

Considerations

The Considerations section provides any useful miscellaneous information about the operation of the feature.

If a feature does not have considerations, the feature description does not contain this section.

Interactions

The Interactions section describes how the feature interacts with other features. For example, certain features must always be used in conjunction with other features. Some features cannot coexist with other features. In some cases, the normal operation of a certain feature modifies the normal operation of another feature. Some features also enhance each other, and when combined, provide improved service to the user. The features are listed in alphabetical order.

Troubleshooting

The Troubleshooting section provides a table that lists the following information:

- Known or common problems that users might experience with the operation of the feature
- Possible causes of the problems
- Actions that an administrator can take to solve the problems

If a feature does not have troubleshooting tips, the feature description does not contain this section.

Related resources

The following documents provide additional information:

Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504

Administering Avaya Aura™ Communication Manager, 03-300509

ATM Installation, Upgrades, and Administration using Avaya Communication Manager, 555-233-124

Avaya Application Solutions: IP Telephony Deployment Guide, 555-245-600

Avaya Communication Manager Basic Administration Quick Reference, 03-300363

Avaya Communication Manager Advanced Administration Quick Reference, 03-300364

Avaya Communication Manager Basic Diagnostics Quick Reference, 03-300365

Avaya Remote Feature Activation (RFA) Users Guide, 03-300149

Avaya Enterprise Survivable Servers (ESS) Users Guide, 03-300428

Avaya Toll Fraud and Security Handbook, 555-025-600

Converged Communications Server Installation and Administration, 555-245-705

DEFINITY® Communications Systems Generic 2.2 and Generic 3 Version 2 DS1/CEPT1/ISDN PRI Reference, 555-025-107

DEFINITY® Enterprise Communications Server Release 1.1 Getting Started with the Avaya R300 Remote Office Communicator, 555-233-769

Avaya Aura™ Communication Manager Hardware Description and Reference, 555-245-207

What's New in Avaya Aura™ Communication Manager, SIP Enablement Services, Avaya Servers and Media Gateways for Release 5.2, 03-300681

Installation, Upgrades and Additions for Avaya CMC1 Media Gateways, 555-233-118

Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300430

Maintenance for Avaya DEFINITY® Server R, 555-233-117

Maintenance for Avaya MultiVantage and DEFINITY Server CSI, 555-233-119

Maintenance for Avaya DEFINITY® Server SI, 555-233-123

Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431

Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300432

Avaya Aura™ Communication Manager Overview, 555-233-767

Avaya Aura™ Communication Manager System Capacities Table, 03-300511

Upgrades and Additions for Avaya DEFINITY® Server R, 555-233-115

Avaya Aura™ Communication Manager Reports, 555-233-505

For information on Fax, Modem, Clear Channel over IP, see *Administering Network Connectivity on Avaya Aura™ Communication Manager,* 555-233-504

For information on IGAR, *see Administering Network Connectivity on Avaya Aura™ Communication Manager,* 555-233-504

For information on H.248 Gateways, *see Administering Network Connectivity on Avaya Aura™ Communication Manager,* 555-233-504

For documents not listed here, go to http://www.avaya.com. Select **Support** and then **Product Documentation**.

Conventions

This section includes the conventions and terms to make you familiar with Communication Manager.

- A "screen" is the display of fields and prompts that appear on a terminal monitor.
- We use the term "telephone" in this book. Other Avaya books might refer to telephones as voice terminals, stations, or endpoints.
- Keys and buttons are printed in a bold font: **Key**.
- Titles of screens are printed in an initial capital letter: Screen Name.
- Names of fields are printed in a bold font: **Field Name**.
- Text (other than commands) that you need to type into a field are printed in a bold font: **text**.
- Commands are printed in a bold constant width font: **`command`**.
- Variables are printed in a bold constant width italic font: ***`variable`***.
- We show complete commands in this book, but you can always use an abbreviated version of the command. For example, instead of typing **`list configuration station`**, you can type **`list config sta`**.
- If you need help constructing a command or completing a field, remember to use **Help**.
  - When you press **Help** at any point on the command line, the system displays a list of available commands.
  - When you press **Help** with your cursor in a field on a screen, the system displays a list of valid entries for that field.
- Messages that the system displays are printed in a constant width font: **system message**.
- To move to a certain field on a screen, you can use the **Tab** key, directional arrows, or the **Enter** key on your keyboard.
- If you use terminal emulation software, you need to determine what keys correspond to **Enter**, **Return**, **Cancel**, **Help**, and **Next Page** keys.
- We show commands and screens from the newest release of Communication Manager and see the most current books. Substitute the appropriate commands for your system and see the manuals you have available.
- The status line or message line can be found near the bottom of your monitor. This is where the system displays messages for you. Check the message line to see how the system responds to your input. Write down the message if you need to call the helpline.

- When a procedure requires you to press **Enter** to save your changes, the screen clears. The cursor returns to the command prompt. The message line shows "**command successfully completed**" to indicate that the system accepted your changes.

Admonishments

Admonishments that might appear in this book have the following meanings:

Note:
A note calls attention to neutral information or positive information that supplements the main text. A note also calls attention to valuable information that is independent of the main text.

Important:
An important note calls attention to situations that can cause serious inconvenience.

Tip:
A tip calls attention to information that helps you apply the techniques and the procedures that the text describes. A tip can include keyboard shortcuts, or alternative methods that might not be obvious.

CAUTION:
A caution statement calls attention to situations that can result in harm to software, loss of data, or an interruption of service.

WARNING:
A warning statement calls attention to situations that can result in harm to hardware or equipment.

DANGER:
A danger statement calls attention to situations that can result in physical injury to yourself or to other people.

SECURITY ALERT:
A security alert calls attention to situations that can increase the potential for toll fraud or other unauthorized use of your telecommunications system.

ELECTROSTATIC ALERT:
An electrostatic alert calls attention to situations that can result in damage to electronic components from electrostatic discharge (ESD).

Trademarks

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

How to obtain Avaya books on the Web

If you have internet access, you can view and download the latest version of the *Avaya Aura™ Communication Manager Feature Description and Implementation*. To view this book, you must have a copy of Adobe Acrobat or Acrobat Reader.

Note:
If you do not have Acrobat Reader, you can get a free copy at http://www.adobe.com/reader.

To get the latest version of this book:

1. Go to the Avaya Web site at http://www.avaya.com/.
2. In the **Go To:** column, click the **Documentation** link.

3. In the **Search Avaya** text box on the Technical Database/Product Documentation screen, type **555-245-205** (the document number). Click **Go**.
4. In the list that appears, select the version of the document that you want. Click the title of the book.

How to comment on this book

Avaya always welcomes your feedback. Contact us through:

- e-mail: document@avaya.com
- fax: 1-303-538-1741
- Your Avaya representative

Mention this document name and number, *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Your comments are of great value, and help us to improve our documentation.

How to get help

If you need additional help, go to the Avaya support Web site at http://www.avaya.com/support/.

If you are:

- Within the United States, click the **Escalation Contacts** link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the **Escalation Contacts** link. Then click the **International Services** link, which includes telephone numbers for the international Centers of Excellence.

You can also access the following services in the USA. You might need to purchase an extended service agreement to use some of these services. Contact your Avaya representative for more information.

Avaya Aura™ Communication Manager Helpline (for help with feature administration and system applications)	1 800 225 7585
Avaya National Customer Care Center Support Line (for help with maintenance and repair)	1 800 242 2121

Avaya Toll Fraud Intervention	1 800 643 2353
Avaya Corporate Security	1 877 993 8442

AAA Services

Use the Authentication, Authorization and Accounting (AAA) Services feature to allow customers to store and maintain administrator account (login) information on a central server. Login authentication and access authorization is administered on the central server.

Note:
For more information, see the *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

Detailed description of AAA Services

This section provides a detailed description of the AAA Services feature.

The AAA Services interactions with Avaya Aura™ Communication Manager use the Pluggable Authentication Module (PAM and Linux) and Name-Switch Service (NSS) within Linux, which are provided on Linux-based Communication Manager servers.

External AAA support is a Linux feature that is separate from Communication Manager, is not controlled by a license file, and is freely available to the customer. Customers can use the same authentication for Communication Manager as is used by other servers on their network.

PAM is a Linux system capability that allows great flexibility in how administrator accounts are processed. For example, simple Linux configuration file changes can change login processing from being local-host based to being LDAP based.

Name-Switch Service (NSS) is a Linux facility that allows user authorization information to be obtained from either local files on the Communication Manager server or from an LDAP server on the network.

This section provides information on the following topics:

- Supported security configurations
- Configuring external AAA servers
- User authentication
- User profiles
- User profiles for Communication Manager server Web page access
- User accounts
- External accounts
- Local host accounts

- Linux groups
- Upgrades from a release that does not support profiles
- Upgrades from a release that supports profiles
- Backup and restore
- Backup and file sync for web access profiles

Supported security configurations

The following security configurations are supported on Communication Manager:

- Local host accounts
  - All authentication, authorization, and accounting information is maintained on the same server to which the user is attempting access. For Communication Manager, this is the Communication Manager server.
  - Use the files /etc/passwd, /etc/shadow, and /etc/group among others.
- LDAP based accounts
  - Require an LDAP server compatible with the LDAP client from www.openldap.org.
  - LDAP client is distributed by RHEL4, and is originally from www.padl.com
  - The following LDAP servers have been tested with Communication Manager:
    - The server from www.openldap.org
    - Microsoft Active Directory
    - SunOne Directory Service
- Radius based accounts
  - Require a radius server compatible with the radius client from www.freeradius.org.
- RSA SecurID based accounts
  - Require a parallel local host account or an LDAP account for authorization information.
  - Can be used directly from the Communication Manager server, when a license is purchased from the vendor and software is installed on the Communication Manager server.
  - Can be used behind a radius server.
- Secure Computing SafeWord accounts
  - Require a parallel host account or an LDAP account for authorization information.
  - Can be used directly from the Communication Manager server, when a license is purchased from the vendor and software is installed on the Communication Manager server.

– Can be used behind a radius server.

Configuring external AAA servers

The Communication Manager default configuration does not contain an entry for an external AAA server. All accounts are authenticated on the local host.

To activate use of an external AAA server, the **/etc/pam.d/mv-auth** file must be edited to incorporate the appropriate line for the server being used, and the additional configuration files edited corresponding to the needs of the AAA service. Activation of an external AAA service will be accomplished by the customer and not by Avaya Services. The customer provides and owns the AAA server on their network and they alone have the data that is necessary to set up the client on the Communication Manager server.

For information regarding configuring AAA Servers, see:

- *Communication Manager Administrator Logins* White Paper on http://support.avaya.com/elmodocs2/white_papers/CM_Administrator_Logins.pdf
- http://www.kernel.org/pub/linux/libs/pam

  This Web site contains PAM documentation such as the System Administrators' Guide.

Also see documentation for:

- individual PAM modules
- applications running on external servers

User authentication

Communication Manager login authentication takes place in Linux PAM modules, and the system configuration determines how user authentication takes place. For example, if the user's account is ASG protected, the Linux PAM module will issue the appropriate challenge. If RADIUS is used, the Linux PAM module will contact the RADIUS server to validate the user. If a token device is used such as *SecurID* from RSA Security, the user may be prompted for a pin plus the token's displayed value.

When logins are configured through Communication Manager/Radius:

- Services logins are authenticated at Communication Manager
- Customer logins may be authenticated at Radius, then Communication Manager

When logins are configured at OpenLDAP:

- Services logins are authenticated at Communication Manager
- Customer logins may be authenticated at LDAP

User profiles

Profiles govern access to the Communication Manager SAT and to the Communication Manager server's web interface. A profile consists of a numeric identifier and that profile's access permissions. Administration for SAT profiles and web profiles are separate processes.

- Communication Manager SAT profiles define access to Communication Manager SAT screens. SAT profile data is maintained within Communication Manager.
- Communication Manager web profiles define access to Web pages in the web interface. Web profile data is maintained in a Linux file.
- SAT profile objects (SAT screens) and web profile objects (Web pages) have no objects in common.
- A profile is identified by a number 0-69, which corresponds to a Linux group. Both Communication Manager and the web interface dedicate fixed permissions to profiles 0-19, which may not be deleted or modified.
- When a profile is created, the profile is assigned to a Linux group whose number is CM_PROFILE_BASE or greater. CM_PROFILE_BASE defaults to 10,000 for both Communication Manager and the Web. The value can be changed through the Web pages.
- Profile numbers are based on the login's Linux group number, minus the CM_PROFILE_BASE. For example, user **dadmin** belongs to Linux group 10,002. The profile number for **dadmin** is 2 (10002 minus 10000).
- When a Linux group is assigned to a login, the login is assigned the profile associated with that Linux group. For example, when Linux group 10,002 is assigned to the **dadmin** login, **dadmin** is automatically assigned user profile 2.
- Communication Manager maintains up to 70 profiles.
- A login may be assigned exactly zero or one user profile. A login may not be assigned to more than one user profile. If a login is not assigned group membership in the range 10,000 to 10,069, that login will have no access to the SAT or the server Web pages. Multiple logins may be assigned to the same profile. The starting value of 10,000 may be changed through the Web Access Mask page.

Customers can create and modify profiles to allow access to Communication Manager functions according to job functions. Examples of such profiles are:

- Security Auditor profile, with read-only access to logs and audit files.
- Security profile, with read-write access to create other administrator logins, create and modify profiles.
- Telephony Application Administrator profile, with read-write access to application configuration, such as trunks.
- Backup administrator profile, with the ability to perform only backups.

- Telephone Provisioning profile, with ability to add/change/delete a certain range of telephone extensions.
- ACD Administrator profile, with the ability to modify call center vectors.
- Checker profiles, with read-only access, able to only view certain changes.

User profiles for SAT form access

On Communication Manager, the profile specifies which SAT screens may be accessed by the user assigned the profile. The profile further defines the type of access to each screen. A user with appropriate permissions can change the SAT profile permissions by editing the User Profile (**`change user-profile`**) form.

The SAT User Profile form specifies access for every Communication Manager SAT form (object). The list of Communication Manager objects is maintained in Communication Manager. The SAT profile form lists all the possible SAT screens in the software regardless of whether the associated feature is enabled, disabled, licensed or not licensed.

On the User Profile form, SAT screens are grouped in categories. SAT screen categories:

- Exist only for the organization of the User Profile form
- Lets the user quickly set permissions for a group or groups of screens for a profile
- Provides a summary of the groups of screens that can be accessed by the profile

SAT profiles

SAT profiles control access to SAT screens based on the command object (SAT screen).

Seventy user-profiles exist in Communication Manager, numbered 0-69, which correspond to a Linux group.

- Profiles 0-19 are dedicated. Profiles 0-17 cannot be edited, copied, viewed, nor removed. Profiles 18 and 19 may be assigned to any customer login.
- Profile numbers 20-69 are available for customer use for customized profiles.

For co-resident applications such as CM Messaging (formerly Intuity Audix IA770) or Octel voice mail adjuncts, a standard profile to support TSC may need to be created for TSC access to Communication Manager.

Table 1: Communication Manager User Profiles

Profile	Profile name	Permissions/access	Notes
0	services super-user	equivalent to the former SAT *init* login. Has all permissions possible with no restrictions.	Cannot be edited, copied, viewed, or removed. Restricted Requires a second user authentication by Communication Manager.
1	services manager	equivalent to the former SAT *inads* login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
2	business partner	equivalent to the former SAT *dadmin* login	Cannot be edited, copied, viewed, or removed. Must be enabled in the license file. The dadmin login can create one login that has craft login permissions and a name other than craft. The second craft login uses Profile 3 and can login without a second challenge.
3	services	equivalent to the former SAT *craft* login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
4-15		Reserved for future use by Avaya.	Cannot be edited, copied, viewed, or removed.
16	call center manager	equivalent to the former SAT MIS login (@MIS) CMS/CCR access	Cannot be edited, copied, viewed, or removed. Assign CMS/CCR logins through the MIS application.
17	snmp	SNMP agent access	Cannot be edited, copied, viewed, or removed.
18	customer super-user	equivalent to the former SAT default *customer super-user* login	Cannot be edited or removed.

1 of 2

Table 1: Communication Manager User Profiles (continued)

Profile	Profile name	Permissions/access	Notes
19	customer non-super user	equivalent to the former SAT default *non-super-user customer* login	This profile is used during upgrades only. It has no SAT permissions. Cannot be edited or removed.
20-69		Available for customer modification	
			2 of 2

Extended profiles

Extended profiles provide additional access control for vector and station forms.

As an example of increased access control through extended profiles, you can use an extended profile to grant access to a specific set of vectors. For example, a user profile has read-only (**r-**) access to the vector form in the standard profile. The extended profile grants access to vector 3 only. The user is able to display vector 3 and is able to list vectors. A user with these restrictions can see (list) all vectors, but can read the detail parameters only for vector 3.

User profiles for Communication Manager server Web page access

On the Communication Manager web server interface, the **Web Access Mask** page specifies which Communication Manager server Web pages a user may access. The web profile is sometimes called the Web Access Mask. The web profile defines the type of access to each Web page. Only those Web pages permitted by the profile appear on the menu when the user assigned the profile accesses the web interface.

The **Web Access Mask** Web page specifies read or read/write access for every Web page.

Communication Manager Web pages allow web users access to specific selected functions that are normally restricted to the root login. Logins that are members of the **susers** Linux group may have full access to the Web pages. Logins that are members of the **users** Linux group may have only limited access to the Web pages.

The web profile is identified by a number 0-69, which corresponds to a Linux group.

- The web profile numbers 0-19 correspond to the fixed profiles 0-19 in Communication Manager. Profiles 0-3, 18 and 19 are built into Communication Manager and are not editable.
- Profiles 0-3 and 18 have access to all Web pages, as members of the Linux group **susers**.
- Profile 19 has access to a subset of Web pages as a member of the **users** Linux group.

- Profiles 4 -17 are reserved for future use.
- Profile numbers 20-69 are available for customer use for customized profiles.

Logins that are members of the **susers** Linux group and a member of the profile group prof18, corresponding to profile 18, have access to all the possible Web pages as illustrated by the menu example in Figure A in Figure 1: Profile 18 (susers) Communication Manager web profile menu on page 78

Logins that are members of the **users** Linux group and a member of the profile group prof19, corresponding to profile 19, are redirected to a subset of the Web pages as illustrated by the menu example in Figure B in Figure 2: Profile 19 (users) Communication Manager web profile menu on page 79.

When adding a user profile, Avaya recommends copying profile 18 for **susers** (customer super-user access) or profile 19 for **users** (customer non-super-user access) depending on the basic Communication Manager web access required, and reducing the permissions as required.

Figure 1: Profile 18 (susers) Communication Manager web profile menu

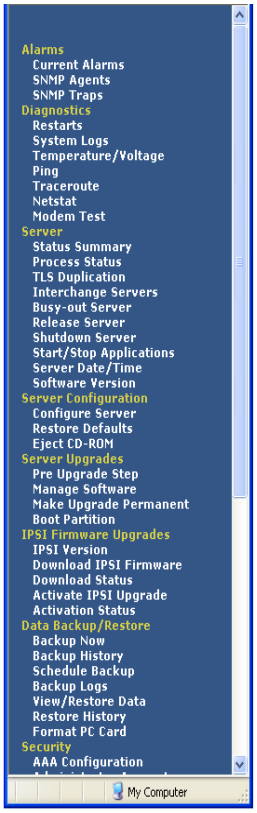


Figure 2: Profile 19 (users) Communication Manager web profile menu

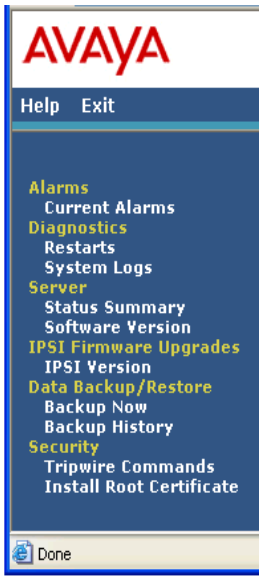
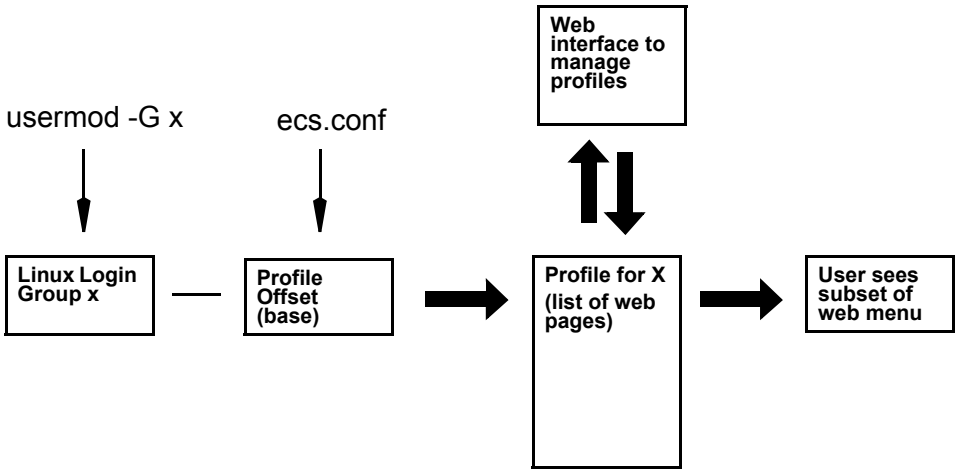


Figure 3: Web user profile overview on page 79 shows the process used to manage Communication Manager web profiles. The user's profile is identified by subtracting the Profile offset base (CM_PROFILE_BASE) from the user's Linux group number.

Figure 3: Web user profile overview



Profile access to restricted objects

Some Communication Manager objects (commands) are accessible only by profiles 0, 1, 2, 3 (logins **init**, **inads**, **dadmin** and **craft**). Profiles 18 and 19 (**customer super-user** and **non-superuser**) and customer created profiles 20-69 never have access to these commands.

Some objects allow different access for Avaya services logins and customer logins. For example, a services login might be able to execute a change or display for a certain object while customer logins can execute only a display for the same object.

The most restricted objects are accessible only by profiles 0, 1, and 2 (logins **init**, **inads**, and **dadmin**). These objects are listed in Table 2: Profile access to restricted objects on page 80.

Table 2: Profile access to restricted objects

Object	Profile 0 init	Profile 1 inads	Profile 2 dadmin
angel (0,1)	x	x	
cumaudits	X	X	X
enable save-translations	X	X	
enable craft2 disable craft2	X	X	X
fw-log	X	X	X
hardware-group	X	X	X
internal-data	X	X	X
MO	X	X	X
MO-all	X	X	X
no-lic-mode	X	X	X
options	X	X	X
peakaudits	X	X	X
software display software errors	X	X	X
tcm	X	X	

User accounts

Create user accounts (logins) to allow access to a subset of administration functionality intended for the job or role associated with the user.

An administrator account consists of a login which belongs to either Linux group **susers** or **users** and no profile group or exactly one profile group for permission to access the Communication Manager SAT and System Management Interface. There are other accounts that need to be in different groups, such as remote access accounts that need to be in the Linux group **remote**. User accounts can be created and stored locally on Communication Manager, or on an external central AAA server.

When Communication Manager software is first installed, only local host accounts are configured. The Linux PAM files on Communication Manager must be edited to incorporate support for any other type of account.

See the *Communication Manager Administrator Logins* White Paper on http://support.avaya.com/elmodocs2/white_papers/CM_Administrator_Logins.pdf for information on editing PAM files and AAA Server configuration.

External accounts

External accounts are accounts where authentication takes place outside of Communication Manager. Login and security information is stored in a central location such as a RADIUS server. Radius clients communicate with the AAA server to authenticate users, and to store accounting information.

At least one local host account should be present in all servers so that access is possible even if external AAA servers are not reachable.

Local host accounts

A local host account is an administrative account in which all information is maintained on the same server where the login occurs, or the data for such an account.

These accounts are authenticated by PAM authentication software that resides on Communication Manager. The PAM authenticates the user based on information in files that are also resident on the Communication Manager server, without interaction with other AAA services. All ASG authenticated accounts must be local host accounts.

Fixed profiles exist for logins **init**, **inads**, **craft**, **dadmin, customer superuser** and **customer non superuser**, as well as profiles for SNMP and CMS access.

Additional local user accounts can be created. A web interface and CLI commands (CMuser commands) exist for adding or removing additional local user accounts.

Local host accounts can be used at the same time as any of the external AAA services.

Administrative logins

Use administrative logins to administer the Communication Manager server through a shell, the SAT interface, or the System Management Interface.

The access provided to an administrative login is controlled by whether or not the login is assigned a shell and the User Profile assigned to the login. See User profiles for Communication Manager server Web page access on page 77. To assign a User Profile to an administrative login, assign an additional group to the login on the **Security** > **Administrator Accounts** of the Server Administration Interface.

Administrative logins cannot be used to establish a PPP session nor to acquire CDR records.

Avaya services logins

Profiles for Avaya services logins **init**, **inads**, and **craft** are programmed into Communication Manager.

Avaya services logins and profiles

Login	Profile
init	0
inads	1
craft	3

Services logins (**init**, **inads**, and **craft**) are ASG authenticated accounts and require two logins when used to access the Communication Manager SAT. PAM requires the first login, and Communication Manager software requires the second login. There is no prompt for the user name on the second challenge.

CDR logins

Use a **CDR** login to retrieve CDR records stored on the Communication Manager server. When creating a **CDR** login on the Communication Manager Security >Administrator Accounts of the Server Administration Interface, enter **CDR_User** as the login group and leave the additional groups field blank.

BusinessPartner login: dadmin

The user login **dadmin** corresponds with Profile 2, business partner. The **dadmin** login must be enabled in the license file to be used to access the Communication Manager SAT.

The **dadmin** login can create one login that has craft login permissions and a name other than craft. The second craft login uses Profile 3 and can login without a second challenge.

A personal identification number (PIN) is added to **dadmin** and (second craft login) **craft2** logins for an additional security for BusinessPartners logins and to reset a user password if an external authentication server is used. As an administrator, you must enter a PIN upon initial SAT access to the **dadmin** and the **craft2** logins. In subsequent accesses first, you must access SAT with **dadmin** or **craft2** logins to be in control of the PIN.

Remote logins: remote

Use a **remote** login to establish a PPP session with the Communication Manager server through its modem interface. When creating a **remote** login on the System Management Interface, specify a **remote** login Login ID (name), but you cannot specify group membership or select a shell. A **remote** login is created in the **remote** Linux group.

Remote logins cannot be used to access a shell, a SAT, CDR records, or the Communication Manager System Management Interface. **Remote** logins cannot be changed to an administrative or CDR login; instead, delete the remote login and create a new administrative or CDR login.

Linux groups

User authorization for administrator logins for Communication Manager servers is specified and controlled by assignment to Linux groups. Each login must be assigned to at least one primary Linux group **susers** or **users** plus one or no profile group, prof18-prof69. When a login is assigned to a Linux group, the user gains access based on the permissions for the group.

Assign logins to **susers** carefully. **Suser** logins have privileged access to the server including the ability to modify many critical system files, and the ability to add, remove and modify system logins.

For login access based on user profiles, create new Linux groups in the range 10,020 - 10,069. Avaya recommends the group name be in the form **prof-*nn*** where ***nn*** is the group number. For example, create **prof22** for the Linux group corresponding to access profile 22. **Prof22** is assigned the group number 10,022. With this naming convention, if a system's existing Linux groups require that the base value (10,000) be changed through the Web Access Mask page, that page will search for groups named in this manner and convert the group numbers to the new base. Groups not named in this manner will not be converted.

Table 3: Linux Groups and access permissions

Linux group name	Linux group number	Communication Manager login	Web access	SAT command access
users	100 (users)	--	Limited Menu	Limited Access
susers	555 (susers)	--	Full Menu	Full Access
remote	888 (remote)	--	PPP access to the Communication Manager platform Logins assigned to the remote group should not be members of any other group.	
voice	102		Access to the coresident voicemail product on the Communication Manager platform	
prof0 - prof69	10,000 - 10,069	Communication Manager profile 0 - 69	Web profile (access mask) 0-69, applied against limited or full Web page menu	--

Pre-release 4.0 Communication Manager software sets Linux groups as shown in Table 4: Existing Login Group Numbers on page 84. Communication Manager Release 4.0 and later application software does not depend on these fixed assignments, but the web interface requires the assignments.

Table 4: Existing Login Group Numbers*1 of 2*

Linux Login Group		Communication Manager Service Level	Communication Manager Login Type	Avaya Logins
Number	Name			
100	users	non-super-user	customer	--
102	voice			tsc
				1 of 2

Table 4: Existing Login Group Numbers *2 of 2*

Linux Login Group		Communication Manager Service Level	Communication Manager Login Type	Avaya Logins
Number	Name			
123	audix			--
555	susers	super-user	customer/services	init, inads, craft, dadmin
888	remote	remote	customer	rasaccess
				2 of 2

Upgrades from a release that does not support profiles

After an upgrade from a release that does not support profiles to a release that does support profiles, logins and their SAT and web access permissions are the same as before the upgrade.

During an upgrade, Linux user authentication information is updated by:

- Copying the /etc/passwd, /etc/shadow, and /etc/group files to a new partition
- Converting the /etc/opt/ecs/asgfile, and /etc/opt/ecs/lacfile files to a new format in the new partition.

Translations from a release before 4.0 are processed into release 4.x as follows:

- A **remote** login is created in the **remote** Linux group if one does not already exist.
- A customer non-super-user login without a change in permissions is associated with profile 19.
- A customer non-super-user login with a change in permissions is associated with the next available unused profile, and the profile is configured to match SAT forms from the prior release.

  A login is created in Linux with membership in the **users** group plus group PROF19 or the new profile number, as appropriate.
- A customer super-user login without a change in permissions is associated with profile 18.
- A customer super-user login with a change in permissions is associated with the next available unused profile, and the profile is configured to match SAT forms from the prior release.

  The login is created in Linux with membership in the **susers** group plus group PROF18 or the new profile number, as appropriate.

- A parallel web access profile is created for each new SAT profile created during the upgrade. The web profile configuration is copied from the web profile 18 for logins in the **susers** Linux group, and from profile 19 for logins in the **users** Linux group.

Upgrades from a release that supports profiles

SAT and web profile information is preserved on upgrades from a release that supports profiles. Each profile that exists in the prior release also exists in the new release.

For profiles 0-19, the new release provides permissions.

For profiles 20-69 that exist in the prior release, permissions after the upgrade are set as follows:

- SAT and web objects that appear in both releases retain their permissions.
- SAT and web objects that appear in the prior release but not in the new release do not appear in profiles in the new release.
- Access permissions for objects that do not appear in the prior release and appear in the new release are set to applicable default permission settings. In most cases, if the User Profile screen Page 1 category field is enabled (y), the object is set to:
  - **w-** for an object that supports add, change and remove actions
  - **r-** for an object that supports display and list actions
  - **--** for an object that does not have the applicable feature license activated

Third-party AAA Services software may need to be reinstalled after a Communication Manager server upgrade. See the *Communication Manager Administrator Logins* White Paper on http://support.avaya.com/elmodocs2/white_papers/CM_Administrator_Logins.pdf for more information.

Backup and restore

When restoring security information from a release that supports profiles, profile information is preserved from the backup.

When restoring security information from a release that does not support profiles, the backup program run by the backup/restore Web pages:

- restores the Avaya Authentication file
- restores the files /etc/passwd, /etc/shadow, /etc/group, which contain user account information for users in **users** and **susers** Linux groups
- adds the needed accounts to Linux as required, including default Communication Manager profiles.

- sets up default profiles and their administrator accounts provided by the new Communication Manager installation
- adds the needed accounts to Linux as required

Backup and file sync for web access profiles

A Communication Manager backup includes the web profile file(s) in the security data set. SAT profiles are backed up as part of Communication Manager translations. Web profiles are file synchronized only when manually requested from the Web Access Mask page.

File synchronization distributes the following files to all the servers in the configuration:

- /etc/passwd
- /etc/shadow
- /etc/group

When a login account or Linux group is created, it appears on all servers in the configuration after file synchronization. The user's home directory (/var/home/user-ID) is created as necessary. However, the content of the user's home directory is not file synchronized.

Initiate web access mask file synchronization from the Communication Manager Web page Security > Web Access Mask.

Administering AAA Services

The following steps are part of the administration process for AAA Services.

- Managing accounts using Communication Manager Web pages
- Managing profiles using the Communication Manager SAT
- Managing passwords and Access Security Gateway
- Administering Communication Manager web access profiles
- Administering user profiles for Communication Manager SAT access

Screens for administering AAA Services

Screen name	Purpose
Maintenance Web Page: Security > Administrator Accounts	Adding an administrator account (login) Changing a login Removing a login Locking a login Adding a login group Removing a login group Adding web access profiles Changing web profiles Duplicating web profiles Deleting web profiles Changing the profile base Displaying the profile base
SAT Screen User Profile	Adding a user profile for using the SAT Adding SAT profiles Adding extended profiles Duplicating SAT profiles Deleting user profiles

Managing accounts using Communication Manager Web pages

The Administrator Accounts web pages allow you to add, change, lock, or remove local administrator logins and login groups on this server. Logins that are authenticated in an external server such as an LDAP server cannot be managed from this page.

Logins that are member of the **susers** Linux group can have full access to all the web pages. Logins that are members of the **users** Linux group have limited access to Communication Manager web pages. The Security > Web Access Mask page Web page allows you to further restrict individual logins in the **susers** and **users** Linux groups based on membership in a secondary (profile) Linux group.

Avaya recommends you use the Communication Manager web interface to manage administrator accounts.

Adding an administrator account (login)

A user account consists of the login, the Linux group, and a profile (additional group).

To create an administrator account using the Communication Manager Web pages:

1. On Communication Manager Maintenance Web Pages, navigate to Security>Administrator Accounts.
2. Enter a name in the box labeled **Enter Login ID or Group Name**.
3. Click on **Add Login**.
4. Click on **Submit**.

   The Administrator Login - Add Login page appears.
5. Click on to enable or fill in the following fields:

- **login group** (users, susers, or remote)
  - users for a login with limited access (formerly known as customer non-super-user login)
  - susers for a privileged login (wide permissions in the server)
- **additional groups** (prof2, prof3, prof18-prof69)

  Assign an access profile, or leave blank if the login needs no access to Communication Manager SAT or Web pages.
- **allow Linux shell access**

  No shell access limits the direct access to a shell on login. To deny shell access for this user, assign the user either no profile group or a SAT profile with shell access (go shell) disabled.
- **lock this account**
- **date on which account is disabled**

  blank if the feature is not used
- **select type of authentication**

  password or ASG. Selecting ASG authentication fails if a license for ASG is not present on the server.
- **enter key or password**
- **re-enter key or password**
- **force password/key change on first login**

  yes or no

- **maximum Number of days a password may be used**

  Number of days before password must be reset. Applies only to this account as it is being created.

- **number of days warning given before password expires**

  0-99999. Applies only to this account as it is being created.

- **days after password expires to lock account**

  0-99999. Applies only to this account as it is being created.

6. Click on **Add**.

If this is new profile:

- Define Communication Manager web access permissions on the Security>Web Access Mask page. See Recommended procedure for adding web profiles on page 93.
- Define Communication Manager SAT access permissions on at the SAT, on the User Profile screen (**`add user-profile`**). See Adding SAT profiles on page 96.

Changing a login

To change an existing login:

1. On Communication Manager Maintenance Web Pages, navigate to Security>Administrator Accounts.
2. Enter the name of the login you want to change.
3. Click on **Change Login**.
4. Click on **Change**.

   The Administrator Logins -- Change Login page appears.
5. Make the desired changes and click on **Change**.

Removing a login

To remove an existing login:

1. On Communication Manager Maintenance Web Pages, navigate to Security>Administrator Accounts.
2. Enter the name or number of the login you want to remove.
3. Click on **Remove Login**.
4. Click on **Delete**.

Locking a login

Lock a login to deny access to the account. For example, lock the login when you want to deny access but don't want to remove the account completely, such as for a person who has left the company.

To lock or unlock a login:

1. On Communication Manager Maintenance Web Pages, navigate to Security>Administrator Accounts.
2. Enter a name or number in the box labeled **Enter Login ID or Group Name**.
3. Click on **Lock/Unlock login**.
4. Click on **Submit**.

Adding a login group

To create a login group (profile):

1. On Communication Manager Maintenance Web Pages, navigate to Security>Administrator Accounts.
2. Enter a name or number in the box labeled **Enter Login ID or Group Name**.
3. Click on **Add Login Group**.
4. Click on **Submit**.

   The Add Login Group page appears.
5. Enter the number of the Login Group.
6. Click on **Add**.

Removing a login group

Do not remove a login group that has any login is assigned to the group.

To remove a login group (profile):

1. On Communication Manager Maintenance Web Pages, navigate to Security>Administrator Accounts.
2. Enter a name or number in the box labeled **Enter Login ID or Group Name** .
3. Click on **Remove Login Group**.
4. Click on **Delete**.

Managing profiles using the Communication Manager SAT

Adding a user profile for using the SAT

To create a user profile in Communication Manager:

1. At the SAT, enter **`add user-profile`**.
2. Edit the profile to restrict or give permission to the user as desired.

Enabling a second craft login at the SAT

To enable a second **craft** login associated to user-profile 3 (create the permissions for the second **craft** login):

- **Dadmin** must be enabled in the license file. **Dadmin** can enable only one second **craft** login.
- The first **craft** login must already exist.
- Create the login using the Communication Manager Security>Administrator Accounts server web pages or in an external AAA server if it doesn't already exist.

1. Login to the Communication Manager server using the **dadmin** login.
2. Enter **`sat`** to invoke Communication Manager.
3. Enter **`enable craft2 xyz`**, where *xyz* is the unique name for the login.

   This login has the same permissions as the **craft** login and uses Profile 3.

Managing passwords and Access Security Gateway

To set or change Access Security Gateway (ASG) or a password, see Adding an administrator account (login) on page 89

Administering Communication Manager web access profiles

Adding web access profiles

When adding a web profile, Avaya recommends copying Profile 18 for **susers** (customer super-user access) or Profile 19 for **users** (customer non-super-user access) depending on the basic Communication Manager access required, and reducing the access permissions as required.

Recommended procedure for adding web profiles

Examine the web menus for profiles 18 and 19. If the menu for profile 19 contains all the Web pages a user needs, copy profile 19 to create the new profile. If the user needs access to pages that are not present in profile 19, copy profile 18 to create a new profile. Edit the new profile to remove access for Web pages the user does not need. Access to Web pages in profile 18 requires the login be in the **susers** group.

To create a web profile (access mask):

1. On Communication Manager Maintenance Web Pages, navigate to Security>Web Access Mask.
2. On the **Web Access Mask** page, click on the **Add** button.
3. Enter the new profile number (20-69) in the box labeled **Enter new Access Mask Number**.
4. Select **Create by Copying values from Access Mask number**.
5. Enter 18 to copy super-user permissions, or 19 to copy non-super-user permissions.

   You may also copy any other existing profile and its unique permissions to create a new profile with those same permissions.
6. Click on **Submit**.

   The **Web Access Mask** page appears.
7. Check the box next to the new profile number.
8. To verify or edit permissions, click on **Change**.

9. In the column beneath the new profile number, verify that a check is in the box for each Web page (menu item) this profile can access.
10. To name the profile, enter a name in the box next to the profile number at the top of the page.
11. Click on **Submit**.

Changing web profiles

To change permissions for a web user profile (web access mask):

1. On Communication Manager Maintenance Web Pages, navigate to Security>Web Access Mask.
2. On the **Web Access Mask** page, check the box next to the profile number to edit.
3. Click on **Change**.
4. On the **Change Access Masks** page, check the box in the row beside a Menu-Item to allow access to that item for this profile.
5. Click on **Submit**.

Duplicating web profiles

Duplicate an existing profile to create a new profile with similar permissions. See Adding web access profiles on page 93.

Deleting web profiles

To delete an existing web profile (web access mask):

1. On Communication Manager Maintenance Web Pages, navigate to Security>Web Access Mask.
2. On the **Web Access Mask** page, check the box next to the profile number to edit.
3. Click on **Delete**.

   The Delete Access Mask page appears.
4. Click on **Submit**.

Changing the profile base

Ensure that no existing Linux groups use the same range as the new set of profiles you are creating.

To change a profile base through the Web:

1. On Communication Manager Maintenance Web Pages, navigate to Security>Web Access Mask.
2. On the **Web Access Mask** page, click on the Change Access Mask Base button.
3. Enter the new Access Mask Base number in the box provided.
4. Click on Submit.

When the Profile Base number is changed:

- Numbers change for Linux groups whose name begins with the string "prof".
- Corresponding Linux group names do not change.

This is an example of the Linux group file before and after changing the profile base number from 10,000 to 20, 000.

This is the Linux group file with a base profile number 10,000:

prof0:x:10000:init

prof1:x:10001:inads

prof2:x:10002:dadmin

prof3:x:10003:craft

prof17:x:10017:acpsnmp

prof18:x:10018:joe, tom

prof19:x:10019:

prof23:x:10023:msa

This is the Linux group file after the base profile number is changed to 20,000:

prof0:x:20000:init

prof1:x:20001:inads

prof2:x:20002:dadmin

prof3:x:20003:craft

prof17:x:20017:acpsnmp

prof18:x:20018:joe, tom

prof19:x:20019:

prof23:x:20023:msa

Displaying the profile base

To display the profile base on the Maintenance Web Pages:

1. On Communication Manager Maintenance Web Pages, navigate to Security>Web Access Mask.
2. The Access Mask Base number appears on the Web Access Mask page.

Administering user profiles for Communication Manager SAT access

Adding SAT profiles

Add a Communication Manager SAT profile to define the accessible SAT forms for a user assigned this profile.

1. At the SAT, using a login with a profile with access to the User-Profile SAT screen, enter **`add user-profile [`*`n`*` |next]`**.
2. In the User Profile screen, fill in the following fields:

- **User Profile Name**: optional field, may be used to identify the profile's purpose or use
- **This profile is disabled**: activates, disables the profile. A user assigned to a profile that is disabled is denied all access.
- **Facility Test Call Notification**: Enter **y** to have the user receive notification at logoff if Facility Test if Notification is still administered.
- **Grant un-owned permissions**: If this profile has write access to the user-profile form, a user with this profile can grant any permission allowed for profile 18 (customer super user) to other profiles even though this profile does not itself have those permissions.
- **Shell Access**: **y** allows the user to execute **`go shell`** from the SAT
- **Acknowledgment required**: Enter **y** to require the user to acknowledge they want to logoff while Facility Test if Notification is still administered.
- Extended Profile: **y** enables the extended profile for this SAT profile.

3. Enter **y** in the **Enbl** column opposite the objects (SAT screens) in the **Name** column to allow users with this profile access to the objects.
4. Optionally, use pages 2-x to further define permissions for each SAT screen. See the description of the **`add user-profile`** command in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431, for more information.

The SAT profile form lists all the possible SAT screens in the software regardless of whether the associated feature is enabled, disabled, licensed or not licensed. The profile form will not enable, disable or otherwise modify what is available on the system.

Related commands:

- **add user-profile**
- **add user-profile-by-category**
- **duplicate user-profile**
- **import user-profiles**

Adding extended profiles

Extended profiles provide additional access control for vector and station forms.

To add extended profile permissions to a new or existing profile for Communication Manager:

1. At the SAT, enter **add user-profile** or **change user-profile**.
2. Set the **Extended Profile** field to **y.**

   See the description of the **extended user-profile** command in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431, for more on the extended profile form.

If the **Extended Profile** field on the user-profile form is **y,** an extended profile may exist even if the vector or station form access is set to "- -" on the standard profile.

Duplicating SAT profiles

Duplicate an existing profile to create a new profile with similar permissions.

1. At the SAT, enter **duplicate user-profile *X*** where *X* is an existing profile.

   The User Profile screen appears.
2. Enter the new profile number in the **User Profile** field and submit the form.

Deleting user profiles

To delete a SAT profile and its extended profile, if one exists:

1. At the SAT, type **remove user-profile *n*** where *n* is the number of the profile to delete.

   The User Profile screen appears.

2. Submit the form.

To delete the extended profile only from an existing profile:

1. At the SAT, type **change user-profile *n*** where *n* is the number of the extended profile to delete.
2. Set the **Extended Profile** field to **n** and submit the form.

   The extended profile for this profile is deleted.

Exporting and importing SAT profiles

You can edit SAT profile information in Microsoft Excel and import the information back into Communication Manager.

To export a SAT profile:

1. At the SAT, with export permissions, enter **export-user profiles**.

   All user-defined profiles (20-69) are saved to a tab delimited file in /var/home/ftp/pub/cmprofiles.txt.

This file can be imported to Microsoft Excel and edited. If you want to re-import the changed file into Communication Manager, export the file from Excel to a tab delimited file in /var/home/ftp/pub/comprofiles.txt.

To import a SAT profile:

1. At the SAT, enter **import-user profiles**.

   The file in /var/home/ftp/pub/cmprofiles.txt is imported.

Displaying the profile base

To display the profile base at the SAT:

1. Enter **display profile-base**.

   The User Profile Base screen appears and shows the profile base number.

Abbreviated Dialing

Use the Abbreviated Dialing (AD) feature to reduce the number of digits that you must dial to place a call. Instead of dialing the entire number, you dial a short code to access the number. The system then dials the stored number automatically. You can also assign abbreviated dialing buttons to telephones, so that you press a single button to dial frequently called numbers.

Abbreviated Dialing is sometimes called speed dialing.

You can store telephone numbers in four different types of abbreviated dialing lists:

- Personal
- Group
- System
- Enhanced

You can also assign privileged numbers to abbreviated dialing lists. Users can use privileged numbers to place calls to numbers that might otherwise be restricted.

Privileged group-number, system-number, and enhanced-number lists provide access to numbers that usually might be restricted.

The switch type and the version determine which lists are available and how many entries you can have on each list. You can assign up to three AD lists to each user or extension. You can assign any combination of a system list, an enhanced list, and as many as three personal lists or three group lists. The list can also have three group lists. Each entry on an abbreviated dialing list can have as many as 24 characters.

Abbreviated Dialing labeling

Users can administer labels for the AD buttons that appear as softkeys on the following telephones:

- 2420 DCP
- 4600 series
- 6400 series
- 8400 series

These personalized labels appear on the menu display of these telephones.

Abbreviated Dialing on-hook programming

With on-hook programming, users can access the programming mode of the telephone without going off-hook. On-hook programming works with the following telephones:

- 2420 DCP
- 4600 series
- 6400 series
- 8400 series, with enabled speakers

With on-hook programming, signaling changes from dual-tone multifrequency (DTMF) to the S-channel. This change allows a longer 60-second timeout period. For nondisplay telephones, signaling remains DTMF, and the timeout period is 10-seconds.

Detailed description of Abbreviated Dialing

This section provides a detailed description of the Abbreviated Dialing feature.

Abbreviated Dialing supports the following types of lists:

- Personal lists

  Use personal lists for users who need their own set of stored numbers. You determine which users have access to a personal list and the size of each list. Either you or the user can assign telephone numbers to personal lists. A personal list is created automatically when you assign the list to an individual telephone. Each user can have as many as three personal lists. You can assign a personal list to an attendant with a data module.

- Group lists

  You can define group lists for groups or departments where members of the group must frequently dial the same numbers.You determine which users have access to group lists. Each user can have access to three group lists. You can program the list or you can designate a user in each group to program the list. Specify this designated user on the Abbreviated Dialing Group List screen.

- System lists

  You can define one system list for the entire organization. Most administrators assign this list to each telephone, and allow everyone in the organization to use the list. If you allow everyone to use the system list, include only numbers that anyone in your organization has permission to call. For example, you might want to add an emergency telephone number or telephone numbers for other office locations to this list.

  The system list can contain up to 100 entries, and can be changed by a system administrator. An administrator can also customize the button labels displayed on Avaya 2420 and Avaya 4620 telephone sets for these system-list entries.

- Enhanced lists

  You can use enhanced lists for telephone users, data-terminal users, and attendants who need more list entries than the number of entries allowed in group-number and system-number lists. Two enhanced-number lists are allowed per system, in addition to the system-number list. The enhanced list can contain any number or dial-access code.You administer the enhanced lists and determine which users can access the lists.

Administering Abbreviated Dialing

The following steps are part of the administration process for the Abbreviated Dialing feature:

- Adding Abbreviated Dialing lists
- Assigning telephones for group lists

This section describes:

- Any prerequisites for administering the Abbreviated Dialing feature
- The screens that you use to administer the Abbreviated Dialing feature
- Complete administration procedures for the Abbreviated Dialing feature

Prerequisites for Abbreviated Dialing

You must complete the following actions before you can administer the Abbreviated Dialing feature:

- View the Optional Features screen, and ensure that the **Abbreviated Dialing Enhanced List** field is set to **y**. If the **Abbreviated Dialing Enhanced List** field is set to **n**, your system is not enabled for Enhanced Lists for the Abbreviated Dialing feature. You will be able to access the other types of lists.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

  For a complete description of the Optional Features screens, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Abbreviated Dialing

Screen name	Purpose	Fields
Abbreviated Dialing List	Add Abbreviated Dialing lists.	• **Size** • **Program Ext**
Station	Define extensions for lists and program buttons used by the Abbreviated Dialing feature.	**Group**

Adding Abbreviated Dialing lists

To add an Abbreviated Dialing group list:

1. Type **`add abbreviated-dialing group next`**. Press **Enter**.

   The system displays the Abbreviated Dialing List screen (Figure 4: Abbreviated Dialing List screen on page 103). In this example, the next available group list is group 3.

Figure 4: Abbreviated Dialing List screen

```
add abbreviated-dialing group next                              Page 1 of 1

                            Abbreviated Dialing List

              Group List: 3           Group Name: _____________
    Size (multiple of 5): __          Program Ext: ________ Privileged? n
DIAL CODE
     01: ____________________________
     02: ____________________________
     03: ____________________________
     04: ____________________________
     05: ____________________________
```

2. In the **Group Name** field, type a name for this list.
3. In the **Size** field, type a number in multiples of 5. This number defines the number of entries on the dialing list.

   For example, if you want to store eight telephone numbers in the list, type **10** in the **Size** field.
4. In the **Program Ext** field, type the extension.
5. Type the telephone numbers that you want to store. Type one number for each dial code.

   Each telephone number can be up to 24 digits long.
6. Press **Enter** to save your changes.

You can display the new abbreviated dialing list to ensure that the information is correct. You can also print a copy of the list.

Assigning telephones for group lists

To assign a telephone access to a group list:

1. Type **`change station n`**, where ***n*** is the extension that you want to assign to the group list. Press **Enter**.

   The system displays the Station screen.
2. Click **Next** until you see the **Abbreviated Dialing** area (Figure 5: Station screen on page 104).

Figure 5: Station screen

```
change station 9876543                                        Page 3 of 3

                                    Station

SITE DATA
      Room: _______                                      Headset? n
      Jack: _______                                      Speaker? n
     Cable: _______                                     Mounting? d
     Floor: _______                                 Cord Length: 0
  Building: _______                                   Set Color: ______

  ABBREVIATED DIALING
       List1: group   3         List2: _________          List3: _________

  BUTTON ASSIGNMENTS
    1: call-appr                          4: __________
    2: call-appr                          5: __________
    3: call-appr                          6: __________
```

3. Type **group** in any of the three **List** fields. Press **Enter**.

   The system displays a blank list number field.

4. Type **3** in the list number field.

   When you assign a group list or a personal list, you must also specify the personal list number or the group list number.

5. Press **Enter** to save your changes.

To use this list, the user at extension 987-6543 dials the Feature Access Code (FAC) for the list and the dial code for the number that the user wants to dial. You can also assign an abbreviated dialing button to this extension. The user can then press one button to dial a specific number on one of the three assigned abbreviated lists of the user.

End-user procedures for Abbreviated Dialing

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Abbreviated Dialing:

- Programming the Abbreviated Dialing feature

Programming the Abbreviated Dialing feature

These instructions apply to most Avaya telephones with display screens, and work with DEFINITY® software release 6.3 or later.

1. On your telephone, press the button labeled **Prog** to enter programming mode. If your telephone does not have the **Prog** softkey, press the **Menu** softkey and navigate to the **Prog** option.

   The telephone goes off hook and enters the speaker phone mode.

2. Select the softkey/feature button you want to program until you see the label of the softkey you want to display.You will see the message **Change number? Yes = 1 No = 2**.
3. Pick the option you want. You will see a message **Enter number:** on the display. Enter the number you want that button to call.
4. Press the **#** key to save your changes.
5. You will see **Enter label** on the display. Use the dial pad to enter the label you want. The label can be up to five characters in length.
6. To exit from the **Prog** mode, hang up your telephone. Pressing the **Exit** button does not exit you from programming mode.

Note:

If the number you are entering for an Abbreviated Dialing button is an outside number, you must include 9 or any other applicable trunk code. Numbers programmed on softkeys can be up to 24 digits in length.

Considerations for Abbreviated Dialing

This section provides information about how the Abbreviated Dialing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Abbreviated Dialing feature under all conditions.

- You cannot remove a telephone or attendant if it is designated as the extension that is allowed to program a group-number list.
- When using an AD button to access a messaging system, the user’s login and password should not be assigned to the button. The system ignores button entries after the messaging access number.
- You can use an abbreviated dialing list at any time during incoming or outgoing calls.

Interactions for Abbreviated Dialing

This section provides information about how the Abbreviated Dialing feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Abbreviated Dialing in any feature configuration.

- Last Number Dialed

  The Last Number Dialed feature redials the same number a user just dialed. This happens even if the user accessed an abbreviated dialing list for the previous call. However, if the last dialed string includes any special characters, these characters are ignored by last-number-dialed call. Examples of special characters might be indefinite wait, mark, pause, suppress, wait and so on.

  If the previously-called number was in an AD privileged list, and if the user is not usually allowed to dial the number because of his or her class of restriction, they cannot redial the number using Last Number Dialed. To redial the number, the user must again access the AD privileged list.

Troubleshooting Abbreviated Dialing

Problem	Possible causes	Action
A user cannot access a abbreviated dial list.	• The specific list might not be assigned to the user's telephone.	• Type **display station *n***, where ***n*** is the extension of the user. Press **Enter**. • Review the current settings of the **List1**, **List2**, and **List3** fields to determine if the list is assigned to the telephone of the user.
	• If the user attempted to use a Feature Access Code to access the list, they may have dialed the incorrect Feature Access Code.	• Type **display feature-access-codes**. Press **Enter** • Verify that the user is dialing the appropriate Feature Access Code.
	• If the user attempted to press a feature button, they might have pressed the incorrect feature button.	• Type **display station *n***, where ***n*** is the extension of the user. Press **Enter**. • Review the current feature button assignments to determine if the user pressed the assigned button.
	• If the user attempted to press the correct feature button, the button may not be set up correctly.	• Type **display station *n***, where ***n*** is the extension of the user. Press **Enter**. • Review the current feature button assignments to ensure if the list number and dial code are correct.
A user states that an abbreviated dialing list dials the wrong number.	• The user is using the wrong dial code. • The dial code is defined incorrectly. • ARS digit conversion was not administered correctly.	• Ask the user the number that was dialed or the button that he or she pressed to determine which list and dial code the user attempted to call. • Access the dialing list and verify that the number stored for the specific dial code corresponds to the number the user wanted to dial. • For example, to access a group list, type **display abbreviated-dialing group *n***, where ***n*** is a group list number. Press **Enter**. • If the user dialed the wrong code, give them the correct code. • If the dial code is wrong, press **Cancel** and use the appropriate change command to access the abbreviated dialing list again. Type the number. Press **Enter**.

Edit Dialing

Edit Dialing feature enables you to pre-dial a number when the telephone is on-hook. During the pre-dialing phase, you can edit the digits of a dialed number. The number is dialed when you go off-hook (lifts handset or presses the **speaker** button) or press the **send soft** key.

Edit dialing feature is available on Communication Manager Release 5.2 or later. The 96xx Series with IP phones with H.323 3.0 or later firmware support this feature. This feature is not supported with IP telephones with SIP firmware.

The **Systems Parameter** field on the Feature-Related System Parameters screen in Communication Manager controls this feature for all Edit Dial capable telephones. When enabled, a telephone goes into the Edit Dial mode in the on-hook state. After enabling a telephone, when you press a dial pad button in a 96xx phone, Communication Manager sends a message to Edit Dial capable telephones. This message instructs the firmware to collect digits to send to Communication Manager.

Feature interactions

When invoked, these features disable Edit Dial and re-enable Edit Dial when the feature terminates. The features listed in this section use on-hook dialing:

- Aux Work Reason Codes
- Automatic Wakeup
- Check In/Out
- Directory
- Do Not Disturb (DND)
- DND Group
- DID View/Remove
- Hotel/Motel Features
- Message Retrieval
- Message Notification On/Off
- Maid Status
- Manual and Clocked Override
- Posted Messages
- VIP Check In

Edit Dialing System Parameters screen

Figure 6: Edit Dialing - Feature Activation

```
change system-parameters features                              Page  10 of  x
                      FEATURE-RELATED SYSTEM PARAMETERS

                 Pull Transfer: n            Update Transferred Ring Pattern? n
         Outpulse Without Tone? y              Wait Answer Supervision Timer? n
         Misoperation Alerting? n               Repetitive Call Waiting Tone? n
    Allow Conference via Flash? y
 Vector Disconnect Timer (min):       Network Feedback During Tone Detection? y
                                    System Updates Time On Station Displays? n

                    Station Tone Forward Disconnect: silence
                             Level Of Tone Detection: precise
          Charge Display Update Frequency (seconds): 30
                           Date Format on Terminals: mm/dd/yy
                       Onhook Dialing on Terminals? y
              Edit Dialing on 96xx H.323 Terminals? y
                 Allow Crisis Alert Across Tenants? y


ITALIAN DCS PROTOCOL
  Italian Protocol Enabled? y
   Apply Intercept Locally? y      Enforce PNT-to-PNT Restrictions? n
```

Edit Dialing on 96xx H.323 Terminals?

Field description

Valid entries	Usage
y/n	To enable Edit Dialing, select **y**. To disable the feature, select **n**. The default value is **n**.

Access Security Gateway

Use the Access Security Gateway (ASG) feature to require the use of an ASG Key to log in to the system, and thus prevent unauthorized access. ASG is an authentication interface that secures the system administration and maintenance ports, as well as the logins on the system. ASG uses a challenge-and-response protocol to confirm the validity of a user. This process reduces the opportunity for unauthorized access.

Detailed description of Access Security Gateway

Use the Access Security Gateway (ASG) feature to authenticate authorized users as users attempt to access Communication Manager. Successful authentication is accomplished when the ASG feature communicates with a compatible key. The challenge-and-response negotiation starts once the system establishes an RS-232 session. The user must type a valid system login ID. Communication Manager then issues a challenge based on the login ID that the user types. The user must provide the expected response.

The core of this transaction is a secret key, which is information that both the lock (ASG) and the key possess. The relevance of the authentication token that is used to perform the challenge-and-response negotiation is limited to the current session.

The supported key consists of a hand-held encryption-generating device called the ASG key. The key is preprogrammed with the appropriate secret key to communicate with corresponding ASG-protected login IDs on Communication Manager.

Administering Access Security Gateway

The following steps are part of the administration process for the Access Security Gateway feature:

- Setting up Access Security Gateway
- Disabling Access Security Gateway
- Restarting Access Security Gateway
- Modifying Access Security Gateway for a lost key
- Monitoring the Access Security Gateway history log

This section describes:

- Any prerequisites for administering the Access Security Gateway feature
- The screens that are required to administer the Access Security Gateway feature
- Complete administration procedures for the Access Security Gateway feature

Prerequisites for administering Access Security Gateway

You must complete the following actions before you can administer the Access Security Gateway (ASG) feature:

- You must have a *superuser* login ID.
- View the Optional Features screen, and ensure that the **Access Security Gateway** field is set to **y**. If the **Access Security Gateway** field is set to **n**, your system is not enabled for the Access Security Gateway feature. Contact your Avaya representative before you continue with this procedure.

  To access the Optional Features screen, type **`change system-parameters customer-options`**. Press **Enter**.

Screens for administering Access Security Gateway

Screen Name	Purpose	Fields
Optional Features	Ensure that the Access Security Gateway (ASG) feature is enabled.	**Access Security Gateway**
Login Administration	Set up the ASG secret key.	• **System Generated Secret Key** or **Secret Key** • Other optional fields as desired
Security-Related System Parameters	Set security-related parameter preferences.	All
Access Security Gateway Session History	View events that are related to ASG session establishment and session rejection.	All

Setting up Access Security Gateway

To set up Access Security Gateway:

1. Type **change login** *n*, where *n* is the alphanumeric *superuser* login ID. Press **Enter**.

   The system displays the Login Administration screen (Figure 7: Login Administration screen on page 113).

Figure 7: Login Administration screen

```
change login 1234
                              LOGIN ADMINISTRATION

               Password of Login Making Change:

           LOGIN BEING ADMINISTERED
                              Login's Name:xxxxxxx
                                Login Type:
                             Service Level:
    Disable Following a Security Violation?
                                                      Access to INADS Port? _

          LOGIN'S PASSWORD INFORMATION
                         Login's Password:
                  Reenter Login's Password:
        Password Aging Cycle Length (Days):

        LOGOFF NOTIFICATION
          Facility Test Call Notification? y     Acknowledgment Required? y
               Remote Access Notification? y     Acknowledgment Required? y

ACCESS SECURITY GATEWAY PARAMETERS
Access Security Gateway? n
```

2. In the **Password of Login Making Change** field, type your password.
3. In the **Access Security Gateway** field, type **y**.

   When you type **y**, the system automatically displays the Access Security Gateway Login Administration screen (page 2).
4. Perform one of the following actions:
   - In the **System Generated Secret Key** field, type **y** for a system-generated secret key.
   - In the **Secret Key** field, type your secret key.
5. Complete any of the remaining, optional fields on page 2 that you want to administer.
6. Press **Enter** to save your changes.

7. Type **change system-parameters security**. Press **Enter**.

   The system displays the Security-Related System Parameters screen (Figure 8: Security-Related System Parameters screen on page 114).

Figure 8: Security-Related System Parameters screen

```
change system-parameters security                              Page 2 of 2

                         SECURITY-RELATED SYSTEM PARAMETERS

  SECURITY VIOLATION NOTIFICATION PARAMETERS

    SVN Station Security Code Violation Notification Enabled? y
            Originating Extension: ________   Referral Destination:
________  Station Security Code Threshold: 10             Time Interval: 0:03
           Announcement Extension: ________

  STATION SECURITY CODE VERIFICATION PARAMETERS

                       Minimum Station Security Code Length: 4
    Security Code for Terminal Self Administration Required? y

  ACCESS SECURITY GATEWAY PARAMETERS

    SYSAM-LCL? n      SYSAM-RMT? y
        MAINT? n       SYS-PORT? n
```

8. In the **Access Security Gateway Parameters** section, determine which of the listed port type fields to set to **y**. In this example, the **SYSAM-RMT** field is set to **y**.

   Note:
   Avaya recommends that you protect the SYSAM-RMT port since the SYSAM-RMT port is a dial-up port, and therefore more susceptible to compromise.

9. Press **Enter** to save your changes.

Disabling Access Security Gateway

To temporarily disable ASG:

1. Type **change login *n***, where ***n*** is the alphanumeric login ID.

   The system displays the Login Administration screen (Figure 7: Login Administration screen on page 113).

2. Click **Next** until you see the Access Security Gateway Login Administration screen.

3. On the Access Security Gateway Login Administration screen, set the **Blocked** field to **y**.

   When you set the **Blocked** field to **y**, you do not remove the login from the system. You temporarily disable the login.

4. Press **Enter** to save your changes.

Note:
A superuser can disable and restart access for another superuser.

Restarting Access Security Gateway

To restart a temporarily disabled ASG access for login:

1. Type **change login *n***, where ***n*** is the alphanumeric login ID. Press **Enter**.

   The system displays the Login Administration screen (Figure 7: Login Administration screen on page 113).

2. Click **Next** until you see the Access Security Gateway Login Administration screen.
3. On the Access Security Gateway Login Administration page, set the **Blocked** field to **n**.
4. Press **Enter** to save your changes.

Modifying Access Security Gateway for a lost key

To modify ASG if the user loses an ASG Key:

1. Modify any logins that are associated with the lost Access Security Gateway Key. See the *Access Security Gateway (ASG) Key Release 1.0 User's Guide* for more information on how to change your Personal Identification Number (PIN).
2. If the login is no longer valid, type **remove login *n*,** where ***n*** is the alphanumeric login ID, to remove the invalid login from the system. Press **Enter**.
3. To keep the same login, change the secret key that is associated with the login to a new value.
4. Using the new secret key value, rekey the devices that generate responses and interact with the login.

Monitoring the Access Security Gateway history log

The Access Security Gateway Session History Log records all events that are associated with ASG session establishment and rejection, except when the **Access to INADS Port** field on the Login Administration screen is set to **y**. You must be a superuser to use the **`list asg-history`** command.

To access the log:

1. Type **`list asg-history`**. Press **Enter**.

   The system displays the Access Security Gateway screen (Figure 9: Access Security Gateway Session History screen on page 116).

Figure 9: Access Security Gateway Session History screen

```
                    ACCESS SECURITY GATEWAY SESSION HISTORY

Date    Time    Port        Login    Status
01/06   12:45   SYSAM-RMT   csand    AUTHENTICATED
01/05   01:32   SYSAM-LCL   jsmith   REJECT-BLOCK
01/05   12:33   SYSAM-RMT   ajones   REJECT-EXPIRE
01/03   15:10   SYSAM-RMT   swrigh   REJECT-PASSWORD
01/02   08:32   SYSAM-LCL   jsmith   REJECT-INVALID
01/02   07:45   SYSAM-RMT   mehrda   REJECT-RESPONSE
```

This screen displays the following fields:

- **Date**. Contains the date of the session establishment or rejection in the mm/dd format, where
  mm = month and dd = day.
- **Time**. Contains the time of the session establishment or rejection in the hh/mm format, where
  hh = hour and mm = minute.
- **Port**. Contains the mnemonic that is associated with the port on which the session was established or rejected. The port mnemonics for G3r systems are:
  - SYSAM-LCL
  - SYSAM-RMT
  - MAINT
  - SYS-PORT

  The port mnemonics for G3si systems are:
  - MRG1

  - INADS
  - NET
  - EPN
- **Login**. Contains the alphanumeric login string that the user entered and that is associated with the session establishment or rejection.
- **Status**. Contains a code that indicates whether the session was established or rejected and, if rejected, the reason for the rejection.

Interactions for Access Security Gateway

This section provides information about how the Access Security Gateway feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the Access Security Gateway feature in any feature configuration.

- Customer Access to Initialization and Administration System (INADS) Port

  If access to the INADS port is disabled on a system-wide basis, administering access to the SYSAM-RMT or INADS port through ASG does not override the INADS port restriction. Administration does not prohibit assignment of ASG to the SYSAM-RMT or INADS port. However, in a configuration where this method of access is blocked, you are denied access to the system through the SYSAM-RMT or INADS port, even if you use a valid ASG login ID.

  If access to the INADS port is disabled for login, administering access to the SYSAM-RMT or INADS port by way of ASG does not override the INADS port restriction.

- Login Administration

  ASG does not modify the standard user interface for Communication Manager login administration. Also, the standard Communication Manager login user interface is maintained in cases where ASG parameters are not administered for the login or the port.

- Security Violation Notification (SVN)

  ASG does not support an interface to SVN. Session rejection events do not appear in the monitor security violations login report. Referral calls are not spawned if the number of rejected ASG sessions exceeds the threshold or the time interval criteria that SVN imposes.

- Security Measurements

  Events that are related to ASG session establishment or rejection do not increment the Successful Logins, Invalid Attempts, Invalid IDs, Forced Disconnects, Login Security Violations, or Trivial Attempts counters that are maintained for the list measurements security-violations detail report. Additionally, ASG-related data is not included in login-specific information that is maintained by the measurements security-violations summary report.

Administered Connections

Use the Administered Connections (AC) feature to establish an end-to-end connection between two access or data endpoints. Communication Manager automatically establishes the connection based on the attributes that you administer. The Administered Connections feature provides the following abilities:

- Support of both permanent and scheduled connections
- Autorestoration (preserving the active session) for connections that are routed over Software Defined Data Network (SDDN) trunks
- An administrable retry interval from 1 to 60 minutes for each AC
- An administrable alarm strategy for each AC
- An establish, retry, autorestoration order that is based on administered priority

Detailed description of Administered Connections

Use the Administered Connections (AC) feature to administer virtual private-line connectivity over the AT&T Switched Network. Access is over an ISDN trunk group for which the **Service Type** field on the ISDN Trunk Group screen is set to **SDDN** (Software Defined Data Network). The system uses the **Destination** field on the Administered Connection screen to route calls when AC is active, based on associated authorized time-of-day fields.

You can establish an AC between:

- Two endpoints on the same server
- Two endpoints in the same private network, but on different servers
- One endpoint on the controlling server, and another endpoint off the private network

In all configurations, administer the AC on the server that has the originating endpoint. For an AC in a private network, if the two endpoints are on two different servers, Automatic Alternate Routing (AAR) through ISDN, DS1, or analog tie trunks and intermediate servers are usually used to route the connection. If required, you can also use Automatic Route Selection (ARS) and Generalized Route Selection (GRS) through the public network. The system routes the call over associated ISDN trunks. When the far-end answers, a connection occurs between the far-end and the near-end extension that is administered in the **Originator** field on the Administered Connection screen.

Access endpoints

Access endpoints are nonsignaling trunk ports. Access endpoints neither generate signaling to the far-end of the trunk nor respond to signaling from the far-end. You designate an access endpoint as the originating endpoint or the destination endpoint in an AC.

Typical applications

The following examples are typical AC applications:

- A local data endpoint that connects to a local or a remote access endpoint, such as:
  - A modular processor data model (MPDM) ACCUNET digital service that connects to SDDN over an ISDN trunk-group DS1 port; an MPDM
  - An MPDM ACCUNET digital service that connects to an ACCUNET Switched 56 Service over a DS1 port
- A local-access endpoint that connects to a local or a remote access endpoint, such as a DSO cross-connect and a 4-wire leased-line modem to a 4-wire modem connection over an analog tie trunk
- A local data endpoint that connects to a local or a remote data endpoint such as a connection between two 3270 data modules

Establishing Administered Connections

The originating server attempts to establish an AC only if one of the following conditions exist:

- AC is active.
- AC is due to be active. That is, the AC is a permanent AC, or it is the administered time-of-day for a scheduled AC.
- The originating endpoint is in the in-service or idle state.

If the originating endpoint is not in service or is idle, no activity takes place for the AC until the endpoint transitions to the necessary state. The originating server uses the destination address to route the call to the desired endpoint. When the server establishes two or more ACs at the same time, the server arranges the connections in order of priority.

AC attempts can fail because:

- Resources are unavailable to route to the destination.
- A required conversion resource is unavailable.

- Access is denied by Class of Restriction (COR), facilities restriction level (FRL), Bearer Capability Class (BCC), or an attempt is made to route voice-band data over SDDN trunks in the public switched network.
- The destination address is incorrect.
- The destination endpoint is busy.
- Other network or signaling failures occur.

In the event of a failure, an error is entered into the error log. This error generates an alarm, if your alarming strategy warrants an alarm. You can display AC failures with the **`display status-administered connection`** command. The originating server continues to try to establish an AC as long as an AC is scheduled to be active, unless the attempt fails because of an administrative error (for example, a wrong number) or a service-blocking condition, such as outgoing calls are barred).

- The administered retry interval of 1 to 60 minutes for each AC determines the frequency with which failed attempts are retried.
- Retries are made after the retry interval elapses, regardless of the restorable attribute of the AC.
- ACs are retried in priority order.
- When you change the time of day on the server, an attempt is made to establish all ACs in the waiting-for-retry state.

Dropping Administered Connections

An AC remains active until one of the following scenarios occurs:

- The AC is changed, disabled, or removed.
- The time-of-day requirements of a scheduled AC are no longer satisfied.
- One of the endpoints drops the connection. An endpoint might drop a connection because of user action (in the case of a data endpoint), maintenance activity that results from an endpoint failure, busying out of the endpoint, or handshake failure. If the endpoints are incompatible, the connection is successful until handshake failure occurs.

Note:
An AC between access endpoints remains connected even if the attached access equipment fails to handshake.

- An interruption, such as a facility failure, occurs between the endpoints. If an AC drops because the AC was disabled, removed, or is no longer due to be active, no action is taken. If an AC drops because of changed AC attributes, the system makes an immediate attempt to establish the connection with the changed attributes, if the AC is still scheduled to be active. Existing entries in the error or alarm log are resolved if the entries no longer apply. If an AC involves at least one data endpoint, and handshake failure causes the connection to be dropped, no action is taken for that AC until you run the **`change administered-connection`** command.

Autorestoration and fast retry

When an active AC drops prematurely, you must invoke either autorestoration or fast retry for autorestoration to be attempted for an active AC. If you administer an AC for autorestoration and the connection was routed over SDDN trunks, auto restoration is attempted. During restoration, connections are maintained between the server and both endpoints. In addition to maintaining the active session, AC also provides a high level of security by prohibiting other connections from intervening in active sessions. Autorestoration is usually complete before the 60-second endpoint holdover interval. If autorestoration is successful, the call might be maintained, but this is not guaranteed. The restoration is transparent to the user, with the exception of a temporary disruption of service while restoration is in progress. A successful restoration is indicated by the **restored** value in the **Connection State** field on the Administered-Connection Status screen. Although a restoration is successful, the data session might not be preserved.

If autorestoration is not active, or if the AC is not routed over SDDN trunks, the server immediately attempts a fast retry to reestablish the connection. The server also attempts a retry if the originating endpoint caused the drop. With fast retry, connections are not maintained on both ends. Fast retry is not attempted for an AC that was last established with fast retry, unless that AC is active for at least 2 minutes. If autorestoration or fast retry fails to restore or reestablish the connection, the call drops, and the AC goes into retry mode. Retry attempts continue, at the administered retry interval, as long as the AC is scheduled to be active.

Administering Administered Connections

The following steps are part of the administration process for the Administered Connections feature:

- Setting up Administered Connections

This section describes:

- Any prerequisites for administering the Administered Connections feature
- The screens that are required to administer the Administered Connections feature

- Complete administration procedures for the Administered Connections feature

Prerequisites for administering Administered Connections

You must complete the following actions before you can administer the Administered Connections feature:

- None

Screens for administering Administered Connections

Screen Name	Purpose	Fields
Data Modules		All
DS1 Circuit Pack		All
Access Endpoint		All
Trunk Group		All
Class of Restriction		All
Class of Service		All
Dial Plan Record		**Local Node Number**
Administered Connection		All
Station	assign one button as **ac-alarm**	**Feature Button Assignments** area
Attendant Console	assign one button as **ac-alarm**	**Feature Button Assignments** area

Setting up Administered Connections

Note:
For detailed information about the screens that you use in the following procedure, see the appropriate Feature Description, or *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

To set up an Administered Connection:

1. In the **Types** field on the Data Modules screen, choose one of the following data module Types. Administer all fields that the screen displays for that data module type.
   - Data Line Data Module. Use with Data Line circuit pack.
   - Processor/Trunk Data Module. Use with:
     - MPDMs, 700D, 7400B, 7400D, or 8400B
     - MTDMs, 700B, 700C, 700E, or 7400A
   - Processor Interface Data Module. See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504 for more information.
   - X.25 Data Module. See *Administering Network Connectivity on Avaya Aura™ Communication Manager* for more information.
   - 7500 Data Module. Use with an ISDN Line 12-BRI-S-NT or ISDN Line 12-BRI-U-NT circuit pack.
   - World Class Core BRI Data Module. Use with wcbri.
2. On the DS1 Circuit Pack screen, administer all fields. Use with server node carriers.
3. On the Access Endpoint screen, administer all fields.
4. In the **Group Type** field on the Trunk Group screen, choose one of the following Group Types. Administer all fields that the screen displays for that group type.
   - ISDN-BRI
   - ISDN-PRI
   - Tie
5. On the Class of Restriction screen, administer all fields.
6. On the Class of Service screen, administer all fields.
7. On the Dial Plan Record screen, administer the **Local Node Number** field with a number that matches the distributed communications system (DCS) server node number and the Call Detail Recording (CDR) node number. Valid values are 1 to 63.
8. On the Administered Connection screen, administer all fields.
9. On the Station screen, assign one button as **ac-alarm**.
10. On the Attendant Console screen, assign one button as **ac-alarm**.

Interactions for Administered Connections

This section provides information about how the Administered Connections feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the Administered Connections feature in any feature configuration.

- Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), Generalized Route Selection (GRS)
- Abbreviated Dialing

  Use Abbreviated Dialing entries in the **Destination** field on the Administered Connections screen. Entries must comply with restrictions.
- Busy Verification of stations and trunks

  This feature does not apply to access endpoints because access endpoints are used only for data.
- Call Detail Recording (CDR)

  For an AC that uses a trunk when CDR is active, the origination extension is the originator of the call. CDR is not available for access endpoints.
- Class of Restriction (COR)

  Reserve a COR for AC endpoints and SDDN trunks to restrict endpoints that are not involved in AC from connecting to SDDN trunks or endpoints that are involved in AC.
- Class of Service (COS) and Call Forwarding

  Assign a COS that blocks Call Forwarding activation at the AC endpoint.
- Data Call Setup

  Do not assign a default dialing destination to a data module when the data module is used in an AC.
- Data Hotline

  Do not assign a hotline destination to a data module when the data module is used in an AC.
- Digital Multiplexed Interface (DMI)

  Use DMI endpoints as the destination in an AC. DMI endpoints do not have associated extensions, so do not use DMI endpoints as the originator in an AC.
- Facility Test Calls

  The feature does not apply to access endpoints, because an access endpoint acts as an endpoint, rather than as a trunk.
- Hunting

  Do not use a hunt group extension as the originating endpoint of an AC.

- Modem Pooling

  If you require a modem in an AC, a modem is inserted automatically. If no modem is available, the connection is dropped.

- Non-Facility Associated Signaling (NFAS) and D-Channel Backup

  Auto restoration for an AC that is initially routed over an NFAS facility might fail if the only backup route is over the facility on which the backup D-channel is administered. The backup D-channel might not come into service in time to handle the restoration attempt.

- Set Time Command

  When you use the **set time** command to change the system time, all scheduled ACs are examined. If the time change causes an active AC to be outside its scheduled period, the AC is dropped. If the time change causes an inactive AC to be within its scheduled period, the server attempts to establish the AC.

  If any AC, scheduled or continuous, is in retry mode and the system time changes, the server attempts to establish the AC.

- System Measurements

  Access endpoints are not measured. All other trunks in an AC are measured as usual.

- Terminal Dialing

  Turn off terminal dialing for data modules that are used in an AC to prevent display of call-processing messages, such as INCOMING CALL, on the terminal.

- Trunk Groups

  To invoke autorestoration, route an AC over SDDN trunks. Because a successful restoration depends on an SDDN path, keep some SDDN trunks idle.

Administrable Alternate Gatekeeper List for IP Phones

Communication Manager 5.1 enhanced the Alternate Gatekeeper List (AGL) feature to allow administrators to specify the number of IP interfaces for each connected network region that are allowed for phones within a specific network region.

The Administrable Alternate Gatekeeper List feature limits the number of entries in the AGL, and is intended to simplify network region administration. This feature can improve system performance and reliability, and also reduce the time that it takes for phones to failover to the Enterprise Survivable Servers (ESS) or Local Survivable Processor (LSP).

This feature enhancement is available to all H.323 IP telephone types, and does not require any Communication Manager license file feature activation or firmware upgrades.

The Alternate Gatekeeper List (AGL) is used by H.323 IP telephones when they cannot reach or register with their primary gatekeeper. The AGL is a list of C-LANs/PE used by H.323 IP telephones to recover to when the current C-LAN is no longer available. The LSPs may be a separate failover set if the alternatives for reaching the main server are exhausted.

From Communication Manager 5.1, H.323 IP telephones in a network region can have an AGL list with no more than 16 members. You can continue to use the AGL feature of prior releases (up to 65 C-LAN/PE members in the AGL), or they can choose to use the more efficient method of controlling telephone recovery by condensing the number of gatekeepers sent by Communication Manager based on new network region administration.

Note:
Communication Manager 5.1 allows 16 C-LANs, 6 LSPs, and 1 Survivable Gatekeeper for a total for 23 gatekeepers.

To use the Communication Manager 5.1 AGL feature, administrators enter a numeric value in the new **AGL** field of the **Inter Network Region Connection Management** screen. The **Inter Network Region Connection Management** screen is used to administer connections between a source network region and all other destination network regions. The entries administered in the **AGL** field within each source network region represent the number of C-LANS and/or PE that Communication Manager builds into each Alternate Gatekeeper List and sends to each IP (H.323) telephone that is in that source network region. Once the numeric values are entered, Communication Manager calculates the total number of gatekeepers that are assigned for each destination region. The total AGL assignments for each region must sum to 16 or lower. If an administrator enters a value that makes the AGL assignment greater than 16, the system displays an error message.

Communication Manager tracks each of the C-LAN/PE addresses sent in the AGL to each telephone. For example, a destination network region containing 20 C-LANs can be administered to have only 3 C-LANs from that region in each AGL. As a result, Communication Manager responds to each new registration request with an AGL constructed using the administered number of C-LANs for the region, and is independent of priority, socket load, and service state.

Note:
If Communication Manager is upgrading to a newer version, the pre-upgrade AGL lists are not disturbed unless the administrator makes any changes to the new fields and enters new values.

For more information on the administration procedures for this feature, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Load balancing of IP telephones during registration

Non-TTS telephones are load balanced at registration using the Gatekeeper Confirm (GCF) message. Each region has a list of available C-LANs or PE, and Communication Manager selects the most available C-LAN within the IP (H.323) telephone's home network region. If there are C-LANs in that network region, the system uses load balancing techniques based on C-LAN priority, and available sockets. If all C-LANs are considered busy (none of the C-LANs are in service, or all C-LANS that are in service have used all the 480 available sockets), Communication Manager moves to directly connected network regions. All directly connected regions are checked beginning with network region 1. All indirect network regions are used if there were no C-LANs administered in the IP telephone's home network region, or directly connected network regions. Indirect network regions are also checked by the system beginning with network region 1.

With the enhanced implementation of the feature in Communication Manager 5.1 for load balancing for non-TTS telephones, the system gives preference to the home region C-LANs, then the direct network region C-LANs, followed by indirect network region C-LANs that are administered using the new **AGL** field on the Inter Network Region Connection Management screen. Any C-LAN within an eligible region may be assigned for load balancing. Within a specific region, the system selects the least loaded C-LAN, unless all C-LANs have reached their limit.

Load balancing for non-TTS telephones is based on the C-LAN received in gatekeeper confirm (GCF). Non-TTS phones use this C-LAN to initiate the registration request (RRQ) as well as establish a socket to Communication Manager after Registration Admission Status (RAS) has been completed.

Socket load balancing for TTS telephones occurs after registration is complete and the AGL has been formed. Communication Manager initiates socket establishment to TTS phones. Load balancing occurs across the C-LANs that were sent in the AGL, with preference being given to the C-LANs in the home region, then the directly connected regions, followed by the indirectly connected regions. Direct network regions and indirect network region C-LANs are considered as two groups. The system checks for the most available C-LAN in directly connected network regions, followed by the available C-LAN in indirectly connected network regions. Communication Manager determines that a preferred set of C-LANs is at their limit before attempting to access the next set of C-LANs.

When sending the gatekeeper list with the administrable AGL feature, the system uses each network region (home, direct, indirect) and sends a subset of the C-LANs starting at a random place in the C-LAN array.

Building the Alternate Gatekeeper Lists

Communication Manager 5.1 builds the AGL for each telephone during registration using the following parameters:

- Communication Manager builds the AGL based on the C-LANs for the home region. For non-TTS and TTS telephones, the AGL is built using a random starting point in the network region C-LAN array. Communication Manager picks the administered number of C-LANs from that initial point, based on the number of C-LANs administered in the **AGL** field of the Inter Network Region Connection Management screen.
- The system then continues building the AGL based on the list of administered directly connected regions. The order of regions is selected by round robin method, and the C-LANs are selected based on the same random algorithm that is used for selecting C-LANs from the home region.
- The system continues building the AGL for indirectly connected regions in the same way as it does for directly connected network regions.

The difference in the Communication Manager 5.1 enhancement of this feature is that the IP (H.323) telephone can now use C-LANs from all network regions as alternate gatekeepers, as long as they are connected (directly or indirectly) to the native region. The alternate gatekeepers are sent in the following order: in-region, directly connected regions, and indirectly connected regions.

Contact your Avaya representative if you have additional questions relating to how Communication Manager 5.1 builds the Alternate Gatekeeper Lists.

Application scenarios

This section describes two common issues that are addressed by the Administrable Alternate Gatekeeper List feature for Communication Manager 5.1.

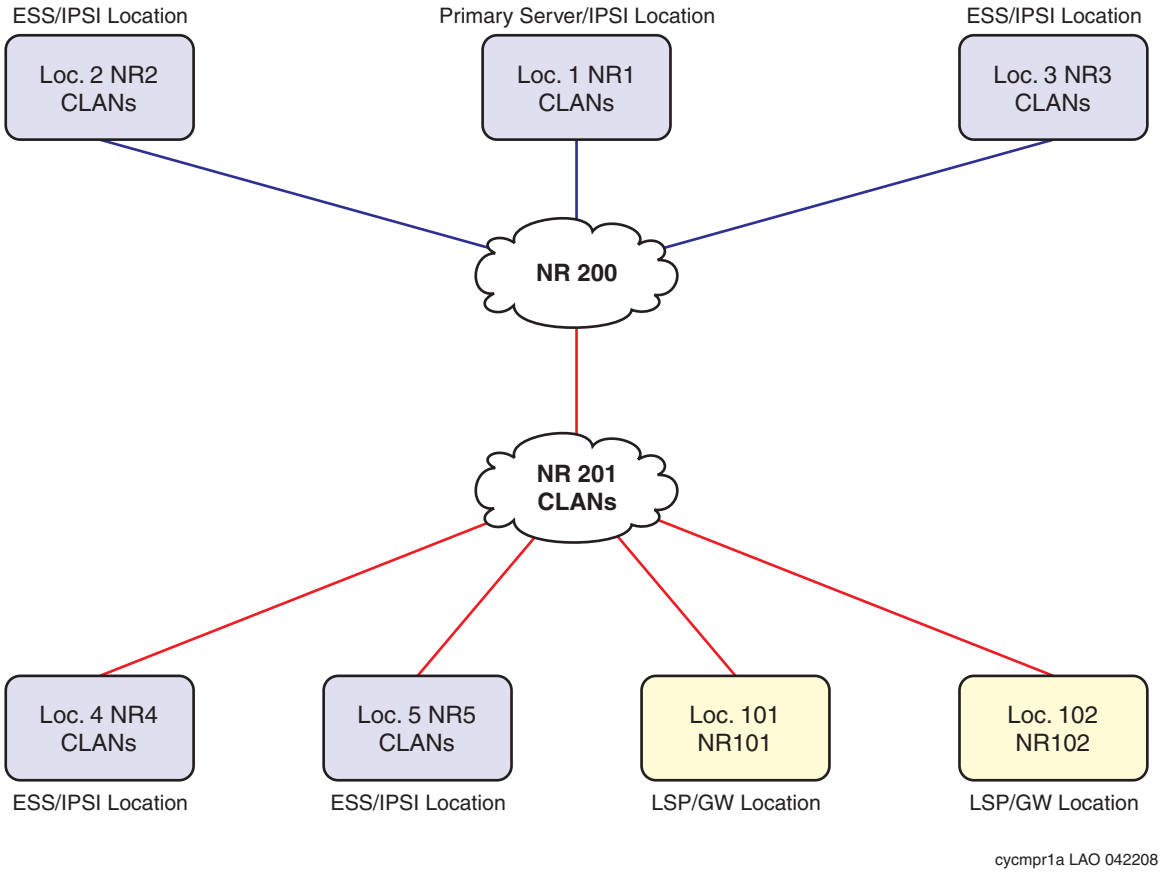
The examples are based on configurations that use WAN facilities.
In both examples, a virtual network region is assigned to the WAN to describe the WAN topology, and to implement Call Admission Control (CAC).

- Example 1 shows how you can ensure that the IP telephone does not receive unwanted C-LANs in the Alternate Gatekeeper List. It also shows the improved configuration for this issue.
- Example 2 shows how pooling C-LANs in a network region results in some IP telephones not receiving an Alternate Gatekeeper List. It also shows the improved configuration for this issue.

Example 1: Unwanted C-LANs in the AGL

Figure 10 shows how unwanted C-LANs can end up in the Alternate Gatekeeper List.

Figure 10: Unwanted C-LANs in Pre-CM 5.1 AGL



In this configuration, the IP telephones in NR1 through NR3 have C-LANs in their network regions as there are no C-LANs that are directly connected to NR200. You can optionally add a few C-LANs in NR200 to share with NR1-NR3 as they are directly connected, and NR 200 is used to consolidate traffic from NR1-NR3 for access to the WAN. Using NR 200 has the additional advantage of isolating C-LANS in each network region to IP telephones in that network region.

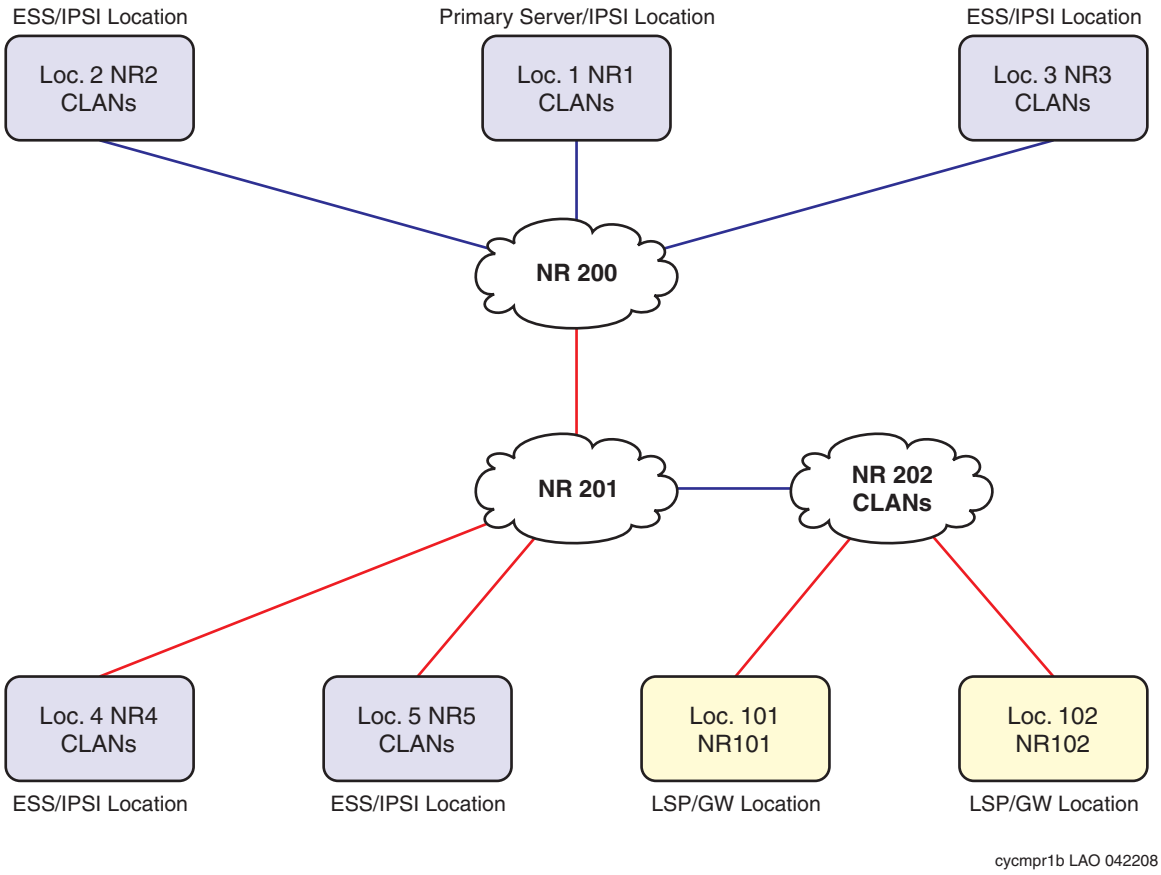
NR4 and NR5 are ESS locations, and the IP telephones in those two locations need local C-LANs that are in NR4 and NR5.

NR101 and NR102 are Gateway/LSP locations and should share pooled C-LANS. In this case, C-LANS are placed in NR201 as it is directly connected to the two NRs. Before Communication Manager 5.1 C-LANs could be in home region of the IP Phone, or in a directly connected NR.

The IP telephones in NR4 and NR5 receive C-LANs in NR201 in the AGL as that NR is directly connected. The IP telephones can end up with C-LANS in their AGL that cannot be used in a WAN failure. This can significantly delay IP telephones in NR4 and NR5 from recovering to a C-LAN that can be used in a WAN failure. This could also significantly delay IP telephones in NR4 and NR5 from recovering to an ESS.

Figure 11 shows a pre-Communication Manager 5.1 workaround that you can implement using another virtual network region.

Figure 11: Pre-CM5.1 workaround for unwanted C-LANs



In this configuration, the IP telephones in NR4 and NR5 use the ip-network-map for NR assignment. The AGL does not contain NR202 C-LANs because that NR is indirectly connected.

The IP telephones in NR101 and NR102 share C-LANs in NR202. Those C-LANs are physically located at location 1. If there are a large number of C-LANs in NR202, it could result in large AGLs and potentially delay recovery to the ESS. This workaround does not address the size of the AGL.

Figure 12 shows the improved configuration of the network region using the Administrable AGL feature for Communication Manager 5.1.

Figure 12: Improved configuration for unwanted C-LANs using the enhanced AGL feature

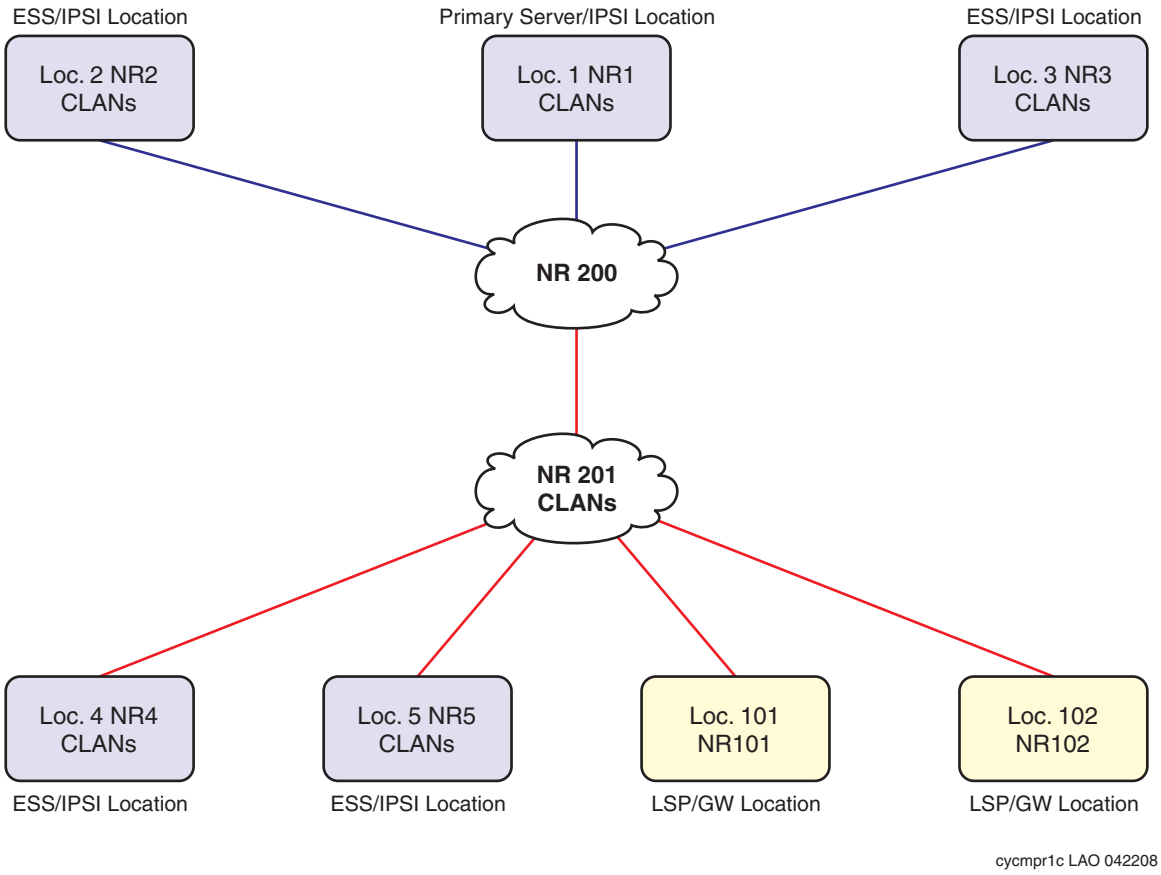


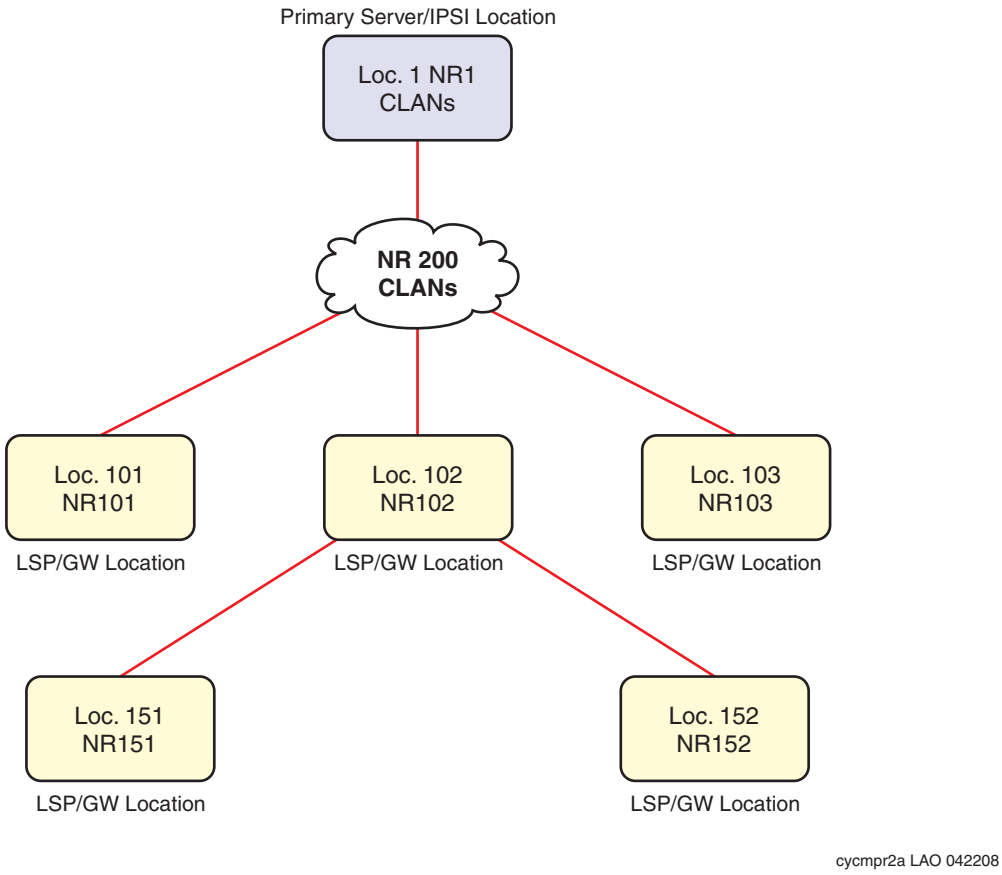
Figure 12 shows a configuration in which the IP telephones in NR4 and NR5 are administered to only use C-LANS in their native NR, and not use C-LANs in NR201. The IP telephones AGLs in NR4 and NR5 contain local C-LANs. The IP telephones in NR101 and NR102 share C-LANs in NR201. Those C-LANS are physically located at location 1. If there are a large number of C-LANs in NR201, it could result in large AGLs and potentially delay recovery to the ESS.

Additionally, with this enhancement, the administrator can specify the number of C-LANs in NR201 and therefore control the size of the AGL.

Example 2: Unable to pool C-LANS because of Network Region Connectivity

Figure 13 shows how network region connectivity issues can prevent the pooling of C-LANs.

Figure 13: Inadequate pooling of C-LANs

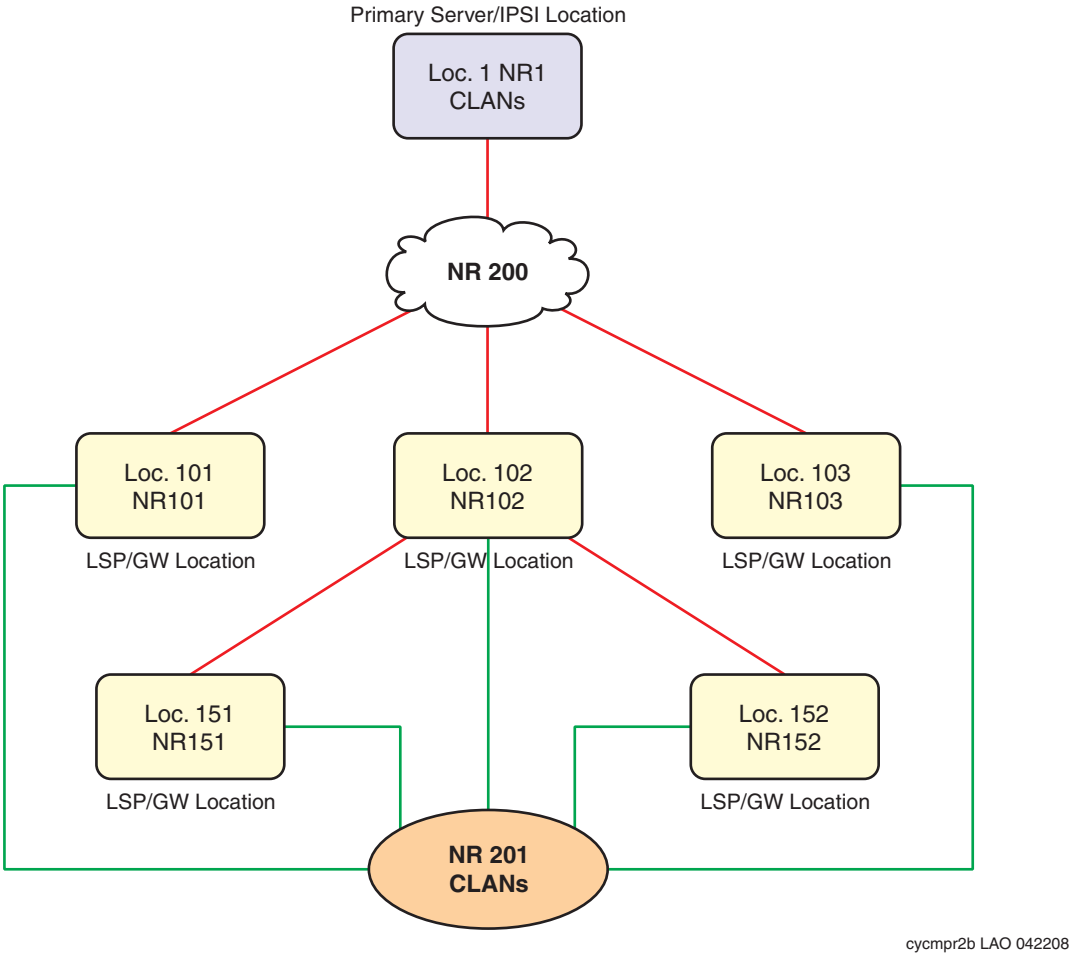


The figure shows a network configuration with numerous Gateway/LSP locations, some of which are directly connected to the WAN, and others that are indirectly connected to the WAN. All of these gateways need to share a pool of C-LANS physically located at location 1.

The IP telephones in NR151 and NR152 are not directly connected to NR200. Also, the system cannot specify the number of C-LANs in NR200 to use to control size of AGL.

Figure 14 shows the workaround that you can use in the pre-Communication Manager 5.1 implementation.

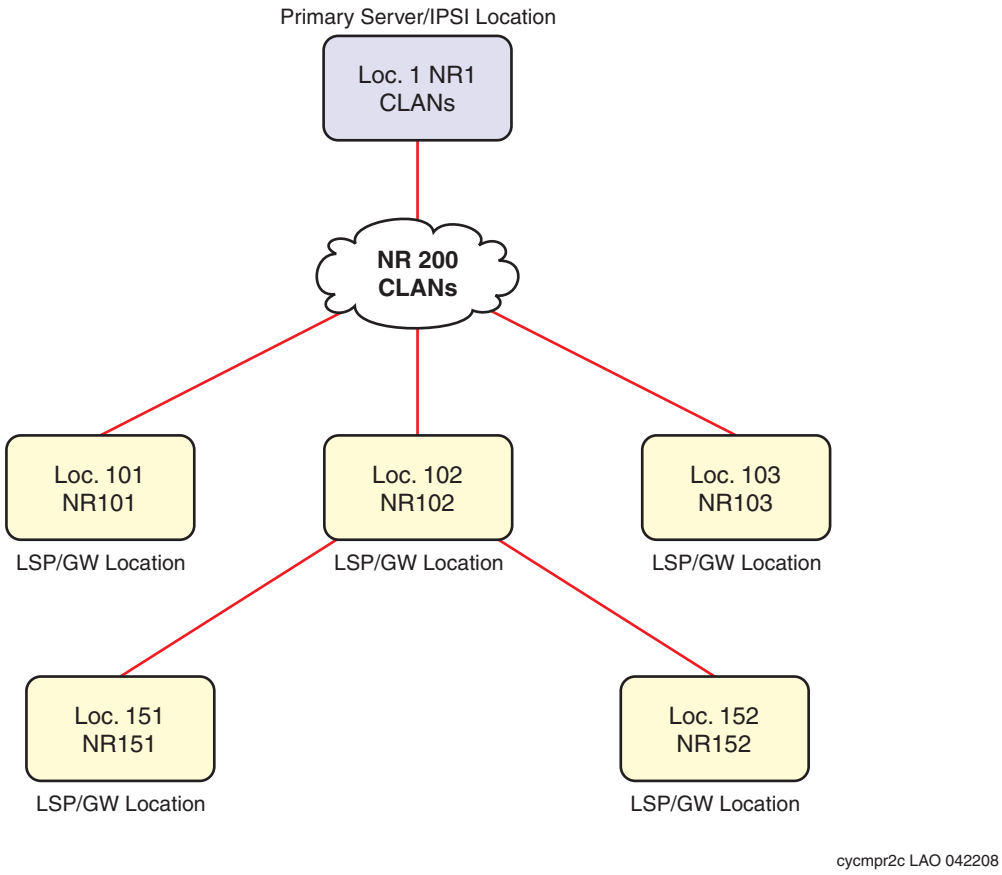
Figure 14: Pre-CM5.1 workaround for inadequate pooling of C-LANs



In this configuration, all the IP telephone network regions are directly connected to a new NR201. The AGL now contains C-LANs in NR201. But you cannot specify number of C-LANs in NR201 that you can use to control size of AGL. This configuration does not reflect the WAN topology.

Figure 15 shows the improved configuration using the Communication Manager 5.1 Administrable AGL feature.

Figure 15: Improved configuration using the CM5.1 AGL feature



All IP telephones AGL contain C-LANs in NR200, including the direct and indirect network regions. You can also specify the number of C-LANs in NR200 and control the size of the AGL.

High-level capacities

The total AGL assignments for each source region must sum to 16 or lower. Each source network region can continue to have 6 LSPs from the phone's home region to be added to the AGL. This brings the total list size to a maximum of 23 (by adding up the AGL, LSP for each region and the Survivable Gatekeeper for the station).

Considerations

If the telephone's IP address is not in one of the ranges in the ip-network-map, the AGL entries consist of the C-LANs/PE from the telephone’s homed region only. Note that administering an phone’s ip-address in a network map allows the associated AGL to work more robustly by accessing directly and indirectly connected regions, as well as the homed region.

Interactions

This section provides information about how the Administrable AGL feature for Communication Manager 5.1 interacts with other features on the system.

- It is possible to have some regions using the pre-Communication Manager 5.1 non-administrable AGL implementation, and some other regions using the new administrable AGL implementation. But you cannot have a single network region using a combination of the two methods. The AGL column can either contain numbers or **all**, but not both. The field can also contain blanks; blanks are ignored by both the old and the new implementation of this feature.
- This feature only applies to H.323 IP telephone registrations and H.323 IP telephone AGLs. The H.323 gateways also register to Communication Manager. This feature does not affect how the gateways obtain and use their own lists of gatekeepers. Also note that this feature has no impact on how IP (SIP) telephones register to SES.
- If an extension number has shared control using the server between an IP (H.323) telephone and an IP (H.323) softphone, Communication Manager displays both the AGL that was sent to the H.323 telephone and the AGL that was sent to the H.323 softphone.
- In prior releases of Communication Manager, the AGL feature only included C-LANs from the same region and from directly connected regions, or all indirectly connected regions (if there were no C-LANS in the same or directly connected regions). With this enhancement, it is now possible to explicitly administer Communication Manager to include C-LANs from indirectly connected regions as well. Also, if you administer a non-zero value in the AGL column for an indirectly connected region, it opens that indirectly connected region's C-LANs to be eligible to be used for load balancing.
- In general, when using the Communication Manager 5.1 Administrable AGL feature, C-LAN priorities should not be used. Note the following additional information:
    - For TTS telephones, the Communication Manager 5.1 enhanced feature takes into consideration priorities and C-LAN socket load, as well as C-LAN’s service state and whether the C-LANs are allowed to be used for H.323 IP telephone registration when load balancing.
    - For non-TTS phones, priorities and C-LAN socket load are taken into account when load balancing.

- For TTS and non-TTS telephones, the Communication Manager 5.1 enhanced feature does *not* take either priorities or C-LAN socket load into consideration when building the AGL.

Administrable Language Displays

Use the Administrable Language Displays feature to display telephone messages in the language of the user. Messages are available in English (the default), French, Italian, Spanish, or one user-defined language that the administrator sets up. To view messages, this feature requires user telephones with a 40-character display.

Communication Manager Release 4.0 or later also supports ISO 8859-1 encoding capability. For more information, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Detailed description of Administrable Language Displays

With the Administrable Language Displays feature, you can select one language for the static messages that telephones and attendant consoles display. The system includes approximately 900 static display messages, such as "Transfer complete." You can select from English, French, Italian, Spanish, a user-defined language, or Unicode.

The following types of information are pre-translated for display in English, French, Italian, and Spanish. If you select **user-defined**, you must enter a translation for each message.

- Automatic Wakeup
- Adjunct Switch Applications Interface (ASAI)
- Busy Verification of Terminals and Trunks
- Call Appearance buttons
- Call Detail Recording (CDR)
- Call Progress Feedback Displays
- Class of Restriction (COR)
- Date-Time Mode
- Days of the Week
- Months of the Year
- Do Not Disturb
- Enhanced Abbreviated Dialing
- Integrated Directory
- ISDN
- Leave Word Calling

- Malicious Call Trace
- Emergency Access to Attendant
- Queue Status
- Miscellaneous Call Identifiers
- Party Identifiers
- Property Management Interface
- Security Violation Notification (SVN)
- Stored numbers
- Station hunting
- Time-of-Day Routing
- Transfer messages

Administering Unicode display

To use Unicode display languages, you must have the appropriate Avaya Unicode Message files loaded on Communication Manager. These files are named *avaya_unicode.txt* (standard phone messages), *custom_unicode.txt* (posted messages and system labels), *avaya_user-defined.txt* (standard phone messages using Eurofont), and *custom_user-defined.txt* (posted messages and system labels using Eurofont).

To use the Phone Message files *avaya_unicode.txt* and *custom_unicode.txt*, you must have Unicode-capable stations, such as the 4610SW, 4620SW, 4621SW, 4625SW, and Avaya Softphone R5.0. Only Unicode-capable stations have the script (font) support that is required to match the scripts that the Unicode Phone Message file uses. To use the user-defined messages files *avaya_user-defined.txt* and *custom_user-defined.txt* you must use an Avaya digital phone that supports Eurofont or Kanafont.

For Communication Manager 2.2 and later, the following languages are available using Unicode display:

- Chinese
- Czech
- Danish
- Dutch
- German
- Hebrew
- Hungarian
- Icelandic

- Italian
- Japanese
- Korean
- Macedonian
- Polish
- Romanian
- Russian
- Servian
- Slovak
- Swedish
- Ukranian

Obtaining and installing Phone Message files

A Unicode Message file for each supported language is available in a downloadable ZIP file on the Avaya support Web site (http://www.avaya.com/unicode). You can also create a new translation or edit an existing translation with the Avaya Message Editing Tool (AMET) (http://support.avaya.com/amet). Additional languages are periodically becoming available, so check this site often for the most up-to-date message files.

Note:
Refer to the *Communication Manager Messages Job Aid* for details on the following procedures.

To administer Unicode display:

1. Download the appropriate Unicode message file to your PC. For an existing translation, download the desired language from http://www.avaya.com/unicode.
2. If necessary, create a new translation, or modify an existing translation, using the Avaya Message Editing Tool (AMET), available at http://support.avaya.com/amet.

   Note:
   Only the Avaya Message Editing Tool (AMET) can be used for translation edits, using any other editor will not update the Phone Message File correctly and such files will fail to install. See the *Avaya Message Editing Tool (AMET) Job Aid* in the Generic Phone Message Package file for more details on using AMET.
3. Transfer the Phone Message file to an Avaya S8*XXX* server that is running Communication Manager 2.2 or later, using the Avaya Web pages, the Avaya Installation Wizard, or ftp.

4. Install Phone Message files with the Avaya Install Web Page. The Avaya Installation Wizard only supports install of Unicode Phone Message files. Note that the Installation Wizard is the same wizard that you use to transfer Phone Message files to an Avaya S8*XXX* server that is running Communication Manager 2.2 or later.
5. After you install *avaya_unicode.txt* or *avaya_user-defined.txt*, you must do a reset 4 to load the file in to Communication Manager memory. Note that a reset 4 is *not* required to load the files *custom_unicode.txt* and *custom-defined.txt*.
6. Set the **Display Language** field on the Station screen to **unicode**. Note that the keyword **unicode** only appears if a Unicode-capable telephone is entered in the Station screen **Type** field. To use a user-defined file, set the **Display Language** field on the Station screen to **user-defined**.

Note:
There is no uninstall option for Phone Message files. You can reload a new Phone Message file. This overwrites existing Phone Message files.

Checking the status of Phone Message file loads

To verify that a Unicode Phone Message file is loaded correctly, run **`status station xxxx`** on any administered station. If the Unicode Phone Message file is loaded correctly, the **Display Messages Scripts** field on the second page contains the scripts that are in this file.The General Status screen for stations contains three Unicode script-related fields. To access the General Status screen, type **`status station xxxx`**, where ***xxxx*** is the extension of the station. The General Status screen appears. Click **Next** to display page 2 of the screen:

Figure 16: General Status screen

```
 status station nnnn                                          page 2 of x

                                GENERAL STATUS

CONNECTED STATION INFORMATION
               Part ID Number: unavailable
                Serial Number: unavailable
          Station Lock Active? No

UNICODE DISPLAY INFORMATION
          Native Name Scripts: 0x00000007:Latn;Lat1;LatA
     Display Messages Scripts: 0x04000007:Latn;Lat1;LatA;Jpan
    Station Supported Scripts: 0x7c000007:Latn;Lat1;LatA;Jpan;Chis;Chit;Korn
```

"Scripts" are a collection of symbols used to represent text in one or more writing systems. The three script fields shown in the **UNICODE DISPLAY INFORMATION** section are as follows:

Native Name Scripts: Scripts supported in the Unicode station name.

Display Messages Scripts: The scripts used in the Unicode Display Language.

Station Supported Scripts: The scripts supported in the IP station that is registered to an extension.

Unicode "Native Name" support

Communication Manager supports Unicode for the "Name" associated with Vector Directory Numbers (VDNs), trunk groups, hunt groups, agent login id, vector names, station names, Invalid Number Dialed Display (Feature-Related System Parameters screen) and Restricted Number Dialed Display (Feature-Related System Parameters screen). The Unicode Name (also referred to as *Native Name* and *Name 2)* fields are hidden fields that are associated with the name fields you administer on the respective screens for each. These fields can only be administered using Avaya Site Administration (ASA) or MultiSite Administrator (MSA).

- The Unicode VDN Name is associated with the name administered in the **Name** field on the Vector Directory screen. You must use MSA.
- The Unicode Trunk Group Name is associated with the name administered in the **Group Name** field on the Trunk Group screen. You must use MSA.
- The Unicode Hunt Group Name is associated with the name administered in the **Group Name** field on the Hunt Group screen. You must use MSA.
- The Unicode Station Name is associated with the name administered in the **Name** field on the Station screen. You must use ASA or MSA.

Administering Administrable Language Displays

The following steps are part of the administration process for the Administrable Language Displays feature:

- Setting the display language
- Entering translations for a user-defined language

This section describes:

- Any prerequisites for administering the Administrable Language Displays feature
- The screens that are required to administer the Administrable Language Displays feature
- Complete administration procedures for the Administrable Language Displays feature

Prerequisites for administering Administrable Language Displays

You must complete the following actions before you can administer the Administrable Language Displays feature:

- Ensure that the **Display Character Set** field on the System Parameters Country-Options screen is set to the character type that you want to display. Avaya sets this field. If the **Display Character Set** field is not set to the character type that you want to display, contact your Avaya representative.
- Ensure that the type of telephone that your company uses has a 40-character display, and supports the characters that you want to display. Each character set requires specific telephones. Contact your Avaya representative for details.
- For Unicode display, ensure that the Communication Manager telephone messages for the Unicode display language are loaded. The file *avaya_unicode.txt* contains Communication Manager telephone messages. The file *custom_unicode.txt* contains Communication Manager posted messages and system labels. You can load these files when you upgrade or install the system. You can also download these files at any time from the Avaya support Web site http://www.avaya.com/support.

  The Avaya Excel Translation Editor for creating Unicode translations requires Microsoft Excel 2000 or above.
- To support Unicode on the 4620SW IP telephone, you must:
  - Install the appropriate version of firmware on the telephone
  - Set the language that you desire

  For more information on administering telephones, see the *4600 Series IP Telephone R2.0 LAN Administrator's Guide* (555-233-507), and the *4620/4620SW IP Telephone R2.0 User's Guide* (555-233-781).

Screens for administering Administrable Language Displays

Screen Name	Purpose	Fields
System Parameters - Country Options	Ensure that the appropriate character set is enabled for the language that you want to use.	**Display Character Set**
Attendant Console	Set the display language.	**Display Language**
Language Translations	Enter user-defined translations of messages.	**Translation**

Setting the display language

To set the display language:

1. Type **change attendant *n***, where ***n*** is the number of the attendant console that you want to change. Press **Enter**.

   The system displays the Attendant Console screen (Figure 17: Attendant Console screen on page 145).

Figure 17: Attendant Console screen

```
change attendant 1                                          Page   1 of   3

                            ATTENDANT CONSOLE 1

        Type: console           Name: Gunther
   Extension: 1000             Group: 1                Auto Answer: none
Console Type: principal           TN: 1                Data Module? n
        Port: 01C1106             COR: 1          Disp Client Redir? n
                                  COS: 1           Display Language: english


DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS (Trunk Access Codes)
    Local Remote            Local Remote              Local Remote
 1: 9                    5:                        9:
 2: 82                   6:                       10:
 3:                      7:                       11:
 4:                      8:                       12:

HUNDREDS SELECT BUTTON ASSIGNMENTS
 1:           5:           9:           13:          17:
 2:           6:          10:           14:          18:
 3:           7:          11:           15:          19:
 4:           8:          12:           16:          20:
```

2. In the **Display Language** field, type the name of the display language that you want to use.

   Note:
   The Display Language value **unicode** is available only for station type 4620SW or 4610SW.

3. Press **Enter** to save your changes.

Entering translations for a user-defined language

To enter translations for a user-defined language:

1. Type **change attendant** ***n***, where ***n*** is the number of the attendant console that you want to change. Press **Enter**.

   The system displays the Attendant Console screen (Figure 17: Attendant Console screen on page 145).

2. In the **Display Language** field, type **user-defined**.
3. Press **Enter** to save your changes.
4. Type **change display-messages** ***n***, where ***n*** is the message for which you want to translate the display language. Click **help** to view the messages that you can choose to translate. Press **Enter**.

   The system displays the Language Translations screen for the type of message that you want to translate. (Figure 18: Language Translations screen on page 146). This example shows the screen for message type Transfer-conference.

Figure 18: Language Translations screen

```
change display-messages transfer-conference                    Page 1 of 3

                              Language Translations

 1.     English: Transfer completed.
    Translation: abtretung abgeschlossen
```

5. In the **Translation** field, type the translation of the message in the user-defined language. In this example, the translation to the German language is **abtretung abgeschlossen**.
6. Press **Enter** to save your changes.

For more information on telephone displays, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Considerations for Administrable Language Displays

This section provides information about how the Administrable Language Displays feature behaves in certain circumstances.

Note:
The considerations stated here apply only to the ISO 8859-1 encoding capability.

- The ASCII (0x00 – 0x7F) does not require any conversion.
- The range 0x80 – 0x9F is not supported when **Display Character Set** on the System Parameters Country-Options screen has the value **Roman**.
- If CID is sent through a tandem server, the CID could display incorrectly on the server where the call terminates if that server does not support 8859-1/Eurofont conversion, or if the QSIG trunk does not have the conversion feature enabled.
- If Communication Manager receives a name in the simple name form from another vendor and if that name contains accented characters, the name will not display correctly. This is because Communication Manager expects a simple name to use the Eurofont character set.
- It is a known issue that this design does not properly handle names received in the extended name form in character sets other than 8859-1. For such cases, the characters outside the ASCII range will be improperly mapped to Eurofont resulting in an incorrect name display.

Troubleshooting Administrable Language Displays

This section lists the known or common problems that users might experience with the Administrable Language Displays feature.

Problem	Possible cause	Action
The characters that appear on the display are not what you entered.	This feature is case sensitive.	Check the table to ensure that you entered the characters in the correct case.
You entered a lowercase "c", but an asterisk (*) appears on the display instead.	Lowercase c has a specific meaning in Communication Manager. Therefore you cannot map c to any other character. An asterisk (*) appears in its place.	Use a different letter for this character mapping.
You entered ~-> or ~<- but nothing appears on the display.	These characters do not exist as single keys on the standard US English keyboard. Therefore the system is not programmed to handle these characters.	Check the model of the keyboard that you are using.

Problem	Possible cause	Action
Enhanced display characters appear in fields that you did not update.	If an existing display field contains a tilde (~) that is followed by Roman characters, and you update and submit that screen, that field displays the enhanced character set.	Remove the existing tilde before you submit the screen.
The terminal displays nothing at all.	Some unsupported terminals do not display anything if a special character is presented.	Check the model of the display terminal that you are using.
You entered a character with a descender and part of the descender appears cut off in the display.	Some of the unused characters in Group2a have descenders that do not appear entirely within the display area. These characters are not included in the character map.	Use Group1 equivalents for the letters g, j, p, q, and y.

Making Standard Telephone Features easier to use

Display messages are provided in additional languages for the following standard telephone features:

- Station Security Code
- Personal Station Access
- Call Pickup
- Station Lock
- Extension to Cellular
- Call Forwarding
- Call Coverage
- Call Park

Note:

This feature is available for all platforms that support Communication Manager Release 5.2 and later. This feature does not apply to stations that act as attendant consoles. At present, this feature does not support IP (SIP) telephones.

An administrator must switch on this feature by using the Feature Related System Parameters screen before the messages are displayed on the telephone, as shown in the Figure 19 and Figure 20:

Figure 19: Feature Related System Parameters Screen

```
change system-parameters features                              Page 9 of x
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: ____________
  CPN/ANI/ICLID Replacement for Unavailable Calls: ____________

DISPLAY TEXT
    Identity When Bridging: principal
     User Guidance Display? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code: ______
          International Access Code: ______

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200

n(o)          y(es)
```

User Guidance Display?

Valid entries	Usage
y/n	To enable the feature, select **y**. To disable the feature, select **n**. The default value is **n**.

Figure 20: Feature-Related System Parameters Screen

```
change system-parameters features                              Page 9 of x
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: ____________
  CPN/ANI/ICLID Replacement for Unavailable Calls: ____________

DISPLAY TEXT
    Identity When Bridging: principal
     User Guidance Display? x

INTERNATIONAL CALL ROUTING PARAMETERS
                Local Country Code: ______
          International Access Code: ______

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200

"x" is an invalid entry; please press HELP
```

User Guidance Display?

Valid entries	Usage
y/n	To enable the feature, select **y**. To disable the feature, select **n**. The default value is **n**. **x** is an invalid entry.

Note:

An example of the display guidance is shown for Station Security Code (Display Guidance) on page 1520. This example is also applicable for features like Personal Station Access, Call Pickup, Station Lock, Extension to Cellular, Call Forwarding, Call Coverage, and Call Park.

Administration Change Notification

Use the Administration Change Notification feature to notify adjunct systems when administration data on Communication Manager is changed. These notifications keep a client application that is running on an adjunct, such as Enterprise Directory Gateway, synchronized with Communication Manager.

Administration Change Notification allows Communication Manager to communicate with the Avaya Directory Enabled Management (DEM) client. This feature provides you with real-time, integrated, directory-based, read-write access to Communication Manager administration data. This access is based on rules that you define. With Administration Change Notification, you can subscribe to notifications whenever the administration data changes in Communication Manager. This feature also provides real-time updates whenever the administration data changes in a particular object, such as a telephone.

Detailed description of Administration Change Notification

Use the Administration Change Notification feature to track changes that are made through the System Access Terminal (SAT), INADS port, a Property Management System (PMS), a Call Management System (CMS), Avaya Site Administration, Avaya Network Administration, or Avaya Directory Gateway. The Administration Change Notification feature also tracks any changes that are made through a telephone interface, such as Terminal Translation Initialization (TTI), Personal Station Access (PSA), and Terminal Self Administration.

Communication Manager only notifies the adjunct about a change to a data object. To obtain details about the change, the adjunct must request this information from the server over a separate link.

Administering Administration Change Notification

The following steps are part of the administration process for the Administration Change Notification feature:

- Initiating Administration Change Notification

This section describes:

- Any prerequisites for administering the Administration Change Notification feature
- The screens that are required to administer the Administration Change Notification feature

- Complete administration procedures for the Administration Change Notification feature

Prerequisites for administering Administration Change Notification

You must complete the following actions before you can administer the Administration Change Notification feature:

- None

Screens for administering Administration Change Notification

Screen Name	Purpose	Fields
Administration Changes	View changes to administration data in Communication Manager.	All

Initiating Administration Change Notification

To initiate Administration Change Notification:

1. From the client application, type **`notify history`**. Press **Enter**.

   The system displays the Administration Changes screen (Figure 21: Administration Changes screen on page 152).

Figure 21: Administration Changes screen

```
notify history

                              ADMINISTRATION CHANGES

Date    Time     Login    Actn    Object      Qualifier

3/16    14:21    Craft    Logn
```

Communication Manager continues to send change notification over the Operations Support System Interface (OSSI) link until you cancel the command.

Administration Without Hardware

Use the Administration Without Hardware (AWOH) feature to administer telephones that are not yet physically on the system. Like administration with hardware, the system preserves all features that the user has activated, such as Call Forwarding and Send All Calls, when you move a telephone. This greatly speeds the process of setting up and making changes to telephones on your system.

Detailed description of Administration Without Hardware

This section provides a detailed description of the Administration Without Hardware (AWOH) feature.

With AWOH you can enter telephone translations without assigning ports. Therefore, AWOH streamlines system initialization, major additions, and rearrangements or changes You can add or change a Station screen, and you can store duplicated telephones without specifying a port location.

Note:

A new command **`list configuration circuit-pack <board code>`**, where ***`<board code>`*** is the code on the faceplate of the circuit pack allows the administrator to list all the requested circuit packs in the system that are plugged in. Those circuit packs that are logically administered (Administration Without Hardware - AWOH) or are unplugged are not listed. Use this command to list the circuit packs that require firmware downloads.

Physical characteristics of an AWOH telephone

AWOH telephones cannot generate alarms or errors, because the physical telephones or data terminals are not associated with a Station screen. Neither the system nor other telephones or data terminals can affect the lamp or the alerting tones of an AWOH telephone. If a user presses a button on telephone or a data terminal that does not have an associated Station screen, the action has not effect on system operation.

User-activated features

When someone moves a telephone or a data terminal, the user-activated features, such as Call Forwarding and Send All Calls, remain active. Any action that changes the lamps or the status of the telephone is reflected when the telephone or the data terminal is again associated with a Station screen.

Association and disassociation

Telephone users, data-terminal users, and technicians can disassociate telephone translations from the current terminal port, and then associate the telephone translations with another terminal port. Users use the Personal Station Access (PSA) feature to disassociate and associate telephones. Technicians use the Terminal Translation Initialization (TTI) feature to disassociate and associate telephones.

An AWOH telephone is considered to be disassociated when no hardware port is assigned to the telephone. To indicate that no hardware is associated with a telephone, type **x** in the **Port** field of the appropriate screen. When the port is assigned later, the AWOH telephone is considered to be associated.

Phantom extensions

You can use phantom extensions to provide call coverage, including CM Messaging coverage, for users who do not have telephones or data terminals that are physically associated on the server.

You can also use phantom extensions for the automatic call distribution (ACD) Dialed Number Identification Service (DNIS). With ACD DNIS, you can administer a phantom extension on the switch for each type of call that ACD agents need to identify.

To use ACD DNIS, either a user with console permissions forwards the phantom extension to an ACD split, or the coverage path of the phantom extension includes an ACD split. The **Name** field for the phantom extension identifies the service that the caller wants. The agent then uses this information to address the caller properly.

Administering Administration Without Hardware

The following steps are part of the administration process for the Administration Without Hardware (AWOH) feature:

- Assigning AWOH for a hunt group queue
- Assigning AWOH to a telephone
- Assigning AWOH to an attendant console
- Assigning AWOH to a data module

This section describes:

- Any prerequisites for administering the Administration Without Hardware feature
- The screens that you use to administer the Administration Without Hardware feature
- Complete administration procedures for the Administration Without Hardware feature

Screens for administering Administration Without Hardware

Screen name	Purpose	Fields
Attendant Console	Assign a port to the attendant console.	**Port**
Data Module	Assign a port to the data module.	**Port**
Hunt Group	Assign port information for a queue.	• **Calls Warning Port** • **Time Warning Port**
Station	Assign a port to a telephone.	**Port**

Assigning AWOH for a hunt group queue

To assign AWOH for a hunt group queue:

1. Type **`change hunt-group n`**, where ***n*** is the number of the hunt group to which you want to assign AWOH. Press **Enter.**

   The system displays the Hunt Group screen (Figure 22: Hunt Group screen on page 156).

Figure 22: Hunt Group screen

```
change hunt-group 1                                          Page 1 of X
                                    HUNT GROUP

            Group Number: ___                                    ACD? n
              Group Name: _____________________________        Queue? y
         Group Extension: ____                                 Vector? y
              Group Type:
                      TN:
                     COR:                                MM Early Answer?
           Security Code: ____
     ISDN Caller Display: ________

            Queue Length: ___
 Calls Warning Threshold:      Port: x      Extension: ____
  Time Warning Threshold:      Port: x      Extension: ____
```

2. In the **Calls Warning Port** field, type **x**.

   Note that the system displays the **Calls Warning Port** field if the **Queue** field is set to **y**.

3. When you type **x** in the In the **Calls Warning Port** field, the system displays an **Extension** field.

   In the **Extension** field, type an extension that a technician can use, along with TTI, to assign a port number from the actual port. When a technician or an administrator assigns a port number, the system removes the extension, and the extension becomes unassigned. An administrator uses the **`change hunt-group`** command to assign the port number.

4. In the **Time Warning Port** field, type **x**.

   Note that the system displays the **Time Warning Port** field if the **Queue** field is set to **y**.

5. When you type **x** in the In the **Time Warning Port** field, the system displays an **Extension** field.

   In the **Extension** field, type an extension that a technician can use, with TTI, to assign a port number from the actual port. When a technician or an administrator assigns a port number, the system removes the extension, and the extension becomes unassigned. An administrator uses the **`change hunt-group`** command to assign the port number.

6. Press **Enter** to save your changes.

Assigning AWOH to a telephone

To assign AWOH to a telephone:

1. Type **change station *n***, where ***n*** is the number of the extension to which you want to assign AWOH. Press **Enter.**

   The system displays the Station screen (Figure 23: Station screen on page 157).

Figure 23: Station screen

```
change station 1014                                          Page 1 of X
                              STATION

Extension: 1014               Lock Messages? n                    BCC: 0
     Type:                    Security Code:                       TN: 1
     Port:                  Coverage Path 1:                      COR: 1
     Name:                  Coverage Path 2:                      COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                          Message Lamp Ext: 1014
           Speakerphone: 2-way                   Mute button enabled? y
       Display Language? English                    Expansion Module?
                  Model:
                                                  Media Complex Ext:
                                                       IP Softphone? y
                                                Remote Office Phone? y
```

2. In the **Port** field, type **x**.
3. Press **Enter** to save your changes.

Assigning AWOH to an attendant console

To assign AWOH to an attendant console:

1. Type **change attendant *n***, where ***n*** is the number of the attendant console to which you want to assign AWOH. Press **Enter.**

   The system displays the Attendant Console screen (Figure 24: Attendant Console screen on page 158).

Figure 24: Attendant Console screen

```
change attendant 1                                          Page   1 of   3
                            ATTENDANT CONSOLE 1

         Type: console           Name: 27 character attd cons name
    Extension: 1000             Group: 1                Auto Answer: none
 Console Type: principal           TN: 1                Data Module? y
         Port: 01C1106             COR: 1          Disp Client Redir? n
Security Code:                     COS: 1           Display Language: english
                                                   H.320 Conversion? n

DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS (Trunk Access Codes)
    Local Remote           Local Remote             Local Remote
 1: 9                   5:                       9:
 2: 82                  6:                      10:
 3:                     7:                      11:
 4:                     8:                      12:

HUNDREDS SELECT BUTTON ASSIGNMENTS
 1:           5:            9:           13:           17:
 2:           6:           10:           14:           18:
 3:           7:           11:           15:           19:
 4:           8:           12:           16:           20:
```

2. In the **Port** field, type **x**.
3. Press **Enter** to save your changes.

Assigning AWOH to a data module

To assign AWOH to a data module:

1. Type **change data-module *n***, where ***n*** is the number of the data module to which you want to assign AWOH. Press **Enter.**

   The system displays the Data Module screen (Figure 25: Data Module screen on page 159).

Figure 25: Data Module screen

```
add data-module next                                          Page   1 of   1
                                DATA MODULE

  Data Extension: 502             Name:                              BCC: 2
            Type: pdm              COS: 1         Remote Loop-Around Test? n
            Port:                  COR: 1           Secondary data module? n
             ITC: restricted        TN: 1                    Connected To: dte


ABBREVIATED DIALING
  List1:

SPECIAL DIALING OPTION:



ASSIGNED MEMBER ( Station with a data extension button for this data module )

         Ext      Name (first 26 characters)
     1:
```

2. In the **Port** field, type **x**.
3. Press **Enter** to save your changes.

Reports for Administration Without Hardware

The following reports provide information about the Administration Without Hardware feature:

- None

Considerations for Administration Without Hardware

This section provides information about how the Administration Without Hardware feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Administration Without Hardware under all conditions. The following considerations apply to Administration Without Hardware:

- None

Interactions for Administration Without Hardware

This section provides information about how the Administration Without Hardware (AWOH) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of AWOH in any feature configuration.

- Association and disassociation interactions
  - Attendant

    An attendant cannot disassociate the attendant telephone if the attendant has a call in a queue, a call on hold, or a call that is active. An attendant cannot dissociate the attendant telephone under those conditions, even if the attendant is in Position Available mode.
  - Attendant Night Service

    A night service telephone cannot be removed while the telephone is in night service. See the "Night Service" feature for more information.
  - Attendant Release Loop Operation

    The system reclassifies calls as attendant group calls if the attendant holds the calls with the release loop operation, and if the attendant disassociates the attendant telephone before the attendant timed-reminder interval expires.
  - Automatic Callback

    If a telephone becomes disassociated while another telephone has automatic callback active for the disassociated telephone, the automatic callback light turns off. The callback sequence does not occur for the telephone that has automatic callback active.
  - Bridged Call Appearance

    If a telephone has a bridged call appearance of an off-hook telephone, the first telephone can disassociate at any time, and not disrupt a call that is in progress on the bridge.

    If a telephone with a bridged call appearance associates itself while the extension for the bridged appearance is on a call, the associated telephone can join the call.

    You cannot disassociate a telephone from a bridged call appearance. You must disassociate a telephone from the port on which the telephone resides.
  - Call Coverage

    If an AWOH telephone disassociates while Send All Calls or Go to Coverage is active, both features remain active.

- Call Coverage Answer Group

  If a technician or an administrator associates a telephone, the telephone cannot join calls that are in progress at the call-coverage answer group. The telephone can join subsequent calls.

- Call Forward

  A telephone can disassociate while Call Forwarding is active.

  If a Call Forwarding destination disassociates, Call Forwarding to that extension remains active.

- Call Park

  If a line appearance is available, a user can disassociate while a call to that telephone is parked. The user can then retrieve the call from another telephone.

- Call Pickup

  If a line appearance is available, a member of a Call Pickup group can disassociate a telephone at any time.

  If a call is in progress to any extension in a pickup group, any member of the group can disassociate or associate a telephone. The pickup group member who dissociates or associates a telephone does not join the group for the call in progress. The member can participate in subsequent calls.

- Customer-premises equipment (CPE) Alarm

  If a telephone that is administered with a CPE alarm becomes associated with a port while an alarm is active, the telephone receives the alarm when the telephone is associated.

- Hunt Group with Uniform Call Distribution (UCD) and Direct Department Calling (DDC)

  If a technician or an administrator associates a telephone, the telephone cannot join calls that are in progress at the hunt group. The telephone can join subsequent calls.

- Hold

  A telephone user can place a call on hold. The user can then disassociate the telephone, associate the telephone, and retrieve the call that the user placed on hold.

- Intercom Group - Auto/Dial

  See the "Data Call Setup" feature for more information.

- Message Light

  You do not need to delete messages before you dissociate a telephone. If a telephone receives messages while the telephone is disassociated, the system updates the message light when someone associates the telephone.

- Send All Calls

  Send All Calls remains active when a telephone is disassociated.

- Station-to-Station Call

  You cannot disassociate a telephone while someone is active on a call at the telephone.

- Terminating Extension Group (TEG)

  If a technician or an administrator associates a telephone, the telephone cannot join calls that are in progress at the TEG. The telephone can join subsequent calls.

- Transfer

  After user A successfully uses the Transfer feature to connect a caller with user B, user A can dissociate the telephone, The system processes the call between the caller and the transferred-to user as a station-to-station call.

- Trunk Group Night Service

  You disassociate a night service destination that is a telephone the same way that you disassociate a telephone that is not a night service destination. See the "Data Call Setup" feature for more information.

  You disassociate a night service destination that is an attendant the same way that you disassociate an attendant that is not a night service destination. See the "Attendant" feature for more information.

- Attendant interactions
  - Attendant Group

    If all attendants of a group use AWOH consoles, internal callers receive ringback tone indefinitely. Attendant AWOH consoles operate the same way as AWOH telephones in group interactions.

  - Attendant Override

    When an attendant activates Attendant Override, the attendant hears a busy signal for calls to AWOH extensions, and the attendant bypasses Call Coverage for the extensions.

  - Attendant Return Call

    If the attendant extends a call to a telephone, and then the attendant dissociates the attendant telephone before the system returns the call to the attendant, the system reclassifies the call. The system reclassifies the call as an attendant group call, and routes the call to an attendant group.

  - Emergency Access to Attendant

    A caller receives a busy signal if:

    - The Emergency Access feature to the attendant is active.
    - All attendants use AWOH consoles.
    - No backup extension is administered.
    - The backup extension is also an AWOH extension.

- Interposition Calling, Attendant to Attendant

  A caller receives the intercept tone for a call to an attendant who has an AWOH console.

- Night Station Service

  A caller receives a busy signal if the attendant activates Night Station Service, and the night service endpoint in an AWOH extension.

- Serial Calling

  With a serial call, the attendant is not in a busy state after the attendant releases a call. Because the attendant is not in a busy state, the attendant can disassociate the attendant telephone.

  If the attendant extends a call to a telephone, and then the attendant dissociates before the system returns the call to the attendant, the system reclassifies the call. The system reclassifies the call as an attendant group call, and routes the call to an attendant group.

  When an attendant attempts to extend a call to an AWOH extension, the attendant hears a busy signal.

- Data Modules

  Users can use the following methods to associate and disassociate data modules:

  - Data-terminal dialing
  - Telephone dialing
  - Other devices

  The devices include the use of a default set type to associate, and then remove the default set type, and replace the default set type with the proper data endpoint.

  Because digital-terminal data modules (DTDMs) reside on some telephone types, the port is automatically inherited from the host telephone. The DTDM receives a port identification when the telephone associates or disassociates.

  - Administered Connections

    If you administer a connection without hardware translation, the system attempts to establish a connection only when both endpoints are associated with hardware translation.

    You disassociate an administered connection when you type **x** in the **Port** field on the Data Module screen. A technician uses Terminal Translation Initialization (TTI) to disassociate an administered connection.

  - Hunt Group - Uniform Call Distribution (UCD) and Direct Departmental Calling (DDC)

    See the "Call Coverage" feature for more information.

  - Terminal-to-Data Module Call

    See the "Data Call Setup" feature for more information.

- Transfer

  See the "Transfer" feature for more information.

- Data-terminal interactions
  - Administered Connections

    An administered connection endpoint can be an AWOH extension.
  - Data Call Setup
    - Data Terminal Dialing

      A keyboard-dialed call that terminates to a data endpoint that is an AWOH telephone, causes a BUSY message on the screen. A busy signal indicates that the terminal is in use, out of service, or AWOH.
    - Telephone Dialing

      See the "Data Call Setup" feature for more information.
  - Hunt-Group (UCD and DDC)

    See the "Call Coverage" feature for more information.
  - Incoming Destination

    If the incoming destination is an AWOH extension, the caller hears ringback tone from the central office (CO). The system routes incoming calls based on features that are active for the extension. These features include, for example, Call Forwarding and Call Coverage.
  - Terminal-to-Data Module Call

    If a data endpoint is an AWOH telephone, the caller either sees a BUSY message on the screen or hears a busy signal, depending on the originating hardware. See the "Data Call Setup" feature for more information.
- Telephone interactions
  - Abbreviated Dialing

    AWOH does not change any aspect of the Abbreviated Dialing feature.

    A telephone that has Abbreviated Dialing active, and then becomes disassociated, retains the abbreviated dialing list entries.
  - Automatic Call Distribution

    A user cannot log an AWOH telephone into an Automatic Call Distribution (ACD) split. The user can log on directly or use a Bridged Call Appearance.
  - Automatic Callback

    A user cannot activate the Automatic Callback feature for a call to an AWOH extension. If a user attempts to use the Automatic Callback feature for a call to an AWOH extension, the system sends the reorder tone to the user.

- Bridged Call Appearance

  A user can use a bridged call appearance of an AWOH extension to place a call.

  A user can use a bridged call appearance of an AWOH extension to answer a call to the AWOH telephone.

  An AWOH extension can contain a bridged call appearance, but a user cannot use the bridged call appearance on the AWOH telephone to place a call.

- Busy Verification of Terminals and Trunks

  When you use busy verification of terminals and trunks on an AWOH extension, the telephone appears to you as an out-of-service telephone.

- Call Coverage

  AWOH telephones interact with Call Coverage as if all call appearances are busy.

  Call Coverage can be active at a disassociated telephone.

- Call Forward

  Call Forwarding can be active at an AWOH telephone, while the telephone is in a disassociated state. When the extension is associated, Call Forwarding is active.

- Call Park

  A call to an AWOH extension can be parked only if the primary extension has a bridged call appearance on a non-AWOH telephone. A call that is parked from a bridged call appearance is parked on the primary extension.

- Call Waiting Termination

  Call Waiting Termination can be administered on a single-line AWOH extension, but the caller receives a busy signal if the extension is disassociated.

- Conference

  Users cannot include an AWOH extension in a conference call.

- Customer-Provided Equipment (CPE) Alarm

  If a CPE alarm is active for an AWOH extension, no equipment is available to ring or light.

- Data Buttons

  Data buttons are not lit for AWOH data modules.

- Display

  The AWOH feature does not change the display for calls that originate or terminate from a bridged call appearance for an AWOH extension.

- Facility Busy Indication

  A telephone can have a busy indicator light for an AWOH extension, but the light is not lit. The light is not lit because Facility Busy Indication indicates whether an extension is off-hook or on-hook, even if you assign bridged appearances. An AWOH extension is always on-hook.

  You can administer a busy indicator light on AWOH extensions.When an administrator or a technician assigns a port to the extension, the busy indicator light functions as usual.

- Incoming Destination

  If the incoming destination is an AWOH extension, the caller hears ringback tone from the central office (CO). The system routes incoming calls based on features that are active for the extension, such as Call Forward and Call Coverage.

- ISDN-BRI voice terminals

  If TTI is enabled, you cannot use the SAT to enter **x** in the **Port** field of a BRI telephone Station record that is already connected to the switch. Instead, you must dial the TTI disassociate code from the telephone. For more information, see the "Terminal Translations Initialization (TTI)" feature.

- Leave Word Calling

  You can leave a leave-word-calling message at an AWOH extension.

- Manual Message Waiting

  When a user activates Manual Message Waiting toward an AWOH extension, no telephone exists on which to light the message waiting lamp. However, once the AWOH extension is associated with a port or telephone, the message waiting lamp lights.

- Manual Signaling

  Manual Signaling to an AWOH extension has no effect on system operation, because no terminal exists to signal.

  The system does not send a message to the originator of the call to inform the caller that the extension is an AWOH extension, and therefore cannot receive the signal.

- Personal Central Office Line (PCOL)

  You can administer AWOH extensions with PCOL. If a call terminates at an AWOH extension that does not have Call Coverage active, the caller receives the ringback tone. The ringback tone indicates that the call is unanswered. If the AWOH extensions has Call Coverage active, the system routes the call to coverage.

- Priority Calling

  A user who sends a priority call to an AWOH extension hears a busy signal.

- Send All Calls

  Send All Calls remains active on AWOH extensions.

- Station Hunting

  You can assign an AWOH extension to a telephone hunting chain.

- Station-to-Station Call

  The system processes a call to an AWOH extension in the same way that the system processes a call to a telephone for which all call appearances are busy.

- Transfer

  The system processes a transfer to an AWOH telephone in the same way that the system processes a call to a telephone that is busy.

Alphanumeric Dialing

Use the Alphanumeric Dialing feature to allow users to enter a alphanumeric name to place data calls instead of a numeric string.

Detailed description of Alphanumeric Dialing

This section provides a detailed description of the Alphanumeric Dialing feature.

With Alphanumeric Dialing, a user can place a data call with Data Call Setup and an alphanumeric string or alpha-name for the call-destination address. For example, a user can type 9+1-800-telefon instead of 9+1-800-835-3366 to place a call. Users need to remember only the alpha-name of the far-end terminating point.

With Alphanumeric Dialing, you can change a mapped string (digit-dialing address) without having to inform all users of a changed dial address. Users dial the alpha name.

When a user enters an alphanumeric name, the system converts the name to a sequence of digits according to an alphanumeric-dialing table. If the name that the users enters is not in the table, the system denies the call attempt. The user receives either an Invalid Address message (DCP) or a Wrong Address message (ISDN-BRI).

Because data terminals use DCP or ISDN-BRI data modules to access the switch, dialing procedures vary:

- For DCP, at the `DIAL` prompt, users type the alphanumeric name and then press **Enter**.
- For ISDN-BRI, at the `CMD` prompt, users type **d**, a space, the alphanumeric name, and then press **Enter**.

Administering Alphanumeric Dialing

This section describes:

- Any prerequisites for administering the Alphanumeric Dialing feature
- The screens that you use to administer the Alphanumeric Dialing feature
- Complete administration procedures for the Alphanumeric Dialing feature

Screens for administering Alphanumeric Dialing

Screen name	Purpose	Fields
Alphanumeric Dial Table	Map alphanumeric names to strings	• **Alpha-name** • **Mapped String**

Considerations for Alphanumeric Dialing

This section provides information about how the Alphanumeric Dialing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Alphanumeric Dialing under all conditions. The following considerations apply to Alphanumeric Dialing:

- You cannot use Alphanumeric Dialing on telephones that have Hayes modems.
- More than one alphanumeric name can refer to the same digit string.

Announcements

Use the Announcements feature to administer announcements that play for callers to your business. For example, you can inform callers that:

- The call cannot be completed as dialed
- The call is in a queue
- All lines are busy

Announcements are often used in conjunction with music.

The source for announcements can be either integrated or external.

- Integrated announcements reside on a circuit pack in the carrier, such as the TN2501AP circuit pack, or embedded in a media gateway processor circuit pack (called a “v VAL source” throughout this feature description).

  See Local announcements on media gateways on page 174 for a definition of v VAL.

- External announcements are stored on a separate piece of equipment (called an “adjunct”), and played back from the adjunct equipment.

Note:
This feature description uses the term “announcement source” to mean either integrated or external sources for announcements.

Announcements enhancements in Communication Manager 4.0

Starting with Communication Manager 4.0, there are several capacity increases with announcements and tone detectors.

Note:
These changes apply only to the S8720 Server in an XL configuration. It is also supported in the following configurations: LSP/ESS for a S8720 Server in an XL configuration, the S8720XL ESS, S8500C ESS or LSP, and S8300CLSP.
You can also use a S8500A/B ESS or LSP if you have added 512 MB RAM.

The capacity changes are as follows:

- You can have 128 TN2501 VAL boards within a single Communication Manager configuration. VAL boards are a right to use feature and require a new license file for upgrades.
- The number of announcement files supported on the TN2501 VAL boards has gone from 256 to 1024.

Note:
This change applies to the S8720 Server XL and other non-XL configurations.

- The total supported announcements has gone to 9000 from 3000. This applies to TN2501 VAL boards and the vVALs. This does not apply to the TN750 circuit packs.
- The number of touch tone receivers (TTRs) in a system is now 8000. This does not apply to H.248 gateways as they use a separate TTR resource.
- An announcement group is considered as a single announcement source. For a single sourced announcement extension, each group is one administered file. Each administered announcement extension is counted as one extension as can been seen on the Announcement/audio sources Screen. The total capacity of 3000 for non-XL servers and 9000 for the S8720XL server. Each instance of the announcement file counts as a separate entity towards the system limit of administered files.
  For an audio group, each source listed in the group where the announcement file resides counts as an administered file.

Detailed description of Announcements

Use the Announcements feature to play pre-recorded verbal messages to callers. You can also use announcements with music.

For Communication Manager V11 or later, multiple telephone sessions are allowed. One session is associated with each active integrated announcement source. An announcement that is stored on an announcement source can play through any port on the announcement source.

Any announcement, except those announcements that are administered for “barge-in” (see Barge-in announcements on page 177), can play simultaneously through multiple ports. All ports can play the same announcement at the same time, and the system can connect multiple users to each of these announcements.

Audio files on the announcement source, gateway, or adjunct equipment can be grouped together based on two other features, Locally Sourced Announcements and Locally Sourced Music-on-Hold. For more information, see the “Locally Sourced Announcements and Music-on-Hold” feature.

The Announcements feature supports three general types of announcements:

- A delay announcement explains the reason for the delay and encourages the caller to wait.
- A forced announcement explains an emergency or a known service problem. Use a forced announcement when you anticipate numerous calls about a specific issue.
- An information announcement gives the caller instructions on how to proceed, information about the number called, or information that the caller might need.

Use the Announcements feature when:

- Direct Inward Dialing (DID) calls cannot be completed as dialed
- Incoming private-network-access calls cannot be completed as dialed
- Calls enter a split or a skill
- DDC, UCD, or direct-agent calls are in queue for an assigned interval
- ACD and Call Vectoring calls are in queue for an assigned interval
- The destination of a call is a recorded announcement extension
- The system routes a call to a vector that contains an announcement step
- An announcement extension is specified as a coverage point
- An announcement is the incoming destination of a trunk group
- The Hospitality Automatic Wakeup feature is in use

The Announcements feature supports the following capabilities:

- Voice Announcements over LAN
- VAL Manager
- Local announcements on media gateways
- Announcement devices and types
- Barge-in announcements

Voice Announcements over LAN

Voice Announcements over LAN (VAL), that use a TN2501AP integrated announcement circuit pack:

- Plays announcements over the time-division multiplexing (TDM) bus
- Has up to 1 hour of announcement storage time for each circuit pack
- Has 33 ports: 31 playback, 1 dedicated record, and 1 Ethernet
- Supports a 10/100 MB Ethernet interface, to allow announcement and firmware file portability over a LAN, using file transfer protocol (FTP) server functions
- Supports generated **`.wav`** announcement files

Also see Local announcements on media gateways on page 174.

VAL Manager

Avaya VAL Manager is a stand-alone application that you can use to copy announcement files and Communication Manager announcement information over a LAN connection. VAL Manager is part of the Avaya Integrated Management suite of products.

VAL Manager provides:

- Simplified administration for adding, changing, and removing Communication Manager announcement information
- The ability to back up and restore announcement files and information to and from Communication Manager
- The ability to view the status of announcements on the VAL announcement source

Announcements are stored in **`.wav`** files that can be sent to a voice announcement over a LAN announcement source without conversion. VAL Manager also provides a repository to back up and restore announcement files, and simplifies administration.

Over your LAN with VAL Manager, you can:

- View the current status of announcements
- Add, change, and remove announcements
- Copy and back up announcement files from Avaya S8*XXX* servers to VAL Manager, and back again.

Local announcements on media gateways

Local announcements that are embedded in certain media gateway processor circuit packs are known as virtual Voice Announcements over LAN (called “virtual VAL” or “v VAL”). Use VAL Manager to manage local announcements. Use v VAL for media gateway embedded sources.

Local announcements (v VAL sources) are embedded in the following media gateway processor circuit packs:

Media Gateway	Playback Channels	Total Announcement Time
G250	6	10 minutes
G350	6	10 minutes
G700	15	20 minutes

Announcement devices and types

With the Announcements feature, you can administer either integrated announcements or announcements that are recorded on external devices. External devices connect to the server by means of analog-line circuit packs or auxiliary trunk interfaces, such as a TN2183 or a TN763.

The system stores integrated announcements on an integrated announcement source. The system can store multiple announcements on each announcement source up to the system capacity. The system can connect multiple users to each of these announcements.

Analog line types

External announcement machines for recorded announcements can be interfaced using one of the analog line types. The external announcement machine can then be connected by an analog line port.

Analog: The analog announcement type provides an analog telephone interface using an analog line port for use with an announcement/audio source device that emulates analog telephones. The switch starts playback by applying ringing; the device indicates playback has stopped by going on-hook (opening the loop). The switch does not indicate to the device to stop playback. Use the analog type for announcements that play for a specific period and then go on-hook at the end. When the device goes on-hook to indicate that the playback ended, the caller listening to the announcement hears a click. (See DS1 types, Auxiliary trunk types, or Integrated types for alternative types).

Analog-fd: Like the analog type, analog-fd provides an analog line interface and ringing starts the playback. However, a forward disconnect signal (open loop for about one-half second) is sent to the device to stop playback when there are no callers left to hear it.

Analog-m: Like the analog type, analog-m provides an analog line interface. However, ringing is not applied to start playback. Use this type for continuous playing music or audio sources. The device stays in an off-hook state when active and goes on-hook when it is not playing, is turned off, or is disconnected. This announcement type is used when the **Q** (queue) field is set to **b** to provide barge-in repeating or continuous-play announcements.

DS1 types

The DS1 types provide analog-like interfaces with DS1 line ports, which are called Line Side DS1 or Line Side T1. Each of these types indicate to the announcement, music, or audio-source device to start playback using the Line Side T1 equivalent of ringing. The DS1 types also expect off-hook from the device to indicate that the playback is active and on-hook to indicate that the playback is not active.

The ds1-id and ds1-sa types provide a forward disconnect using transitions of the A signaling bit to the device, which indicates when playback should be stopped. Callers listening to announcements do not hear clicks when the device disconnects (goes on-hook).

ds1-fd: The ds1-fd announcement type provides a TIA/EIA Foreign eXchange (FX) type DS1 interface. The forward disconnect signal is a toggle of the A bit from 0 to 1 and then back to 0 after 600 msecs. This type is used for Line Side T1 ports on the IVR system when they are used as an analog-like announcement device and is the recommended method for interfacing.

ds1-sa: The ds1-sa announcement type provides a TIA/EIA special-access type DS1 interface. The forward disconnect signal is a toggle of the A bit from 1 to 0 and then back to 1 after 600 msecs.

ds1-ops: The ds1-ops announcement type provides a TIA/EIA off-premises-station type DS1 interface that is used when the device does not support forward disconnect.

Auxiliary trunk types

The Auxiliary Trunk announcement type supports an external announcement machine connected using a 4-wire auxiliary trunk interface, such as a 15A announcement system. The switch indicates to the device to start or stop the playback on the S lead; the device indicates that the playback is active on the S1 lead.

aux-trunk: Use the aux-trunk (auxiliary trunk) announcement type with a 4-wire interface external device when the playback is to be stopped and started by way of the S1 lead and S1 is used by the device to indicate playback started.

aux-trk-m: Use the aux-trk-m (auxiliary trunk music) with a 4-wire interface device for continuously playing music or audio sources that do not indicate that playback is active on the S1 lead. This announcement type is used when the Q field is set to b to provide barge-in repeating or continuous-play announcements

Integrated types

The integrated announcement type stores announcements internally on the switch on an Integrated announcement source or embedded gateway processor equivalent. This can include TN2501AP Voice Announcements over LAN (VAL), or an H.248 Media Gateway VAL source.

The TN2501AP circuit pack has 31 ports that are available for playing announcements. The G700 v VAL source has 15 play ports, while the G350 and G250 v VAL source has 6 play ports. Integrated announcement sources are recommended for VDN of Origin Announcements and for other general and ACD announcement needs.

The following announcement circuit packs or sources are obsolete and not supported in Communication Manager configurations:

- TN750, TN750B, or TN750C announcement circuit packs
- Co-resident SSP sources (DEFINITY One or S8100)

integrated: Use the integrated announcement type for announcements that are stored on TN2501AP VAL sources, or co-resident v VAL sources. This announcement type is recommended for general, ACD, and vectoring announcements and for VDN of Origin Announcements.

integ-rep: The **integ-rep** (integrated-repeating) announcement type is used to provide integrated, repeating automatic wakeup announcements, and is implemented along with the **multi-integ** hospitality announcement type setting. This type can also be used for call center applications in vectoring where a continuous repeating announcement is required.

integ-mus: The **integ-mus** (integrated-music) announcement type is the same as the **integ-rep** type except that the **Q** field is set to **b** to provide a continuous repeating barge-in operation. This type is typically used to provide music on delay or on hold.

Any announcement that is stored on an announcement source can play through any port on the announcement source. Any announcement, except those announcements that are administered for “barge-in,” can play simultaneously through multiple ports. All 16 ports can play the same announcement at the same time.

You must set the **Q** field to **y** on the Announcements/Audio Sources screen for each extension that you want to queue for integrated announcements. Integrated announcements queue only when all ports on the announcement source that contains the announcement are busy. The same queuing pool is used for all announcement sources. The system controls the announcement queue length for integrated announcements, but you must set the queue length for analog or aux-trunk announcements.

Barge-in announcements

The system usually connects multiple callers to the beginning of an announcement, regardless of announcement type. However, you can also administer auxiliary trunk announcements, DS1 announcements, and integrated announcements to connect callers to hear a message that is already in progress. This capability is called “barge-in.”

Barge-in operation

When you administer barge-in by setting the **Q** field to **b**, only one port plays the announcement at any one time. When the system routes a call to that announcement, the call immediately connects to the port and the caller hears the announcement as it is playing.

Most administrators administer barge-in announcements to repeat continually while callers are connected to the port. In this way, the caller listens until the system plays the entire announcement.

Non-barge-in operation

If an announcement port is available when a call arrives, the system connects the call to the announcement starting from the beginning.

If an announcement port is not available and the announcement is administered with **no** as the queue option, the call does not enter the queue for the announcement and the caller hears busy or other feedback, depending upon how the announcement was accessed.

If an announcement port is not available and the announcement is administered with **yes** as the queue option, the call enters the announcement queue. When a port becomes available, the switch connects the calls waiting in the queue, up to the system limit, to the beginning of the announcement.

Announcement sources in the G700, G350, and G250 Media Gateway

The Announcements feature provides a v VAL source for each G700, G350, and G250 Media Gateway that is registered to either an Avaya S8300 or an Avaya S87xx Server. The S87xx-type server systems supports 10 integrated TN2501AP circuit packs, plus an additional 250 v VAL sources for a total of 260. The S8300 supports 50 v VAL sources.

In Communication Manager 4.0 or later, the S8720 with the Increased Capacities Configuration supports up to 128 VAL boards (TN2501) and 250 v VAL sources per system.

Note:
The S8300 does not support standard port networks or TN-type circuit packs. Also, the software resources for integrated announcement sources and G700, G350, and G250 v VAL sources are separated. The G700, G350, and G250 v VAL sources are counted separately towards the limit of 50 on the S8300, and 250 on the S87xx-type server systems.

Compression rates

The TN2501AP VAL circuit pack and media gateway v VAL sources only support the 64Kbps compression rate. The **Rate** field defaults to this rate.

Announcement sessions

You can record, play back, or delete integrated announcements by initiating an announcement session. To do this, you must have console permissions assigned to your Class of Service (COS) for the internal station, or Remote Access barrier code in order to initiate an announcement session.

You can transfer to and from a computer or delete announcement files over the LAN for the TN2501AP and H.248 v VAL sources using the Voice Announcement Manager (VAM) software or using an FTP client in conjunction with SAT commands.

Announcements for the VAL sources can also be recorded with a telephone using the procedures discussed in this section. Use those procedures to record announcements on the TN2501AP circuit packs, as well as for embedded v VAL sources on the G700, G350, and G250 Media Gateways.

Announcement recordings

Once an end user accesses an announcement session, the user can dial **1** to record an announcement, **2** to play an announcement, or **3** to delete the announcement. If the announcement source memory is more than 90% full, then Communication Manager gives stutter dial tone when the user gains access to an announcement session. Even if the user hears stutter tone, the user should begin speaking to record the announcement.

Note:
You need to have a telephone or console with a class of service (COS) that provides console permissions to record announcements.

With VAL announcement sources, recording by telephone always uses a recording port that is dedicated for telephone access on the TN2501AP circuit packs or v VAL sources.

VAL announcement sources support recording announcements as PC **`.wav`** files, either on a local PC or made by a professional recording studio. The files are moved onto the VAL source using FTP.

Note:
You cannot use a telephone to record an announcement with an audio group assignment. Using FTP, move each pre-recorded file to each of the sources defined for the audio group.

For more information, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Announcement session process

To begin an announcement session, the user must dial the administered Feature Access Code (FAC) followed by the announcement session.

- If an announcement session is already in progress, or if a save or restore command is in progress, then the user hears reorder tone (fast busy) and the system drops the call.
- If the telephone session port to an integrated announcement source is in use, then the user hears reorder tone followed by silence. This indicates that the port will be reserved for an announcement session. The user should redial the FAC and extension every 45 seconds to gain access to the port.

Note:
You need to have a telephone or console with a class of service (COS) that provides console permissions to record announcements.

Multiple telephone sessions are allowed, with one session associated with each active integrated announcement circuit pack.

Once a telephone user accesses an announcement session, the user can dial **1** to record an announcement, **2** to play an announcement, or **3** to delete an announcement. If the announcement source memory is more than 90% full, then the switch gives stutter dial tone when the user gains access to an announcement session. Even if the user hears stutter tone, the user can begin speaking to record the announcement.

Avaya recommends that you use a digital or IP telephone, since these telephones provide the best quality and functionality.

Tip:
Do not use remote telephone connections that route over IGAR (Inter-Gateway Alternate Routing)-supported facilities. The beginning portion of the recording, about four or five seconds, is not recorded after hearing the ready tone.

Locally Sourced Announcements and Music

The Locally Sourced Announcement and Music feature is based on the concept of audio source groups. This feature allows announcement and music sources to be located on any or all of the Voice Announcement with LAN (VAL) circuit packs or on virtual VALs (v VAL) in a media gateway. The VAL or v VAL circuit packs are assigned to an audio group. The audio group is then assigned to an announcement or audio extension as a group sourced location. When an incoming call requires an announcement or music-on-hold, the audio source that is closest to the incoming call trunk plays the file that is assigned to the announcement extension.

For more information, see the feature description on “Locally Sourced Announcements and Music."

Administering Announcements

The following steps are part of the administration process for the Announcements feature:

- Adding/changing/displaying or removing announcement extensions
- Adding a TN2501AP VAL circuit pack
- Listing all administered circuit packs
- Setting up a media gateway for announcements
- Recording and changing announcements
- Deleting and erasing announcements
- Setting up continuous-play announcements
- Recording VAL announcements
- Converting announcement files to VAL format
- Using FTP to Manage VAL announcements
- Recording announcements for TTY callers

This section describes:

- Any prerequisites for administering the Announcements feature
- The screens that you use to administer the Announcements feature
- Complete administration procedures for the Announcements feature

Prerequisites for administering Announcements

You must complete the following actions before you can administer the Announcements feature:

- None

Screens for administering Announcements

Screen name	Purpose	Fields
Announcements/Audio Sources	Add, change, or delete individual announcement extensions, and the properties of the announcements. The announcement extension and file names must be defined before the announcement can be recorded using a telephone.	All
Circuit Packs	Administer this screen only if you want to administer the **Board Location** on the Announcements/Audio Sources screen, and you do not have the TN2501AP circuit pack plugged in.	All
Integrated Announcements/ Audio	List all existing announcement sources that have been administered.	All
Media-Gateway	Administer this screen to indicate that the media gateway will be used as a v VAL source.	**V9** field set to **gateway-announcements** **NOTE:** These v VAL sources must also be enabled using the **`enable announcement-board`** command (see Setting up a media gateway for announcements on page 189).

Screen name	Purpose	Fields
IP Node Names	Assign an IP address for each TN2501AP circuit pack.	All
IP Interfaces	Use this screen to assign a network region to an IP interface device, or to administer Ethernet options.	• **Node Name** • **Subnet Mask** • **Gateway IP Address** • **Network Region** • **Enable Ethernet Port**
Data Module	Assign an ethernet data module for the TN2501AP circuit pack.	All
Station	Set the Class of Service (COS) for the Announcements feature used for recording using a telephone.	**COS**
Feature Access Code (FAC)	Set up a Feature Access Code (FAC) to allow you to record announcements.	**Announcement Access Code**
Feature-Related System Parameters	Administer this screen if you plan to use Announcements with the feature that is associated with each field shown in the **Fields** column at right. Also used to set direct agent announcements.	• **DID/Tie/ISDN Intercept Treatment** • **Controlled Outward Restriction Intercept Treatment** • **Controlled Termination Restriction (Do Not Disturb)** • **Controlled Station-to-Station Restriction**
Hospitality	Administer this screen if you plan to use Announcements with the Hospitality feature.	• **Announcement Type** • **Length of Time to Remain Connected to Announcement**
Trunk Group	Administer this screen if you plan to use Announcements with the Trunk Group feature.	**Incoming Destination**
Coverage Path	Administer this screen if you plan to use Announcements with the Call Coverage feature.	**Coverage Points**

Screen name	Purpose	Fields
Hunt Group	Administer this screen if you plan to use Announcements with the Hunt Group feature.	• **First Announcement Extension** • **Second Announcement Extension**
Call Vector	Administer this screen if you plan to use Announcements with the Call Vectoring feature.	All fields that require announcements
VDN	Administer the VDN of Origin Announcement (VOA) extension.	**VDN of Origin Annc. Extension**

Adding/changing/displaying or removing announcement extensions

You need to assign an extension for each announcement that you want to record. After you define an announcement extension, you use the extension to record and access the announcement. You can define up to 256 announcement extensions.

If you have Communication Manager 4.0 or later, and a S8720 Server with the XL configuration or a non-XL configuration, you can define up to 1024 announcement extensions. You must have a license file that supports the increased capacities.

Note:
Announcement extensions and file names must first be defined before you can record announcements using a telephone.

To add announcement extensions:

1. Type **`add announcement xxxx`** Press **Enter**.

   The system displays the Announcements/Audio Sources screen.

Figure 26: Announcements/Audio Sources screen

```
add announcement 26451                                        Page   1 of  1

ANNOUNCEMENTS/AUDIO SOURCES

  Extension: 26451_____________                      COR: 1
  Annc Name: collect_some_digits                      TN: 1
  Annc Type: integrated                            Queue? y
 Group/Port:                                 Queue Length:
  Protected? n                                       Rate: 64
```

2. In the **Extension** field, type the extension that you want to assign to this announcement.

   In the **Annc Name** field, type the unique name of the announcement that you are associating with the extension.
   If you use a TN2501AP circuit pack or a media gateway v VAL source, you must type a name, with no blank spaces, in the **Name** field. Do not type the file extension **.wav** in the **Name** field. This name becomes the unique file name for the announcement file. The system adds the **.wav** file extension to the name when the file is added to the announcement source.

   For rules in naming files, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878, the Announcements/Audio Sources screen, in *Administering Avaya Aura™ Communication Manager*, 03-300509. Also see Announcement file format requirements on page 195.

3. In the **Annc Type** field, type the announcement type. See Announcement devices and types on page 174 for more information.
   If the **Annc Type** is integrated, you will see the related fields **Group/Port** and **Protected**.
4. In the **COR** field, type the Class of Restriction that is associated with this announcement.
5. In the **TN** field, type the tenant partition, if any, that is associated with this announcement.

Note:
After the **Annc Name** field, the remaining fields may or may not appear, depending on the value that you typed in the **Annc Type** field.

6. In the **Queue** (queuing) field, perform one of the following actions:

   - If you want calls to wait to hear an announcement when all the ports on the announcement source are busy, type **y**. If the announcement is assigned to an audio group (see the “Locally Sourced Announcements and Music-on-Hold” feature), the system selects and plays the file in the closest announcement group.

Important:
Avaya strongly recommends setting the **Queue** field to **y** for Call Center applications.

- If you do not want calls to wait to hear an announcement when all the ports on the announcement source are busy, type **n**. If you type **n** in this field, a queue is not created, and the caller hears a busy signal or other feedback, depending on how the announcement was accessed.

7. The system displays **N/A** in the **Queue Length** field. You cannot change this field for integrated announcements. The length of the queue for integrated announcements is preset.
8. In the **Protected** field, perform one of the following actions:
   - If you want to allow users with console permissions or FTP sessions to change the announcement, type **n**.
   - If you do not want to allow users with console permissions or FTP sessions to change the announcement, type **y**. If you type **y** in this field, the announcement is protected and cannot be changed or overwritten by a new version of the file.
9. In the **Group/Port** field, type one of the following values:
   - The location of the TN2501AP circuit pack.
   - ***ggg*v9** for G700, G350, or G250 v VAL sources, where ***ggg*** is the number of the media gateway.
   - **G*nn***, where ***nn*** equals 1-50 and is the audio group number of the locally-sourced announcement or locally-sourced Music-on-Hold group.

Note:
You can have numerous announcement and music-on-hold files, each assigned to a different extension, in a single audio group. For more information on audio groups, locally-sourced announcements, and locally-sourced music-on-hold, see the “Locally Sourced Announcements and Music-on-Hold” feature.

Important:
If you administer a TN2501AP circuit pack, and it is not yet installed in the carrier, you must administer the Circuit Packs screen. For more information on this screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

10. Repeat steps 2 through 8 with the correct information for each announcement you want to record. To get to the next screen, press **Next**.
11. Press **Enter** to save your changes.

Important:
These steps only create the administered extension and name for the announcement file. You fill the file space when you record an announcement or transfer an announcement file to the announcement source through a file transfer protocol (FTP) session.

Important:
If you want to change an announcement, use the command **change announcement *xxxx*.** To display announcements, type **display announcement *xxxx***. To remove announcements, type **remove announcement *xxxx***.

Note:
To administer DID Intercept announcements in a multi-location system where each location or city needs a different announcement, enter an audio group in the **Group/Port** field instead of a VAL port.

Adding a TN2501AP VAL circuit pack

After a TN2501AP VAL circuit pack is physically installed on your system, you must configure it in the Communication Manager system.

To add a TN2501AP VAL circuit pack:

1. Type **change node-names ip**. Press **Enter**.

   The system displays the IP Node Names screen (Figure 27: IP Node Names screen on page 186).

Figure 27: IP Node Names screen

```
change node-names ip                                          Page 1

                                IP NODE NAMES

Name                      IP Address              Name          IP Address
 1. _______________     ___.___.___.___   17. _______________   ___.___.___.___
 2. _______________     ___.___.___.___   18. _______________   ___.___.___.___
 3. _______________     ___.___.___.___   19. _______________   ___.___.___.___
 4. _______________     ___.___.___.___   20. _______________   ___.___.___.___
 5. _______________     ___.___.___.___   21. _______________   ___.___.___.___
 6. _______________     ___.___.___.___   22. _______________   ___.___.___.___
 7. _______________     ___.___.___.___   23. _______________   ___.___.___.___
 8. _______________     ___.___.___.___   24. _______________   ___.___.___.___
 9. _______________     ___.___.___.___   25. _______________   ___.___.___.___
10. _______________     ___.___.___.___   26. _______________   ___.___.___.___
11. _______________     ___.___.___.___   27. _______________   ___.___.___.___
12. _______________     ___.___.___.___   28. _______________   ___.___.___.___
13. _______________     ___.___.___.___   29. _______________   ___.___.___.___
14. _______________     ___.___.___.___   30. _______________   ___.___.___.___
15. _______________     ___.___.___.___   31. _______________   ___.___.___.___
16. _______________     ___.___.___.___   32. _______________   ___.___.___.___
```

2. In the **Name** field, enter a name for the circuit pack.
3. In the **IP Address** field, assign a valid IP address to the circuit pack.
4. Press **Enter** to save your changes.

To set up an IP interface, assign a network region, and enable the ethernet port for the circuit pack:

1. Type **add ip-interface *n***, where ***n*** is the cabinet location of the circuit pack. Press **Enter**.

   The system displays the IP Interfaces screen (Figure 28: IP Interfaces screen (showing TN2501 VAL board) on page 187).

Figure 28: IP Interfaces screen (showing TN2501 VAL board)

```
add ip-interface 02a12                                    Page   1 of   1
                                  IP INTERFACES


                  Type: VAL
                  Slot: 02A12
           Code/Suffix: TN2501
             Node Name: manta_val10
            IP Address: 172.22 .21 .14
           Subnet Mask: 255.255.0  .0
       Gateway Address: 172.22 .22 .254
  Enable Ethernet Port? y

ETHERNET OPTIONS
                  Auto? y
```

2. Enter the appropriate information in the **Node Name**, **Subnet Mask**, **Gateway Address**, and **Network Region** fields.
3. Set the **Enable Ethernet Port** field to **y**.
4. Press **Enter** to save your changes.

To add an ethernet data module:

1. Type **add data-module next**.

   The system displays the Data Module screen (Figure 29: Data Module screen on page 188).

Figure 29: Data Module screen

```
 add data-module next                                          Page   1 of   1
                               DATA MODULE

  Data Extension: 40500           Name:                              BCC: 2
            Type: pdm              COS: 1         Remote Loop-Around Test? n
            Port:                  COR: 1           Secondary data module? n
             ITC: restricted        TN: 1                    Connected To: dte


ABBREVIATED DIALING
  List1:

SPECIAL DIALING OPTION:

ASSIGNED MEMBER ( Station with a data extension button for this data module )

         Ext           Name (first 26 characters)
     1:
```

2. In the **Name** field, enter an appropriate name for this data module.
3. In the **Type** field, enter **ethernet**. The system displays the ethernet-specific fields.
4. In the **Port** field, enter the cabinet location of the VAL circuit pack followed by port number **33**.

   Note:
   Although the VAL circuit pack has only 32 ports, the data module uses 32 +1, or **33** for its port value.
5. In the **Link** field, enter a communication interface link number between 1 and 99.
6. Press **Enter** to save your changes.

To ensure that the VAL circuit pack has been properly added:

1. Type **`status link n`**, where ***n*** is the link number that you just assigned on the Data Module screen. The link should display a status of **in-service/idle**.

Listing all administered circuit packs

You can review announcement settings and ensure that the announcement administration is correct by listing all existing administered circuit packs.

To list all existing administered circuit packs:

1. Type **list integrated-annc-boards**. Press **Enter**.

   The system displays the Integrated Announcements/Audio screen (Figure 30: Integrated Announcements/Audio screen on page 189).

Figure 30: Integrated Announcements/Audio screen

```
list integrated-annc-boards                                          Page   1

                          INTEGRATED ANNOUNCEMENTS
Board Location: 03C12              Time Remaining @ 64Kbps: 7

Intern Group  Announcement                              Length     Size
Number Number Extension       Name                      (Sec)      (Kb)
  NA          27102__________ dtmf5_mu                   5         233
  NA          27103           voa_3c12                   3         217
  NA          27107           collect_digits_3c12        0         none
  NA          27109           dr_evil                    2         83
  NA     1    27111           direct_agent_annc_3c12     3
```

Setting up a media gateway for announcements

If you are going to use a G700, G350, or G250 Media Gateway as a v VAL source, you must first set up the gateway to accept announcements.

To set up a media gateway as a v VAL source:

1. Type **change media-gateway *n***, where ***n*** is the number of the media gateway. Press **Enter**.

   The system displays the Media Gateway screen (Figure 31: Media Gateway screen on page 190).

Note:

If you need a list of the media gateway numbers, type **list media-gateway**. Press **Enter**. The system displays the Media-Gateway Report screen, listing all the media gateways and their numbers.

Figure 31: Media Gateway screen

```
change media-gateway 5                                          Page 1
                            MEDIA GATEWAY

        Number: 5                            IP Address: 172.17 .24 .123
          Type: g700               FW Version/HW Vintage: 25 .17 .0  /0
          Name: MG5                          MAC Address: 00:03:0d:01:09:c2
     Serial No: 01DR123456789               Encrypt Link? n
Network Region: 205                            Location: 5
    Registered? y                   Controller IP Address: 172.19 .18 .137
 Recovery Rule: none                             Site Data:
     Slot   Module Type              Name                   test changes
      V1:   S8300                    ICC MM
      V2:   MM710                    DS1 MM
      V3:   MM712                    DCP MM
      V4:   MM710                    DS1 MM



      V8:
      V9: gateway-announcements
```

2. Set the **V9** field to **gateway-announcements**.

   Note:
   There is no physical port named “V9” on a G700, G350, or G250 Media Gateway. The V9 port is virtual, and is used only for announcements.

3. Press **Enter** to save your changes.

   For more information on this screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

If you are using a v VAL source, you must now enable the v VAL source that has the **V9** field set.

1. Type **enable announcement-board *ggg*V9**, where ***ggg*** is the number of the media gateway in the Media Gateway screen. In this example, type **enable announcement-board 5V9**.
2. Press **Enter** to save your changes.

   Note:
   Use the gateway IP address as the v VAL address for FTP sessions.

Recording and changing announcements

You can use a system telephone or an attendant console to record a new announcement for callers to hear when callers dial a specific extension. Use the same procedure to change an existing announcement.

For recording VAL announcements, see Recording VAL announcements on page 194.

Prerequisites

You must complete the following actions before you can record announcements:

- Ensure that you have a telephone or an attendant console with a Class of Service (COS) that provides console permissions to record announcements. For more information on Class of Service, see the “Class of Service” feature.
- Ensure that a Feature Access Code (FAC) has been set up to record announcements using a telephone. For more information on Feature Access Codes, see the “Feature Access Code (FAC)” feature.
- Ensure that the necessary extensions, file names, and port addresses have been assigned using the Announcements/Audio Sources screen.

To record or change an announcement:

1. From a telephone or console, dial the Announcement Feature Access Code (FAC). For more information on FACs, see the “Feature Access Code” feature.
   - If you hear dial tone, continue with Step 2.
   - If you hear a fast busy signal, hang up. Redial the FAC and the extension every 45 seconds until you hear dial tone.

   Note:
   You cannot record an announcement using a telephone for an extension with Locally Sourced Announcement/Music audio group (Gn) assigned. These files must be recorded using a PC. They can also be recorded to a single sourced extension using a telephone, then, using the FTP process, transferred to each of the sources in the audio group.
2. Dial the announcement extension.

   Do not enter the announcement session command until you hear dial tone. Enter "#" after the extension or wait for the dial tone to continue.
3. When you hear dial tone, dial **1** to begin recording.
   - If you hear a beep or a stutter tone, begin recording. If the integrated source memory becomes full while you are recording, the system drops your connection and does not retain the announcement.
   - If you hear intercept tone, hang up. Record your announcement on another extension that is assigned to a different VAL circuit pack or v VAL source.

4. To end the recording:
   - If you are using a digital telephone, press the pound key (**#**). You hear a dial tone again, and you can continue your session.
   - If you are using an analog telephone, hang up quietly. If your analog telephone is not connected through lineside DS1, the system might record an electrical click at the end of the recording. You must redial the Announcement FAC to continue your session.
5. If you are using a digital telephone, and you want to listen to the announcement that you just recorded, dial **2**. The recording plays back through the handset.
6. If you are not satisfied with the announcement, press:
   - **1** to rerecord the announcement
   - **3** to delete the announcement, and to end the recording session
7. To listen to the announcement after you hang up, dial the announcement extension from any telephone or attendant console. The announcement plays through the handset.

   When you directly dial an announcement extension, for which an announcement has not been recorded, you hear silence instead of a busy tone with the VAL-type sources, such as the TN2501AP circuit pack or the v VAL source.

Note:
You must wait 15 seconds after you record an announcement before you can dial the extension to hear the announcement replay. During this 15-second window, you cannot record a new announcement, and no one can play this announcement. However, you can rerecord the announcement during this 15-second period. To rerecord the announcement, dial the Announcement FAC, dial the extension, and then press **1** before the 15-second timer expires.

Deleting and erasing announcements

You can use a system telephone or an attendant console to delete recorded announcements from an integrated announcement source.

Note:
The system denies any attempt to delete an announcement while it is playing, being transferred, or being backed up to FLASH (amber LED is flashing), regardless of whether the attempt is from a system telephone, the SAT, or through an FTP session.

Before you start, gather the following information:

- Look up the announcement extension, which is mapped to a specific announcement source by location.

1. At the SAT, type **`list integrated-annc-boards`**. Press **Enter**.

   The system displays the Integrated Announcements/Audio screen (Figure 30: Integrated Announcements/Audio screen on page 189).

2. Determine the extension(s) for the announcement(s) that you want to delete.

- Write down the Feature Access Code (FAC) for an announcement session. For more information on FACs, see the “Feature Access Code” feature.

To delete or erase an announcement:

1. From a telephone or an attendant console, dial the Announcement FAC.
2. When you hear dial tone, dial the announcement extension.
3. When you hear dial tone, dial **3** to delete the announcement. You hear a confirmation tone. If the announcement is protected or is playing at the time you perform this step, you hear a fast busy signal (the reorder tone), and the system does not delete the announcement.
4. Hang up the telephone.
5. To ensure that an announcement was deleted, dial the extension of the deleted announcement. If the announcement was deleted, you hear a busy signal.
6. Repeat Steps 1 through 5 for each announcement that you want to delete. You can delete only one announcement at a time.

Deleting an announcement extension

You might also want to remove the announcement extension from the system. To remove the announcement extension:

1. Type **`change announcements`**. Press **Enter**.

   The system displays the Announcements/Audio Sources screen (Figure 26: Announcements/Audio Sources screen on page 184).

2. Delete the information in the **Ext**, **Name**, and **Type** fields.
3. Press **Enter** to save your changes.

Erasing an announcement source

Finally, to erase an announcement on the announcement source:

1. Type **`erase announcements`** ***`n`***, where ***`n`*** is the address of the announcement source that contains the announcement that you want to erase.

   The system displays a warning message that confirms the deletion.

2. Press **Enter** to erase the announcements on the announcement source.

Setting up continuous-play announcements

You can set up announcements to continuously repeat while callers are connected to the announcement, so that a caller can listen until the system plays the entire announcement. With a “barge-in” queue, you do not need a separate port for each announcement.

For example, you can set up an Automatic Wakeup announcement to repeat, and use a barge-in queue. When guests pick up the telephone to hear an announcement at a particular time, they use only one port. The message repeats on that port until the last guest goes off-hook and the message ends.

To set up a continuous-play announcement:

1. Type **`change announcements`**. Press **Enter**.

   The system displays the Announcements/Audio Sources screen (Figure 26: Announcements/Audio Sources screen on page 184).

2. In the **Q** field, type **b** on the same line as the extension for the announcement.
3. Leave the name that is in the **Name** field, or enter a new description for the announcement.
4. Press **Enter** to save your changes.

Recording VAL announcements

You can record an announcement for callers to hear when the callers dial a specific extension, or as part of call vectoring. Use the same steps to change an existing announcement.

You can record announcements at a:

- Professional recording studio
- Computer
- System telephone

Prerequisites

You must complete the following actions before you can record VAL announcements:

- Ensure that the announcement administration is complete. You must assign a name to the file before you can record an announcement. For more information, see Adding/changing/displaying or removing announcement extensions on page 183.
- If you are replacing a TN750C announcement circuit pack with the TN2501AP circuit pack or media gateway v VAL source:

  - Get a list and a description of the announcements that are stored on the TN750C circuit pack.
  - Rerecord the announcements on a computer or at a professional recording studio as **.wav** files (CCITT µ-Law [pronounced “mu-Law”] or A-Law, 8-KHz, 8-bit mono), so that the files are ready to transfer to the new announcement source after the announcement source is installed and administered.

- If you replace an older TN750 announcement circuit pack with the new TN2501AP circuit pack or media gateway v VAL source:
  - Remove previous announcement administration.
  - Record new announcements for the TN2501AP circuit pack or media gateway v VAL source.
  - Rerecord any announcements that currently reside on the TN750 circuit packs that you are replacing. You cannot transfer or restore TN750 announcements from a Flash card, tape, or optical disk to the TN2501AP circuit pack or media gateway v VAL source.

CAUTION:
When you change a VAL announcement, the TN2501AP circuit pack or media gateway v VAL source is activated to perform a Flash auto-save backup 5 minutes later. If you try to record a new announcement during this backup process, the new recording fails, and a denial event is logged to the Event Report screen.

For information on viewing the denial events, see Viewing the Event Report on page 206.

Announcement file format requirements

To be compatible with the TN2501AP circuit pack or media gateway v VAL source and Communication Manager, announcement recordings must have the following parameters:

- CCITT A-Law or CCITT µ-Law compression format. Do not use PCM.
- 8-KHz sample rate
- 8-bit resolution (bits per sample)
- Mono (channels = 1)
- The µ-Law compression format is used in the United States, and A-Law compression format is used internationally. Use the compression format that is specified on the Location Parameters screen.
- Filenames for the VAL announcement sources cannot contain blank spaces, nor any of the following characters:
  - Period (.)
  - Comma (,)

- Colon (:)
- Asterisk (*)
- Question mark (?)
- Less than (<)
- Greater than (>)
- Forward slash (/)
- Backward slash (\)

The filename itself is case sensitive, but the file extension **.wav** must be lowercase. Announcements that are recorded in this format occupy 8-KB per second of file space for each second of recorded speech. For example, a 10-second announcement creates an 80-KB **.wav** file.

Do not type the **.wav** file extension for the file name in the Announcements/Audio Sources screen. The system does not display the **.wav** file extension on this screen.

To record a VAL announcement at a computer:

1. At the computer, open the application that you use to record **.wav** files, such as Microsoft Sound Recorder.
2. Set the recording parameters.
3. Speak into a microphone that is connected to the computer and record the announcement.
4. Assign a name to the **.wav** file, following the rules for defining announcement names on the Announcements/Audio Sources screen. Make sure that the resulting file name on the PC *does* have the **.wav** file extension as part of the name.

   Important:
   For the system to access this announcement file, the file name, minus the **.wav** file extension, must exactly match the name on the Announcements/Audio Sources screen.
5. Play the announcement back at the computer before you transfer the file to the announcement source.

To use a system telephone to record an announcement, see Recording and changing announcements on page 191.

Converting announcement files to VAL format

If you share recordings in a multisite environment with Communication Manager and Avaya Interactive Voice Response (IVR) systems, you can convert announcement files for use on either system. If you want to convert an announcement file to the required format, you can use a sound recording utility application, such as Microsoft Sound Recorder.

To convert a previously recorded announcement, or a file that is compatible with an Avaya Interactive Voice Response system, to a format that is compatible with Communication Manager:

1. Open the sound recording application on your computer. For example, you might use Microsoft Windows Sound Recorder.
2. Open the file that you want to convert.
3. Check the file properties to determine if you must change the parameters.
4. If you must change the recording parameters, look for a conversion tool. Some tools have a **Convert Now** option. Other tools, for example, Microsoft Sound Recorder, are included with the **Save As** function.
5. Change the file parameters to parameters that are listed in Announcement file format requirements.

Note:
In some applications, assigning the format (for example, CCITT µ-Law) sets the remainder of the default parameters. Check each parameter carefully, and change the default setting to match the required parameters if necessary. Note that CCITT µ-Law or A-Law can be referred to as ITU G.711 µ-Law or ITU G.711 A-Law, respectively.

Converting announcements for Interactive Voice Response

The Interactive Voice Response (IVR) system has a recording conversion utility that supports file formats that are similar to the formats that VAL requires. However, the conversion utility can read only PCM-format announcement files.

To convert an announcement file for use on an IVR system:

1. If the companding format of the file is already PCM, go to Step 5.

   If you are unsure what the file format is, continue with Step 2.
2. At a computer, open the sound recording application.
3. Open the file that you want to convert.
4. Save the announcement (**Convert Now** or **Save As**) with these parameters:
   - Format: PCM
   - Bits/Sample: 8
   - Sample Rate: 8-KHz
   - Mono (channels = 1)

Note:
The recording conversion utility requires that announcement files be in PCM format. VAL files must be in CCIT A-Law or µ-Law format.

5. Open the file in the recording conversion utility.
6. Convert the file to SSP format.

Deleting VAL announcements

Prerequisites

You must complete the following actions before you can delete VAL announcements:

- Look up the announcement information. Type **`list directory board`**. Press **Enter**.
- Determine which announcements that you want to delete, either by extension or file name.
- Decide whether you are:
  - Using the SAT to delete individual VAL announcement files
  - Using the SAT to delete all VAL announcements on a circuit pack
  - Deleting and erasing announcements

Note:
The system denies any attempt to delete an announcement while the announcement is playing, being transferred, or backed up to Flash memory.

Using the SAT to delete individual VAL announcement files

To use the System Administration Terminal (SAT) to delete an announcement:

1. Type **`remove file board board-location`** ***`/annc/filename.wav`***, where ***`filename.wav`*** is the name of the file that you want to delete. Press **Enter**.

Note:
File names are case sensitive, and require the **`.wav`** file extension.

The ***`/annc`*** portion of the command directs the system to the announcement subdirectory on the announcement source. The **`/closed.wav`** portion indicates to delete the file **`closed.wav`**.

Using the SAT to delete all VAL announcements on a circuit pack

To use the System Administration Terminal (SAT) to delete all announcement files on a VAL circuit pack:

1. Type **`busyout board`** ***`board-location`***, where ***`board-location`*** is the 5-character number that is assigned to the circuit pack. Press **Enter**.

Note:
When the VAL circuit pack is busied out,

- Both the RSCL and the Ethernet ports are busied out.
- The firmware takes down the Ethernet link.
- FTP is disabled because the Ethernet link is not functioning.
- Announcements on that circuit pack cannot play.

2. Type **`erase announcements board board-location`**, where ***`board-location`*** is the 5-character number that is assigned to the circuit pack. Press **Enter**.

   CAUTION:
   This command deletes the specified announcement file in both RAM and Flash memory. The circuit pack firmware ignores the protect flag (**Pro** field) when you erase the announcement files.

3. Type **`list directory board`**. Press **Enter**.
4. Verify that no files are listed.

   Note:
   The announcement directory on the TN2501AP circuit pack or the v VAL source is **/annc**.

5. Type **`list integrated-annc-boards`**. Press **Enter**.

   Check the list. The **Length in Seconds** field shows **0** if the announcement was deleted.

To use a system telephone to delete VAL announcements, see Deleting and erasing announcements.

Using FTP to Manage VAL announcements

This section includes information on how to set up and terminate a file transfer protocol (FTP) session, and outlines announcement tasks that you can perform in an FTP session.

An FTP session has three basic components:

- Setting up an FTP session
- Performing tasks in an FTP session
- Ending an FTP session

SECURITY ALERT:
Read and observe all Security Alerts regarding enabling and disabling the VAL file system and FTP sessions. VAL refers to TN2501AP circuit packs or media gateway v VAL sources.

Setting up an FTP session

To set up an FTP session into the VAL circuit pack, you must:

- Prepare the VAL circuit pack for the FTP session. This action:
  - Allows an FTP session on an individual VAL circuit pack
  - Creates an ftp-login and ftp-password for that session
- Start an FTP session from a computer or a network management terminal. Before you can start the FTP session, you must know the:
  - IP address of the VAL circuit pack.
  - ftp-login and ftp-password of the VAL circuit pack.

Preparing the VAL circuit pack for the FTP session

To prepare the VAL circuit pack for the FTP session, including setting the user name and the password:

1. Type **`enable filesystem board`** ***`board-location`*** **`login`** ***`ftp-username ftp-password`***, where ***`ftp-username`*** is a string of 3 to 6 alphanumeric characters, and ***`ftp-password`*** is a string of 7 to 11 alphanumeric characters. Press **Enter**.

   For example, the command **`enable filesystem board 01A11 login romeo shakespeare`** enables an FTP session into the VAL circuit pack in Cabinet 1, carrier A, slot 11. The ftp-username (3 to 6 characters) for this session is **romeo**, and the ftp-password (7 to 11 characters) is **shakespeare**.

   When the FTP session on the circuit pack is enabled, the announcement and the firmware files are available to anyone who knows the IP address of the VAL circuit pack, the ftp-username, and the ftp-password.

   SECURITY ALERT:
   Avaya recommends that you use a unique ftp-login and ftp-password for each FTP session.

If you are unfamiliar with FTP client application software, contact your network administrator for information about access to an FTP session.

The following points apply to FTP sessions into the VAL circuit pack:

- In FTP sessions, file names are case sensitive, and require the **`.wav`** file extension.

- Only one FTP session can be active at a time. If an FTP session is already active for a particular VAL circuit pack, the system denies a second attempt to establish an FTP session from another remote host.
- The VAL circuit pack has two user-accessible directories:
  - /annc for playable announcements.
  - / (root) for temporary storage of embedded software updates. Use this directory only for software updates.
- FTP sessions time out after 10 minutes of inactivity.

Starting an FTP session

To start an FTP session:

1. At the FTP client, type **`ftp val-ip-address`**, where ***`val-ip-address`*** matches the VAL IP address that is administered on the IP Node Names screen. Press **Enter**.
2. At the username prompt, type the ftp-username. Press **Enter**.
3. At the password prompt, type the ftp-password. Press **Enter**.

   The system displays the message **User logged in**.

   Note:
   Once you are logged in, you are in the announcements directory (**`/annc`**).
4. If you are moving files to or from the VAL circuit pack, you must set the system to binary mode. To set the system to binary mode, at the FTP client, type **bin**. Press **Enter**.

   The system sets the **Types** field to **I**, binary mode.

   CAUTION:
   If you do not transfer announcement files in binary mode, the files can be corrupted, and the FTP session can fail.

Performing tasks in an FTP session

Once the FTP session is established, you can perform any of these announcement tasks:

- Moving announcements from the VAL circuit pack
- Using FTP to delete VAL announcements
- Setting up v VAL
- Moving announcements to an announcement source or another LAN device
- Combining copy and move tasks

Moving announcements from the VAL circuit pack: When you move a file from the VAL circuit pack, you are either:

- Backing up (archiving) an announcement file

- Copying an announcement to another VAL circuit pack (restoring)

Moving a file in an FTP session means that you copy the file from the VAL circuit pack to the default directory of the FTP client computer.

To back up or save an announcement from the VAL circuit pack to the client computer through an FTP session:

1. At the FTP client computer, type **get *filename.wav***, where ***filename.wav***. is the name of the announcement file. Press **Enter**.

   The system writes the announcement file to the directory from which you started the FTP session.

   Note:
   FTP upload or download of announcement files does not preserve the created time stamp. The file receives the current date and time when the file is written to the circuit pack or to the computer.

2. List the contents of the FTP client directory and ensure that the announcement file is listed.
3. End the FTP session. See Ending an FTP session for the procedure.

Using FTP to delete VAL announcements: You can use FTP to delete an announcement from an announcement source, or a LAN device.

Note:
The system denies any attempt to delete an announcement while the announcement is playing, being transferred, or backed up to Flash memory.

To delete an announcement on an announcement source through an FTP session:

1. Ensure that you complete the steps in Setting up an FTP session.
2. At the computer client, type **delete *filename.wav***, where ***filename.wav***. is the name of the announcement file. Press **Enter**.

   Note:
   The system immediately removes the announcement file from volatile RAM memory. Approximately 5 minutes later, the system removes the announcement file from nonvolatile ROM Flash memory.

3. List the contents of the announcement directory, and ensure that the file is not listed.

   Note:
   The **.wav** file extension on the announcement files is visible when you view the announcement directory from the FTP client.

4. End the FTP session. See Ending an FTP session for the procedure.
5. At the SAT, type **change announcements**. Press **Enter**.

   The system displays the Announcements/Audio Sources screen (Figure 26: Announcements/Audio Sources screen on page 184).

6. Delete the entire line that is associated with the announcement.

7. Press **Enter** to save your changes.

Setting up v VAL : A virtual VAL (v VAL) source uses the IP address of the media gateway. Type **`list media-gateway`** to find this IP address. Make sure that the v VAL is administered, and that the **V9** field on the Media Gateway screen is administered and enabled.

Moving announcements to an announcement source or another LAN device: You can copy an announcement file on the announcement source to another LAN device. Ensure that you *did not just administer* the announcement on the Announcements/Audio Sources screen. If announcement administration precedes the file transfer:

- The announcement appears with a zero (0) length on the Integrated Announcements screen.
- The **Time Remaining** field on the Integrated Announcements screen does not refresh to reflect the presence of the new announcement file on the announcement source.

Use the following procedure to ensure that the announcement length is accurate:

1. Administer the announcement on Communication Manager with the **`change announcements`** command. Use the identical file name in the **Name** field *without* spaces or the **`.wav`** file extension.
2. Try to play the announcement that was administered first and transferred second. The system returns a busy signal at the first play attempt.
3. Try to play the announcement that was administered first and transferred second in a telephone access session. Again, the system returns a busy signal at the first play attempt.
4. Rerecord this announcement with the same filename at a system telephone. See Recording and changing announcements for the procedure.

To copy an announcement to an announcement source or another LAN device:

1. At the FTP client, type **`put filename.wav`**, where ***`filename.wav`*** is the name of the announcement file. Press **Enter**.
2. List the contents of the VAL announcement directory or the LAN device, and ensure that the announcement file is listed.

   Note:
   FTP upload or download of announcement files does not preserve the created time stamp. The file receives the current date and time when the file is written to the announcement source or to a computer.
3. After you ensure that the announcement is on the VAL source, administer the announcement on Communication Manager with the **`change announcements`** command. Use the identical file name in the **Name** field *without* spaces or the **`.wav`** file extension.
4. End the FTP session. See Ending an FTP session for the procedure.

Combining copy and move tasks: When you combine copy (the **get** command) and move (the **put** command) announcement files, you can rearrange VAL announcements.

Note:
To move an announcement to a VAL source from another VAL source in an FTP session, you must first establish an FTP session into the source from which you are restoring an announcement.

1. List the directory contents of the announcement source that contains the announcement that you want to copy. Ensure that the announcement file is listed.
2. At the FTP client, type **get *filename.wav***, where ***filename.wav*** is the name of the announcement file. Press **Enter**.

   The system writes a copy of the file to the directory from which you started the FTP session.
3. List the contents of the FTP client directory, and ensure that the announcement is listed.
4. End the FTP session to the announcement source *from which you copied the announcement file*. See Ending an FTP session for the procedure.
5. Set up a new FTP session into the destination announcement source. See Setting up an FTP session for the procedure.
6. At the FTP client, type **put *filename.wav***, where ***filename.wav*** is the name of the announcement file. Press **Enter**.
7. List the contents of the VAL announcement directory, and ensure that the announcement is listed.
8. End the FTP session to the announcement source *to which you copied the announcement file*. See Ending an FTP session for the procedure.

Ending an FTP session: FTP sessions to a announcement source originate at the FTP client end.

To end an FTP session, you can:

1. Type **bye** or **quit** to log out from the FTP client. Press **Enter**
2. Type **disable filesystem board *board-location***, where ***board-location*** is the 5-character number that is assigned to the announcement source. Press **Enter**. This command clears the ftp-username and the ftp-password.
3. Allow the system to time out after 10 minutes of inactivity.

SECURITY ALERT:
A higher degree of system security is provided if you both log out of the FTP session and disable the announcement source.

Note:
If you only disable the announcement source file system, you can continue your FTP session. However, new FTP session logins are not allowed.

Recording announcements for TTY callers

Record announcements for Teletypewriter device (TTY) callers in the same way as you record voice announcements. However, instead of recording from the handset of your telephone, you record from a TTY device. You can use an acoustic coupler into which you place the telephone handset to attach the device to your telephone, or plug the TTY device directly into the back of a digital telephone. After you call the announcement extension, and press **1** to record, you type the announcement into the TTY device.

If you use an acoustic coupler to connect your telephone for recording, you can record TTY and voice into a single announcement. In this case, after you press **1** to record, you can type the TTY message, and then immediately pick up the handset to record the voice message. For this type of recording, digital telephones also offer the option to press the pound key (**#**) to complete the recording, which eliminates any extraneous noise at the end of the recording. Unfortunately, this method for combined TTY and voice recordings is likely to create extraneous noise in the middle of your announcements.

A better alternative to recording with your telephone is to create **.wav** files on other recording applications, such as a PC, and then copy and save the **.wav** files to your announcement source. See Moving announcements to an announcement source or another LAN device for the procedure. In this case, the announcement files must meet the same criteria as voice recordings. See Announcement file format requirements for more information.

Reports for Announcements

The following reports provide information about the Announcements feature:

- Event Report

  If a working VAL announcement file is deleted over FTP, the next attempt to play the announcement fails, and the system adds a software event to the Event Report. You can view the Event Report to see if the announcement was deleted, and to see if other events occurred that are related to announcements.

  For information on how to access this report, see Viewing the Event Report on page 206.

- Voice Announcement Measurements

  You can view a report of announcement measurements. This report includes how many times an announcement was queued to play, how many callers dropped while in the queue, and how many times all announcement ports were busy during the report period.

  For information on how to access this report, see Viewing Voice Announcement Measures on page 207.

Viewing the Event Report

If a working announcement file is deleted through FTP, the next attempt to play the announcement fails, and the system adds a software event to the Event Report. You can view this log to see if the announcement has been deleted, and to see if other events have occurred related to announcements.

To access the report:

1. Type **`display events`**. Press **Enter**.

   The Event Report input screen appears (Figure 32: Event Report on page 206). This input screen helps you focus the report on events of a certain type or from a certain time period.

Figure 32: Event Report

```
display events                                          Page  1 of  1
                              EVENT REPORT

  The following options control which events will be displayed.

         EVENT CATEGORY

            Category: denial

         REPORT PERIOD

            Interval: ___     From: __/__/__:__ To: __/__/__:__

         SEARCH OPTIONS

                           Vector Number: ___
                              Event Type: _____
```

2. In the **Category** field, select or type **denial**.
3. You can further limit the report by setting the Interval field to one of the following selections (select from the help list or type the first letter):
   - **all**
   - **month**
   - **day**
   - **hour**
   - **minute**

4. Press **Enter**.

   The system displays the Events Report screen for the parameters that you set (Figure 33: Events Report on page 207).

Figure 33: Events Report

```
display events                                              Page   1  of  1
                                EVENTS REPORT

Event Event                        Event     Event      First       Last     Evnt
Type  Description                  Data 1    Data 2     Occur       Occur     Cnt

2028  Annc file has bad format  8C0009    0        05/14/11:55 05/14/12:04  2
2027  Annc not found on board   8C0007    0        05/14/12:09 05/14/12:09  1
```

5. Look at the 2027 entry in the **Event Type** field.
   - The **Event Description** field explains that the announcement is not on the announcement source.
   - The **Event Data 1** field contains the announcement number (hexadecimal in the lower three digits).

     This denial event only appears once in the Events Report.

Viewing Voice Announcement Measures

You can view the Voice Announcement Measurements report, including how many times an announcement was queued to play, how many callers dropped while in queue, and how many times all announcement ports were busy during a specified period.

To access the report for all announcements that were accessed today during peak hours:

1. Type **`list measurements announcements all today-peak`**. Press **Enter**.

   The Voice Announcement Measurements screen appears (Figure 34: Voice Announcement Measurements screen).

Figure 34: Voice Announcement Measurements screen

```
list measurements announcements all today-peak

Switch Name: ST10                              Date: 1:06 pm  THU OCT 6, 2005

                    VOICE ANNOUNCEMENT MEASUREMENTS

                                      Meas Play  Calls          Queue Mport Mx Max
Extension  Name (first 24 chars)___   Hour Reqts Que   ASP PSP Drops Plays Pt Cls
27100      collect_some_digits        2300 0     0     0   0   0     0     0  0
27102      dtmf5_mu                   2300 0     0     0   0   0     0     0  0
27103      voa_3c12                   2300 0     0     0   0   0     0     0  0
27104      voa_2b04                   2300 0     0     0   0   0     0     0  0
27105      collect_digits_2b04        2300 0     0     0   0   0     0     0  0
27106      dtmf5_mu                   2300 0     0     0   0   0     0     0  0
```

For detailed information on these reports and the associated commands, see *Avaya Aura™ Communication Manager Reports,* 555-233-505.

Interactions for Announcements

This section provides information about how the Announcements feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Announcements in any feature configuration.

- Automatic Call Distribution (ACD)

  Recorded announcements are used extensively for ACD, Call Vectoring, Call Prompting, Expert Agent Selection (EAS), Vector Directory Number (VDN) of Origin Announcement, Direct Department Calling, and Uniform Call distribution (UCD) features. See the individual features for interaction details.

- Automatic Wakeup

  If you use an integrated, multiple-integrated, or external type of announcement for Automatic Wakeup, you can also administer the announcement to repeat and to allow “barge-in” as a queue type. The benefit of repeating announcements and “barge-in” queues is that you do not need a separate port for each wakeup announcement. When guests go off-hook to receive an announcement at a particular time, the guests use only one port. The message repeats on the port until the last guest goes off-hook, and the message ends.

Troubleshooting Announcements

This section lists the known or common problems that users might experience with the Announcements feature.

Problem	Possible cause	Action
No sound or poor sound quality.	Bad file format.	Ensure that the file formats are compatible. A good announcement file format must have the following parameters: • 8-Kbps sample rate • 8-bit resolution (bits per sample) • A-law or μ-Law companding format • Mono (channels = 1)
	Incorrect companding mode.	Ensure that the same companding mode is administered on page 1 of the Location Parameters screen (type **`change location-parameters`**) for both environments.
An announcement does not play.	If a working VAL announcement file is deleted over FTP, the next attempt to play the announcement fails, and the system adds a software event to the Denial Events Log.	View the Denial Events log to determine if the announcement was deleted. If the announcement was deleted, restore or rerecord the announcement.
The system displays error code E28 when you attempt to restore announcements.	An integrated announcement source is not installed in the system.	Install an integrated announcement source.
The system displays error code E31 when you attempt to restore announcements.	A call is connected to the announcement on the announcement source and the port is busy.	Wait for the call to disconnect, and try to restore announcements again. If the system crashes, or if there is a processor interchange during the restore announcements process, the restore process fails. There is no valid announcement on the announcement source. Repeat the process when the system is operating properly.

Announcement capacities and load balancing

Understanding how Communication Manager handles announcements helps with questions of capacity the load-balancing of announcement traffic. The Avaya S87XX Series and S8300 Servers support up to 3,000 announcements across the Communication Manager system. Each of as many as 10 integrated announcement circuit packs (and each G700 virtual VAL source) is limited to 256 announcements.

If you are running Communication Manager 4.0 or later, and have a S8720 system with increased capacities configuration, you can have up to 128 VAL boards (TN2501) and 250 vVAL sources per system for a total of 378 announcement sources. VAL boards are a RTU (right to use) feature.

If you have a system that does not support increased capacities, the limit remains at 10 TN2501 VAL boards.

All Avaya G700 Media Gateways in the system can be assigned as VAL sources, for a maximum of 250 G700 VAL sources in a large S87XX Series server configuration also with up to 10 VAL circuit packs, providing an ultimate capacity of 260 sources for the Avaya S87XX Series servers.

Each VAL circuit pack has 31 playback ports (with 60 minutes of storage capacity) and each G700 VAL source has 15 playback ports (with 20 minutes storage capacity). Initially each caller that is to hear a non-barge-in announcement on that source is connected to an available port until each port has one caller connected. Initially 31 callers can be hearing an announcement from a single VAL circuit pack (15 with a G700 VAL source). The same announcement can be playing from multiple ports, each starting at a different time. Once all ports are busy playing announcements, subsequent callers that are to hear an announcement residing on that circuit pack/source are queued for that source.

Communication Manager queue size over all integrated announcement sources is 4,000 callers (S87XX Series/S8300 servers). When a port becomes available, all callers (up to 1,000) waiting in the queue for a specific announcement on that source are connected to the available port to hear the announcement play from the beginning on a first-in, first-out basis.

At any given time you can have as many as 1,000 callers hearing the same announcement on a given port of a circuit pack/source, yielding a (theoretical, system-wide) capacity of 31,000 callers connected to a VAL circuit pack (or 15,000 callers connected to a G700 Media Gateway virtual VAL source). Factor in barge-in announcements which continuously play from a single port (that can have as many as 1,000 callers connected at the same), and this provides a very, very large capacity for playing announcements.

The **`measurements announcements`** commands can be used to monitor the system and help determine burst conditions, allowing for better load balancing of the traffic.

Non-volatile storage of announcements on VAL

The VAL circuit pack has a RAM-based file system on which the announcements are stored. This is where a newly recorded or FTPd announcement resides. The VAL constantly checks to determine whether changes have been made to the file system (file added or deleted or renamed). Once a change has been detected, the VAL waits for 5 minutes of stability. After such a stable period, the VAL backs up the RAM based file system to its FLASH. The FLASH version of the file system is non-volatile and is what is restored upon reset/reseat.

If you record a new announcement and immediately reset the circuit pack, the announcement will be lost. The yellow LED blinks while a backup from RAM to FLASH occurs. All of the above is true regardless which (if any) of the **`.wav`** files on the circuit pack are administered announcements. It is just the way the circuit pack (firmware) operates.

Note:
Only files with a **`.wav`** extension in the **/annc** directory are backed up to FLASH.

Attendant Auto Start and Don’t Split

Use the Attendant Auto Start and Don’t Split features to allow an attendant to press any key on the keypad to start a call without the need to first press the **Start** button. If the attendant is on an active call and presses digits on the keypad, the system automatically splits the call and dials the second call.

The Don’t Split feature deactivates the Auto Start feature, and allows the system to send touch tones over the line.

Detailed description of Attendant Auto Start and Don’t Split

This section provides a detailed description of the Attendant Auto Start and Don’t Split features.

Auto Start and Don’t Split are two features that work together. These two features reduce the number of buttons that attendants must press to handle calls.

Auto Start

If the attendant is on a call and presses any key on the keypad, the system automatically splits the current call, places the call on hold, and dials the next call. The system disables the **Start** button, and does not allow end-to-end signaling.

To extend a current call to another extension, the attendant dials the extension. The system automatically places the current call on hold. Once the called party answers, the attendant presses the **Release** button to extend the call.

Don’t Split

To deactivate the Auto Start feature and not split a current call, the attendant presses the **Don’t Split** button. One use of the Don’t Split feature is to send touchtones to pick up answering machine messages. When the Don’t Split feature is active, parties on the call hear the keys that the attendant presses.

To reactivate the Auto Start feature and allow end-to-end signaling, the attendant can:

- Press the **Don’t Split** button again

- Press Cancel
- Allow the current call to terminate

Administering Attendant Auto Start and Don’t Split

The following steps are part of the administration process for the Attendant Auto Start and Don’t Split features:

- Assigning a Don’t Split button

This section describes:

- Any prerequisites for administering the Attendant Auto Start and Don’t Split features
- The screens that you use to administer the Attendant Auto Start and Don’t Split features
- Complete administration procedures for the Attendant Auto Start and Don’t Split features

Prerequisites for administering Attendant Auto Start and Don’t Split

You must complete the following actions before you can administer the Attendant Auto Start and Don’t Split features:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Auto Start and Don’t Split

Screen name	Purpose	Fields
Attendant Console	Assign a **Don’t Split** button.	Any unassigned button in the **Feature Button Assignments** area

Assigning a Don’t Split button

To assign a **Don’t Split** button:

1. Type **change attendant *n***, where ***n*** is the number of the attendant console. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 35: Attendant Console screen on page 215).

Figure 35: Attendant Console screen

```
change attendant 1                                          Page 3 of 4
                                ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split_____                          13: __________
  2: dont-split                          14: __________
  3: act-tr-grp                          15: __________
  4: deact-tr-g                          16: __________
  5: __________                          17: __________
  6: hold _____ *                        18: __________
  7: __________                          19: forced-rel
  8: aux-work       RC:    Grp:          20: __________
  9: __________                          21: __________
 10: __________                          22: __________
 11: __________                          23: night-serv *
 12: __________                          24: pos-busy__ *
```

3. In the **Feature Button Assignments** area, assign **dont-split** to an available button.

   In this example, we assign **dont-split** to button **2**.

4. Press **Enter** to save your changes.

Reports for Attendant Auto Start and Don’t Split

The following reports provide information about the Attendant Auto Start and Don’t Split features:

- None

Considerations for Attendant Auto Start and Don’t Split

This section provides information about how the Attendant Auto Start and Don’t Split features behave in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Auto Start and Don’t Split under all conditions. The following considerations apply to Attendant Auto Start and Don’t Split:

- If an attendant enables Auto Start, and then dials an Automatic Alternate Routing (AAR) number where the values in the **min** and the **max** fields in the AAR Analysis Table are not equal, the attendant must press the pound key (**#**) after the digit string. If the attendant does not press the pound key, the system does not process the call.

Interactions for Attendant Auto Start and Don’t Split

This section provides information about how the Attendant Auto Start and Don’t Split features interact with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Auto Start and Don’t Split in any feature configuration.

- Call Detail Recording (CDR) Account Code Dialing

  If the system is using Call Detail Recording Account Code Dialing, the Auto Start and the Don’t Split features are not activated.

- Visually Impaired Service (VIS)

  If VIS is activated or deactivated while Don’t Split is active, the system automatically deactivates the Don’t Split feature.

Attendant Auto-Manual Splitting

Use the Attendant Auto-Manual Splitting feature to allow the attendant to announce an incoming call to a user without being heard by the calling party. The attendant can also use the Attendant Auto-Manual Splitting feature to consult privately with the called party without being heard by the calling party.

Detailed description of Attendant Auto-Manual Splitting

This section provides a detailed description of the Attendant Auto-Manual Splitting feature.

The Attendant Auto-Manual Splitting feature allows the attendant to split the calling party away from a conversation. The attendant can then confidentially determine if the called party wants to accept the call.

The system automatically activates the Attendant Auto-Manual Splitting feature when the attendant, who is active on a call, presses any of the following buttons:

- Start
- An extension
- Any Hundreds Select button plus an extension
- Trunk Group Select

Administering Attendant Auto-Manual Splitting

The following steps are part of the administration process for the Attendant Auto-Manual Splitting feature:

- The system activates the Attendant Auto-Manual Splitting feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509

This section describes:

- Any prerequisites for administering the Attendant Auto-Manual Splitting feature
- The screens that you use to administer the Attendant Auto-Manual Splitting feature
- Complete administration procedures for the Attendant Auto-Manual Splitting feature

Screens for administering Attendant Auto-Manual Splitting

Screen name	Purpose	Fields
Attendant Console	Set up an attendant console.	All

Attendant Backup

Use the Attendant Backup feature to give access to most attendant console features from specially administered backup telephones. This allows you to answer calls more promptly, thus providing better service to your callers.

When the attendant console is busy, you can answer overflow calls from the backup telephones by pressing a button or dialing a Feature Access Code (FAC). You can then process the calls as if you are at the attendant console.

You can assign the Attendant Backup feature to only multiappearance telephones. Avaya recommends the following multiappearance telephone models as a backup for the attendant:

- 6408
- 6416
- 6424

Detailed description of Attendant Backup

This section provides a detailed description of the Attendant Backup feature.

You can configure your system to have backup telephones for the attendant. With the Attendant Backup feature, designated users can answer calls that the attendant cannot immediately answer. These designated users can also provide some of the services that the attendant usually provides.

Designated users can access some attendant console features from the backup telephones when the:

- Queue of received calls reaches one of the following administered warning levels:
  - Number of calls in the queue
  - Time that a particular call has been in the queue
- Attendant console is in Night Service

A user with console permissions can:

- Activate Automatic Wakeup for another extension
- Activate and deactivate controlled restrictions for another extension, or a group of extensions
- Activate and deactivate Do Not Disturb for another extension, or a group of extensions

- Activate Call Forwarding for another extension
- Add and remove agent skills
- Record integrated announcements

To assign the Attendant Backup capabilities, you use **Console Permissions** field on the Class of Service screen.

Attendant Backup supports the following capabilities:

- Attendant Backup Alerting

Attendant Backup Alerting

The Attendant Backup Alerting feature notifies the backup telephones that the attendant needs assistance to handle calls. The system provides both audible and visual alerting to backup telephones when the calls in the attendant queue reach the administered warning levels. When the queue drops below the administered warning level, alerting stops.

Audible alerting also occurs when the attendant console is in Night Service, regardless of the size of the attendant queue.

Once the system alerts the backup telephones, designated users can answer an attendant call by:

- Pressing the **atd-qcalls** button
- Dialing the Feature Access Code (FAC) for Trunk Answer Any Station (TAAS) feature.

Administering Attendant Backup

The following steps are part of the administration process for the Attendant Backup feature:

- Setting up Attendant Backup telephones

This section describes:

- Any prerequisites for administering the Attendant Backup feature
- The screens that you use to administer the Attendant Backup feature
- Complete administration procedures for the Attendant Backup feature

Prerequisites for administering Attendant Backup

You must complete the following actions before you can administer the Attendant Backup feature:

- Assign a Class of Service (COS) value to the multiappearance telephones that you use for Attendant Backup. On the Class of Service screen, you must set the **Client Room** field to **n**, and the **Console Permissions** field to **y**.

  For more information, see the Considerations for Attendant Backup, as well as the "Class of Service" feature.

- On the Feature Access Code (FAC) screen, type a FAC in the **Trunk Answer Any Station** field. Then share the FAC with each of the attendant backup users. For more information, see the "Feature Access Code" feature.

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Backup

Screen name	Purpose	Fields
Class of Service	Ensure that the Attendant Backup feature is set up correctly.	**Client Room**
	Assign console permissions to the backup telephones.	**Console Permissions**
Console Parameters	Administer the Attendant Backup Alerting feature.	**Backup Alerting**
	Set the queue warning parameters.	• **Calls in Queue Warning** • **Time in Queue Warning (sec)**
Feature Access Code (FAC)	Assign a FAC for backup telephone users.	**Trunk Answer Any Station**
Station	Assign an **atd-qcalls** feature button for backup telephone users.	Any available button field in the **Feature Button Assignments** area.

Setting up Attendant Backup telephones

To allow your system to alert the backup telephones, perform the following procedures:

- Configuring your system
- Defining Class of Service console permissions
- Assigning console permissions to backup telephones
- Training designated users

Configuring your system

To configure the system for the Attendant Backup feature:

1. Type **change console-parameters**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 36: Console Parameters screen on page 222).

Figure 36: Console Parameters screen

```
change console-parameters                                    Page 1 of 5
                            CONSOLE PARAMETERS

         Attendant Group Name: OPERATOR
                          COS: 0                                  COR: 0
       Calls in Queue Warning: 5                      Attendant Lockout? y
        Ext Alert Port (TAAS):
                          CAS: none
                                                Night Service Act. Ext.:
                 IAS (Branch)? n                IAS Tie Trunk Group No.:
          IAS Att. Access Code:                    Alternate FRL Station:
               Backup Alerting? y          DID-LDN Only to LDN Night Ext? n
      Attendant Vectoring VDN:
```

2. In the **Backup Alerting** field, type **y**.

   The system can now notify any telephone that has an **atd-qcalls** feature button when the:

   — Attendant queue reaches the warning level

   — Console is in night service

3. In the **Calls in Queue Warning** field, type the maximum number of calls that can be in the attendant queue before the system alerts the backup telephones.

   In this example, we limit the number to five calls.

4. Click **Next** until you see the **Time in Queue Warning (sec)** field (Figure 37: Console Parameters screen on page 223).

Figure 37: Console Parameters screen

```
change console-parameters                                    Page 2 of 5
                              CONSOLE PARAMETERS

TIMING
  Time Reminder on Hold (sec): 10          Return Call Timeout (sec): 10
  Time in Queue Warning (sec): 120

  INCOMING CALL REMINDERS
      No Answer Timeout (sec): 20                    Alerting (sec): 40
                               Secondary Alert on Held Reminder Calls? y

ABBREVIATED DIALING
     List1: group    1        List2:                 List3:
            SAC Notification? n
                          COMMON SHARED EXTENSIONS
            Starting Extension:                Count:
```

5. In the **Time in Queue Warning (sec)** field, type the maximum number of seconds that a caller can be in the attendant queue before the system alerts the backup telephones.

   In this example, we assign a limit of 120 seconds.

6. Press **Enter** to save your changes.

Defining Class of Service console permissions

To define Class of Service (COS) console permissions for the backup telephones:

1. Type **`change cos`**. Press **Enter**.

   The system displays the Class of Service screen (Figure 38: Class of Service screen on page 224).

Figure 38: Class of Service screen

```
change cos                                                    Page 1 of 1
                          CLASS OF SERVICE

                                  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

   Auto Callback                  n y y n y n y n y n  y  n  y  n  y  n
   Call Fwd-All Calls             n y n y y n n y y n  n  y  y  n  n  y
   Data Privacy                   n y n n n y y y y n  n  n  n  y  y  y
   Priority Calling               n y n n n n n n n y  y  y  y  y  y  y
   Console Permissions            n n n n n n n y n n  n  n  n  n  n  n
   Off-hook Alert                 n n n n n n n n n n  n  n  n  n  n  n
   Client Room                    n n n n n n n n n n  n  n  n  n  n  n
   Restrict Call Fwd-Off Net      n y y y y y y y y y  y  y  y  y  y  y
   Call Forward Busy/DA           n n n n n n n y n n  n  n  n  n  n  n
   Personal Station Access (PSA)  n n n n n n n y n n  n  n  n  n  n  n
   Extended Forwarding All        n n n n n n n n n n  n  n  n  n  n  n
   Extended Forwarding B/DA       n n n n n n n y n n  n  n  n  n  n  n
   Trk-to-Trk Restriction Override n n n n n n n y n n  n  n  n  n  n  n
   QSIG Call Offer Originations   n n n n n n n n n n  n  n  n  n  n  n
```

2. In the **Console Permissions** row, change **n** to **y** in a numbered column.

   Each column is a COS identification number. Sixteen classes of service (COS) are available. In this example, we assign **Console Permissions** to COS 7.

3. To assign any other permissions for this COS, change **n** to **y** in the corresponding column.
4. Press **Enter** to save your changes.

Assigning console permissions to backup telephones

To assign console permissions to backup telephones:

1. Type **change station *n***, where ***n*** is the extension of the backup telephone. Press **Enter**.

   In this example, we change extension 4345. The system displays the Station screen (Figure 39: Station screen on page 225).

Figure 39: Station screen

```
change station 4345                                          Page 1 of 5
                                  STATION

Extension: 4345              Lock Messages? n                    BCC: 0
     Type:                   Security Code:                       TN: 1
     Port:                 Coverage Path 1:                      COR: 1
     Name:                 Coverage Path 2:                      COS: 7
                           Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                           Message Lamp Ext: 1014
          Speakerphone: 2-way                    Mute button enabled? y
       Display Language? English                    Expansion Module?
                   Model:
                                                   Media Complex Ext:
                                                        IP Softphone? y
```

2. In the **COS** field, assign the COS that you created for the console permissions.

   In this example, we assign COS **7** to this telephone.

3. Click **Next** until you see the **Feature Button Assignments** area (Figure 40: Station screen on page 225).

Figure 40: Station screen

```
change station 4345                                          Page 3 of 5

                                  STATION

FEATURE BUTTON ASSIGNMENTS

 9: crss-alert
10: atd-qcalls
11:
12:
13:
14:
15:
16.
```

4. In the **Feature Button Assignments** area, assign **atd-qcalls** to an available button.

   In this example, we assigned **atd-qcalls** to button 10. The **atd-qcalls** button provides visual alerting for this telephone. When the **atd-qcalls** button:

   - Is dark, the attendant queue contains no calls

- Shows a steady light, the attendant queue contains calls.
- Shows a flashing light, the number of calls in the attendant queue exceeds the limit that you set for the queue. At this point, the backup telephone user also hears an alert signal every 10 seconds.

5. Press **Enter** to save your changes.
6. Repeat this process for each backup telephone.

Training designated users

Finally, you must train the backup users. The backup users must know:

- How to interpret the **atd-qcalls** button lights
- If the telephones of the backup users do not have an **atd-qcalls** button, the FAC for the TAAS feature
- Your procedure for how to answer attendant calls
- Your procedure for how to transfer attendant calls

End-user procedures for Attendant Backup

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Attendant Backup:

- If the **atd-qcalls** button on your telephone is flashing, the number of calls in the attendant queue exceeds the maximum limit. You also hear an alert signal every 10 seconds. To answer the call, either:
  - Press the **atd-qcalls** button on your telephone
  - Dial the FAC for the TASS feature

Considerations for Attendant Backup

This section provides information about how the Attendant Backup feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Backup under all conditions. The following considerations apply to Attendant Backup:

- Backup telephone users must meet the following criteria to answer alerting calls in the attendant queue:
  - Have a multiappearance telephone
  - Have an **atd-qcalls** feature button assigned to the telephone
  - Be assigned a Class of Service (COS) that has the **Client Room** COS field set to **n**. Classes of Service are defined on the Class of Service screen.

    If the **Client Room** COS field is set to **y**, the user receives intercept treatment when the user tires to use the Attendant Backup feature.
- When the attendant console is in day mode and the Attendant Backup feature is disabled, backup telephone users do not hear the audible alert signal. Backup telephone users also cannot dial the Feature Access Code (FAC) for Trunk Answer Any Station (TAAS) to answer attendant calls.

Interactions for Attendant Backup

This section provides information about how the Attendant Backup feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Backup in any feature configuration.

- Ringer Cutoff

  Activating the Ringer Cutoff feature disables the audible alerting signal. If a backup telephone has Ringer Cutoff activated, the system audibly alerts the telephone only when the attendant queue exceeds the queue warning level.

  If Ringer Cutoff is not activated, the system audibly alerts the backup telephone every 10 seconds until the attendant queue falls below the queue warning level.
- Trunk Answer Any Station (TAAS)

  If the system is in night mode and a TAAS port is not assigned, backup telephone users must dial the Feature Access Code (FAC) for Trunk Answer Any Station (TAAS) to answer queued calls.
- Tenant Partitioning

  You cannot use the Attendant Backup feature if Tenant Partitioning is enabled.

Attendant Call Waiting

Use the Attendant Call Waiting feature to allow an attendant to notify a single-line telephone user, who is on an existing call, that another call is waiting. Once the attendant notifies the user, the attendant can answer other calls.

Detailed description of Attendant Call Waiting

This section provides a detailed description of the Attendant Call Waiting feature.

The system automatically activates the Attendant Call Waiting feature whenever an attendant originates or extends a call to a single-line telephone user who is on an existing call. When the system activates Attendant Call Waiting, the:

- Attendant hears a call waiting ringback tone
- Telephone user hears a call waiting tone
- Calling party does not hear a tone

The attendant can place a call in progress on hold. After the attendant answers the call on hold, the attendant can use the Hold button to return to the held call. The attendant can alternate between the two calls.

For example, assume that extension 123, a single-line telephone, is busy. An attendant extends an incoming call to extension 123. The attendant hears the call waiting ringback tone, which indicates that Attendant Call Waiting is activated. The attendant can:

- Announce the call-waiting condition to the calling party
- Cancel the Attendant Call Waiting feature, and ask the calling party to call again later
- Release the caller, or place the call on hold at the console

  Releasing an attendant-originated call drops the call completely.

The user at extension 123 hears a call-waiting tone, and knows that a call is waiting. The user can:

- Terminate the existing call
- Place the existing call on hold, and answer the waiting call

If the user does not answer the waiting call before a preassigned time interval, the system returns the call to the attendant.

Administering Attendant Call Waiting

The following steps are part of the administration process for the Attendant Call Waiting feature:

- Setting up single-line telephones
- Changing the call-waiting signal
- Modifying timed intervals

This section describes:

- Any prerequisites for administering the Attendant Call Waiting feature
- The screens that you use to administer the Attendant Call Waiting feature
- Complete administration procedures for the Attendant Call Waiting feature

Prerequisites for administering Attendant Call Waiting

You must complete the following actions before you can administer the Attendant Call Waiting feature:

- The system activates the Attendant Call Waiting feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Call Waiting

Screen name	Purpose	Fields
Station	Allow the attendant to send calls to busy single-line telephones.	**Att. Call Waiting Indication**
Feature-Related System Parameters	Change the call-waiting signal.	**Attendant Originated Calls**
Console Parameters	Indicate the maximum number of seconds that a call can remain on hold before the system alerts the attendant.	**Timed Reminder on Hold**
	Indicate the maximum number of seconds that a call can remain on hold before the call returns to the attendant.	**Return Call Timeout**

Setting up single-line telephones

To allow the attendant to send calls to busy single-line telephones:

1. Type **change station *n***, where ***n*** is the single-line extension that you want to change. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Att. Call Waiting Indication** field (Figure 41: Station screen on page 231).

Figure 41: Station screen

```
change station 35001                                          Page 2 of 3
                                    STATION

FEATURE OPTIONS
           LWC Reception? audix
          LWC Activation? y                      Coverage Msg Retrieval? y
  LWC Log External Calls? n                                Auto Answer: none
             CDR Privacy? n                           Data Restriction? n
   Redirect Notification? y                      Call Waiting Indication? n
 Per Button Ring Control? n                  Att. Call Waiting Indication? y
   Bridged Call Alerting? n                     Distinctive Audible Alert? y
        Switchhook Flash? y                           Adjunct Supervision? y
    Ignore Rotary Digits? y
        H.320 Conversion? n         Per Station CPN - Send Calling Number? _
       Service Link Mode: as-needed
         Multimedia Mode: basic                   Audible Message Waiting? y
    MWI Served User Type:
              AUDIX Name: srl-aud
                                                 Coverage After Forwarding? _
                                                   Multimedia Early Answer? n
                                           Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001                        IP Audio Hairpinning? n
```

3. Set the **Att. Call Waiting Indication** field to **y**.
4. Press **Enter** to save your changes.
5. Repeat this process for each single-line telephone on your system.

Changing the call-waiting signal

You can change the number of alerting tones (1, 2, or 3 beeps) that the user hears when the attendant extends a call. You can set the number of tones to indicate an internal call, an external call, and a priority call. The system defaults are:

- Internal: 1
- External: 2
- Priority: 3

To change the call-waiting signal:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Distinctive Audible Alerting** area (Figure 42: Feature-Related System Parameters screen on page 232).

Figure 42: Feature-Related System Parameters screen

```
change system-parameters features                                  page 5

                          FEATURE-RELATED SYSTEM PARAMETERS

Public Network Trunks on Conference Call: 5              Auto Start? n
    Conference Parties with Public Network Trunks: 6             Auto Hold? n
 Conference Parties without Public Network Trunks: 6         Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180        Bridging Tone? n
                  Short Interdigit Timer (seconds): 3        Conference Tone? n
            Unanswered DID Call Timer (seconds): ____        Intrusion Tone? n
            Line Intercept Tone Timer (seconds): 30     Special Dial Tone? n
               Long Hold Recall Timer (seconds):      Mode Code Interface? n
                     Reset Shift Timer (seconds): 0
    Station Call Transfer Recall Timer (seconds): 0
                              DID Busy Treatment: tone
       Invalid Number Dialed Intercept Treatment: Announcement _____
              Allow AAR/ARS Access from DID/DIOD? _
                Allow ANI Restriction on AAR/ARS? _
     Use Trunk COR for Outgoing Trunk Disconnect? _
                 7405ND Numeric Terminal Display? n            7434ND? n
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                       Attendant Originated Calls: external
   DTMF Tone Feedback Signal to VRU - Connection: _    Disconnection: _
```

3. Change the number of tones (1, 2, or 3 beeps) that a user hears when the system activates the Attendant Call Waiting feature.

   If you change one field, **Internal**, **External**, or **Priority**, Avaya recommends that you change all fields. A user then knows what kind of call the attendant is extending.

4. Press **Enter** to save your changes.

Modifying timed intervals

If either the Timed Reminder on Hold interval, or the Return Call Timeout interval, expires before the call is answered, the call returns to the attendant console.

To modify the timed intervals:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen.

2. Click **Next** until you see the **Timed Reminder on Hold** field and the **Return Call Timeout** field (Figure 43: Console Parameters screen on page 233).

Figure 43: Console Parameters screen

```
change console-parameters                                    Page 2 of 4
                              CONSOLE PARAMETERS

TIMING
  Time Reminder on Hold (sec): 30          Return Call Timeout (sec): 60
  Time in Queue Warning (sec): 30

  INCOMING CALL REMINDERS
      No Answer Timeout (sec): 20                    Alerting (sec): 40
                               Secondary Alert on Held Reminder Calls? y

ABBREVIATED DIALING
     List1: group    1        List2:                 List3:
            SAC Notification? n
                          COMMON SHARED EXTENSIONS
            Starting Extension:                Count:
```

3. In the **Timed Reminder on Hold** field, type the maximum number of seconds that a call can remain on hold before the system alerts the attendant.

   In this example, we set the interval to 30 seconds.

4. In the **Return Call Timeout** field, type the maximum number of seconds that a call can remain on hold before the call returns to the attendant.

   In this example, we set the interval to 60 seconds.

Note:
You must allow at least 5 seconds for each ring at all points in a coverage path. This amount of time ensures that the entire calling path is completed before the system returns the call to the console.

5. Press **Enter** to save your changes.

Considerations for Attendant Call Waiting

This section provides information about how the Attendant Call Waiting feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Call Waiting under all conditions. The following considerations apply to Attendant Call Waiting:

- Attendant Call Waiting applies only to calls that are made to single-line telephones within the system.
- Only one call can wait at a time.

Interactions for Attendant Call Waiting

This section provides information about how the Attendant Call Waiting feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Call Waiting in any feature configuration.

- Automatic Callback

  Activating Automatic Callback at the called telephone denies Attendant Call Waiting.

- Call Coverage

  The system redirects Attendant Call Waiting calls to coverage if the called telephone has Data Privacy or Data Restriction activated. The system redirects the call to coverage if all three of the following conditions are met:

  – The Data Privacy or Data Restriction feature is activated
  – You assign call coverage to a telephone
  – The user activates Send All Calls, or coverage criteria is met
    - The Coverage Don’t Answer interval specifies how long that call remains directed to the called telephone before the system redirects the call to coverage. If Attendant Call Waiting is applicable on the call, the feature is active for the duration of the Don’t Answer interval only. At the end of this interval, the system redirects the call to coverage.

  - If the Return Call Timeout (Timed Reminder) interval expires before the Don't Answer interval expires, the call does not go to coverage, but returns to the attendant console. If the Don't Answer interval expires first, the system redirects the call to coverage. The system can still return the call to the attendant console if a coverage point does not answer the call before the Return Call Timeout expires.
  - If the **Station Hunting** field is assigned, and the called telephone is busy, the system redirects the call to the **Hunt To Station Assignment** value.
  - If Send All Calls is active, or if the redirection criterion is Cover All Calls, the system immediately redirects the call to coverage instead of to Attendant Call Waiting.
  - An attendant can release an extended call at any point during the call with no affect on the preceding operations.

- Data Privacy and Data Restriction

  Activating Data Privacy or Data Restriction at the called telephone denies Attendant Call Waiting.

- Direct Department Calling (DDC) and Uniform Call Distribution (UCD)

  Calls to a DDC group or to a UCD group do not wait. However, calls can enter the group queue, if a queue is provided.

- Loudspeaker Paging

  Activating Loudspeaker Paging at the called telephone denies Attendant Call Waiting.

- Music-on-Hold Access

  If the call is a trunk-transferred call that is administered to receive Music-on-Hold, the calling party hears music. Otherwise, the calling party hears ringing.

- Recorded Telephone Dictation Access

  Activating Recorded Telephone Dictation Access at the called telephone denies Attendant Call Waiting.

Attendant Calling of Inward Restricted Stations

Use the Attendant Calling of Inward Restricted Stations feature to allow an attendant to override an inward restriction Class of Restriction (COR).

Detailed description of Attendant Calling of Inward Restricted Stations

This section provides a detailed description of the Attendant Calling of Inward Restricted Stations feature.

A telephone that is restricted from receiving inbound calls cannot receive public network, attendant-originated, or attendant-extended calls. The Attendant Calling of Inward Restricted Stations feature allows the attendant to override this restriction.

Administering Attendant Calling of Inward Restricted Stations

The following steps are part of the administration process for the Attendant Calling of Inward Restricted Stations feature:

- Setting up Class of Restriction override

This section describes:

- Any prerequisites for administering the Attendant Calling of Inward Restricted Stations feature
- The screens that you use to administer the Attendant Calling of Inward Restricted Stations feature
- Complete administration procedures for the Attendant Calling of Inward Restricted Stations feature

Prerequisites for administering Attendant Calling of Inward Restricted Stations

You must complete the following actions before you can administer the Attendant Calling of Inward Restricted Stations feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Calling of Inward Restricted Stations

Screen name	Purpose	Fields
Class of Restriction	Allow an attendant to override any Class of Restriction that is assigned to a telephone.	**Restriction Override**

Setting up Class of Restriction override

To set up Class of Restriction override:

1. In the Class of Restriction screen, set the **Restriction Override** field to **attendant**.

   For more information, see the "Class of Restriction" feature.

Attendant Conference

Use the Attendant Conference feature to allow an attendant to set up a conference call for as many as six conferees, including the attendant. The attendant can add parties to the conference call from both inside and outside the system.

Detailed description of Attendant Conference

This section provides a detailed description of the Attendant Conference feature.

The Attendant Conference feature allows an attendant to set up a conference call for as many as six conferees, including the attendant.The conference call is held at the attendant console.

To set up a conference, the attendant dials the number of a conferee, and then presses the Split button to add the party.

Administering Attendant Conference

The following steps are part of the administration process for the Attendant Conference feature:

- Setting up Attendant Conference

This section describes:

- Any prerequisites for administering the Attendant Conference feature
- The screens that you use to administer the Attendant Conference feature
- Complete administration procedures for the Attendant Conference feature

Prerequisites for administering Attendant Conference

You must complete the following actions before you can administer the Attendant Conference feature:

- The system activates the Attendant Conference feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Conference

Screen name	Purpose	Fields
Feature-Related System-Parameters	Set up the Attendant Conference feature.	• **Public Network Trunks on Conference Call** • **Conference Parties with Public Network Trunks** • **Conference Parties without Public Network Trunks**

Setting up Attendant Conference

To set up Attendant Conference:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System-Parameters screen.

2. Click **Next** until you see the **Public Network Trunks on Conference Call** field (Figure 44: Feature-Related System-Parameters screen on page 241).

Figure 44: Feature-Related System-Parameters screen

```
change system-parameters features                                Page 6 of 14

                          FEATURE-RELATED SYSTEM PARAMETERS

         Public Network Trunks on Conference Call: 5             Auto Start? n
   Conference Parties with Public Network Trunks: 6              Auto Hold? n
 Conference Parties without Public Network Trunks: 6          Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180         Bridging Tone? n
                  Short Interdigit Timer (seconds): 3          nference Tone? n
              Unanswered DID Call Timer (seconds):            Intrusion Tone? n
              Line Intercept Tone Timer (seconds): 30      Special Dial Tone? n
                 Long Hold Recall Timer (seconds): 0    Mode Code Interface? y
                      Reset Shift Timer (seconds): 0
    Station Call Transfer Recall Timer (seconds): 0
                               DID Busy Treatment: tone
       Invalid Number Dialed Intercept Treatment: tone
              Allow AAR/ARS Access from DID/DIOD? y
                Allow ANI Restriction on AAR/ARS? n
     Use Trunk COR for Outgoing Trunk Disconnect? n
                  7405ND Numeric Terminal Display? y                 7434ND? n
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                           Attendant originated Calls: external
   DTMF Tone Feedback Signal to VRU - Connection:            Disconnection:
```

3. In the **Public Network Trunks on Conference Call** field, type a number between 0 and 5. This number indicates the maximum number of public network trunks that are allowed on an attendant conference call.

   In this example, we set the number to 5. If you set this field to 0, the **Conference Parties with Public Network Trunks** field does not appear.

4. In the **Conference Parties with Public Network Trunks** field, type a number between 3 and 6. This number indicates the maximum number of parties that are allowed on a conference call that involves a public network subscriber.

   In this example, we set the number to 6.

5. In the **Conference Parties without Public Network Trunks** field, type a number between 3 and 6. This number indicates the maximum number of parties that are allowed on a conference call that involves no public network trunks.

   In this example, we set the number to 6.

6. Press **Enter** to save your changes.

Considerations for Attendant Conference

This section provides information about how the Attendant Conference feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Conference under all conditions. The following considerations apply to Attendant Conference:

- Use this feature whenever an attendant must talk with more than one party at the same time, or establish a conference call for parties who are outside the system.
- The attendant can set up only one conference call at a time. The attendant can hold a conference call on the console, or release the conference call.
- The attendant cannot handle other calls while the attendant sets up a conference call.
- No matter who establishes the call, once the attendant is one of the conferees, only the attendant can add another party to the call.

Interactions for Attendant Conference

This section provides information about how the Attendant Conference feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Conference in any feature configuration.

- Bridged Call Appearance

  A user can press the Bridged Appearance button on the telephone and join a conference call only if no more than five parties are on the call.

- Call Vectoring

  A vector directory number (VDN) can be included as a party in a conference call only after vector processing terminates for that call. Vector processing terminates, for example, after a successful route-to command.

- Trunk-to-Trunk Transfer

  If Trunk-to-Trunk Transfer is disabled on the Feature-Related System-Parameters screen, and the attendant releases from a conference call that involves only trunk conferees, the system disconnects the trunks.

  When a user of a BRI, digital, or hybrid multifunction telephone dials enough digits to route a call that might otherwise be routed differently if the user dials additional digits, the telephone does not recognize the Conference or the Transfer buttons. For the telephone to recognize the Conference or the Transfer buttons, the user must either delay dialing for 3-seconds, or dial the pound key (**#**) at the end of the dialed string. This action tells the system to route the call based on the digits that were already dialed, and not wait for additional digits. The system then completes the call.

  Attendant conferencing might not operate properly if the central office (CO) does not provide answer supervision. In this case, the **Answer Supervision Timeout** and **Outgoing End of Dial** fields are set to the same nonzero number, and the **Receive Answer Supervision** field is set to **n**.

  If the CO provides answer supervision, you can set the **Answer Supervision Timeout** field to **0**, and the **Receive Answer Supervision** field to **y**.

Attendant Control of Trunk Group Access

Use the Attendant Control of Trunk Group Access feature to allow the attendant to control outgoing and two-way trunk groups. The attendant usually activates this feature during periods of high use. This is helpful when an attendant wants to prevent telephone users from calling out on a specific trunk group. Some reasons are to reserve a trunk group for incoming calls or for a very important outgoing call.

This feature also prevents telephone users from directly accessing an outgoing trunk group that the attendant has controlled.

Detailed description of Attendant Control of Trunk Group Access

This section provides a detailed description of the Attendant Control of Trunk Group Access feature.

When an administered threshold for a trunk group is reached, a warning lamp for that trunk group lights on the attendant console. The attendant can then access control of that trunk group. To gain direct access to an outgoing trunk group, the attendant presses the button that is assigned to that trunk group.

When the Attendant Control of Trunk Group Access feature is activated:

- Internal callers who use a trunk access code to dial out are connected to the attendant
- The attendant can prioritize outgoing calls for the remaining trunks

The system processes Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) route pattern calls without the need for attendant control.

Each attendant console has 12 designated Trunk Hundreds Select buttons. These buttons can be administered for the Attendant Control of Trunk Group Access feature. You can also administer each console with up to 12 feature buttons for Trunk Hundreds Select buttons, which gives you up to 24 buttons to use for this feature.

Each Trunk Hundreds Select button has a busy lamp. The busy lamp lights when the telephones of all members of the trunk group are busy.

Note:
If you administer one of the two-lamp feature buttons on a basic console as a Trunk Hundreds Select button, use the bottom lamp as the busy lamp.

The Trunk Hundreds Select buttons have the following two additional lamps for Attendant Control of Trunk Group Access:

- Warn (warning) lamp

  The warning lamp lights when the administered number of trunks are busy in the associated trunk group. You administer the **Busy Threshold** field on the associated Trunk Group screen to determine when to light this warning lamp.

- Cont (control) lamp

  The control lamp lights when the attendant activates the Attendant Control of Trunk Group Access feature for the associated trunk group. You assign the **act-tr-grp** and **deact-tr-g** buttons on the Attendant Console screen to allow the attendant to activate and deactivate the trunk group access.

Administering Attendant Control of Trunk Group Access

The following steps are part of the administration process for the Attendant Control of Trunk Group Access feature:

- Setting the trunk group threshold
- Assigning Attendant Control of Trunk Group Access buttons

This section describes:

- Any prerequisites for administering the Attendant Control of Trunk Group Access feature
- The screens that you use to administer the Attendant Control of Trunk Group Access feature
- Complete administration procedures for the Attendant Control of Trunk Group Access feature

Prerequisites for administering Attendant Control of Trunk Group Access

You must complete the following actions before you can administer the Attendant Control of Trunk Group Access feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Control of Trunk Group Access

Screen name	Purpose	Fields
Trunk Group	Determine the threshold for when to light the warning lamp.	**Busy Threshold**
Attendant Console	Assign buttons to allow the attendant to activate and deactivate trunk group access.	Any unassigned buttons in the **Feature Button Assignments** area.

Setting the trunk group threshold

To set the trunk group threshold:

1. Type **change trunk-group *n***, where ***n*** is the number of the trunk group. Press **Enter**.

   The system displays the Trunk Group screen.

2. In the **Busy Threshold** field, type the number of trunks that must be busy to light the warning lamp on the attendant console. The range is from 1 to 255.

   For example, a trunk group contains 30 trunks. If you want to alert the attendant when 25 or more trunks are in use, type **25**.

3. Press **Enter** to save your changes.

Assigning Attendant Control of Trunk Group Access buttons

To assign Attendant Control of Trunk Group Access buttons:

1. Type **change attendant *n***, where ***n*** is the number of the attendant console. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 45: Attendant Console screen on page 248).

Figure 45: Attendant Console screen

```
change attendant 1                                          Page 3 of 4
                                ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split_____                          13: __________
  2: __________                          14: __________
  3: act-tr-grp                          15: __________
  4: deact-tr-g                          16: __________
  5: __________                          17: __________
  6: hold _____ *                        18: __________
  7: __________                          19: forced-rel
  8: aux-work      RC:    Grp:           20: __________
  9: __________                          21: __________
 10: __________                          22: __________
 11: __________                          23: night-serv *
 12: __________                          24: pos-busy__ *
```

3. In the **Feature Button Assignments** area, assign **act-tr-grp** and **deact-tr-g** to two available buttons.

   In this example, we assign **act-tr-grp** to button **3**, and **deact-tr-g** to button **4**.

4. Press **Enter** to save your changes.

Interactions for Attendant Control of Trunk Group Access

This section provides information about how the Attendant Control of Trunk Group Access feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Control of Trunk Group Access in any feature configuration.

- Authorization Codes

  Authorization codes do not collect when a trunk group has an incoming destination set to the attendant.

- Automatic Route Selection (ARS) and Automatic Alternate Routing (AAR)

  Activating Attendant Control of Trunk Group Access removes the controlled trunk groups from the ARS and the AAR patterns. Deactivating the feature reinserts the groups into the patterns. The system does not route ARS calls to the attendant.

- QSIG

  QSIG trunks do not support Attendant Control of Trunk Group Access.

- Uniform Dial Plan (UDP)

  Activating Attendant Control of Trunk Group Access removes the controlled trunk groups from preferences. Deactivating the feature allows the UDP to access the trunk groups.

Attendant Direct Extension Selection

Use the Attendant Direct Extension Selection (DXS) feature to allow an attendant to track the idle or busy status of an extension. This feature also allows an attendant to place or extend calls to extensions without the need to dial the extension.

The Attendant DXS feature is sometimes referred to as the Attendant Direct Extension Selection with Busy Lamp Field feature.

Detailed description of Attendant Direct Extension Selection

This section provides a detailed description of the Attendant Direct Extension Selection (DXS) feature.

With Attendant DXS, you can use either Standard or Enhanced DXS Tracking:

- Standard DXS Tracking

  If your attendant console has one or more Hundreds Select buttons, the attendant can press both a Hundreds Select button and a DXS button to access an extension.

- Enhanced DXS Tracking

  Use Enhanced DXS Tracking if your attendant console:

  — Does not use Hundreds Select buttons

  — Uses Hundreds Select buttons, but you have one or more hundreds groups that are not administered by a Hundreds Select button

  To access an extension, the attendant can:

  — Press a Group Select button

  — Dial the first 2 or 3 digits of the extension

  — Press the DXS button to access an extension

When the system tracks a group of extensions, the attendant can press the DXS button to place or extend subsequent calls to extensions in that group without the need to reselect the group. Whether the attendant uses a Hundreds Select button or the Group Select button, both capabilities eliminate the need to dial extensions.

Extensions might be telephones, hunt-group extensions, off-switch extensions such as uniform dial plan (UDP) extensions, or other extensions.

Whichever method you use to access and track DXS extensions, you can use a Group Display feature button to view the group of extensions that are currently being tracked. This button on the console indicates the range of extensions that the selector console is tracking.

Note:
An associated DXS lamp for a vector directory number (VDN) is always dark. The attendant can use the DXS button to place a call to a VDN.

Attendant DXS supports the following capabilities:

- Standard DXS Tracking
- Enhanced DXS Tracking

Standard DXS Tracking

The basic selector console has 8 Hundreds Select buttons, and 100 DXS buttons. The enhanced selector console has 20 Hundreds Select buttons, and 100 DXS buttons. You can assign 12 additional Hundreds Select buttons to feature buttons on the attendant console.

The total number of Hundreds Select buttons for each attendant, including both attendant console feature buttons and selector console buttons, cannot exceed 20.

Enhanced DXS Tracking

Enhanced DXS Tracking is helpful if you have more than 100 telephones, but use a console that does not have Hundreds Select buttons administered. Enhanced DXS Tracking is also helpful if you have more telephones than Hundreds Select buttons, and thus have hundreds groups that are administered with Hundreds Select buttons.

To use Enhanced DXS, assign a Group Select button on the Attendant Console screen. The attendant uses this button to track and extend calls to telephones that do not have associated Hundreds Select buttons. You can not use Enhanced DXS Tracking if your extensions have fewer than 3 digits.

Group Display button

You can administer a **Group Display** button on the Attendant Console screen to help the attendant track extension status. When the attendant presses this button, the system displays the range of extensions that are currently tracked by the selector console. Administer the **Group Display** button for either the feature area or the display area of the console.

If the attendant presses this button, the system identifies the digits that are associated with a **Hundreds Select** button. If no **Hundreds Select** button is lit, the system identifies the digits that were last entered with the **Group Select** button. The system continues to track the selected group of extensions until the attendant selects a new group of extensions.

Administering Attendant Direct Extension Selection

This section describes the prerequisites and the screens for the Attendant Direct Extension Selection (DXS) feature.

Prerequisites for administering Attendant Direct Extension Selection

You must complete the following actions before you can administer the Attendant Direct Extension Selection (DXS) feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Direct Extension Selection

Screen name	Purpose	Fields
Attendant Console	Assign a DXS button.	Any available button field in the **Hundreds Select Button Assignments** area

Considerations for Attendant Direct Extension Selection

This section provides information about how the Attendant Direct Extension Selection (DXS) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Direct Extension Selection (DXS) under all conditions. The following considerations apply to Attendant Direct Extension Selection (DXS):

- With this feature, the attendant can place calls to:

  - 800 extensions with the basic selector console
  - 2,000 extensions with the enhanced selector console
  - Up to 99,999 extensions with the Group Select feature button (extension numbers from 100 to 99,999)

  If the attendant is tracking a hundreds group with either a Hundreds Select button or the Group Select feature button, the attendant presses the DXS button to access an extension.
- This feature provides the attendant with a visual indication of the idle or busy status of the extensions that are assigned to the selected hundreds group. You can simultaneously monitor up to 100 extensions for idle or busy status.
- Enhanced DXS Tracking does not support extensions with fewer than 3 digits.
- Extension tracking is possible only for the system on which the attendant resides.

Interactions for Attendant Direct Extension Selection

This section provides information about how the Attendant Direct Extension Selection (DXS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Direct Extension Selection (DXS) in any feature configuration.

- Attendant Display

  When the attendant uses the Attendant Direct Extension Selection with Busy Lamp Field, the alphanumeric display identifies the call through the Attendant Display.
- Call Coverage

  If Send All Calls is activated, or if the Call Coverage redirection criteria are met, the system redirects an extended call to the coverage path.
- Centralized Attendant Service (CAS)

  When the attendant uses a DXS button to make a CAS call, the attendant hears ringback tone after a few seconds.

Attendant Direct Trunk Group Selection

Use the Attendant Direct Trunk Group Selection feature to allow the attendant direct access to an idle outgoing trunk. With this feature, the attendant gets directs access to an idle outgoing trunk when the attendant presses the button that is assigned to the trunk group. This feature eliminates the need for the attendant to memorize, or look up, and dial the trunk access codes (TACs) that are associated with frequently used trunk groups.

Detailed description of Attendant Direct Trunk Group Selection

This section provides a detailed description of the Attendant Direct Trunk Group Selection feature.

You can use up to 12 designated Trunk Hundreds Select buttons on each console. You can also administer up to 12 of the feature buttons as additional Trunk Hundreds Select buttons, for a total of 24 Trunk Hundreds Select buttons per console. Each button allows the attendant direct access to an outgoing select trunk group.

While an attendant talks on a call, the attendant can be split away that call and place a new call to the outgoing trunk that is specified by the trunk group select button. The attendant can then press Release to connect the split-away parties to the dial tone on the trunk. Or the attendant can dial the destination, and press Release to connect the split-away party to the called party.

All Trunk Hundreds Select buttons, including any that are administered on the feature buttons, have a Busy lamp. This lamp lights when all trunks in the associated trunk group are busy. If you administer one of the two-lamp feature buttons on a basic console as a Trunk Hundreds Select button, use the bottom lamp as the Busy lamp. Six of the designated buttons on a basic console, or all 12 designated buttons on an enhanced console also have a Warning lamp and a Control lamp. The Warning lamp lights when a preset number of trunks in the associated trunk group are busy. The Cont lamp lights when the attendant activates Attendant Control of Trunk Group Access for the associated trunk group.

You can assign Loudspeaker Paging zones instead of trunk groups to Trunk Hundreds Select buttons. The Busy lamp then indicates the idle or the busy status of the associated Loudspeaker Paging zone.

Administering Attendant Direct Trunk Group Selection

This section describes the prerequisites and the screens for the Attendant Direct Trunk Group Selection feature.

Prerequisites for administering Attendant Direct Trunk Group Selection

You must complete the following actions before you can administer the Attendant Direct Trunk Group Selection feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Direct Extension Selection

Screen name	Purpose	Fields
Attendant Console	Assign trunk access codes (TACs) for local and remote systems.	Any available button field in the **Direct Trunk Group Select Button Assignments** (Trunk Access Codes) area

Considerations for Attendant Direct Trunk Group Selection

This section provides information about how the Attendant Direct Trunk Group Selection feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Direct Trunk Group Selection under all conditions. The following considerations apply to Attendant Direct Trunk Group Selection:

- Attendant Direct Trunk Group Selection eliminates the need for the attendant to memorize, or look up, and dial a trunk access code (TAC) that is associated with frequently used trunk groups. A label that is associated with each Trunk Hundreds Select button identifies the destination or use of the button. For example, buttons might be labeled Chicago, FX, or WATS. The attendant presses the button to select an idle trunk in the desired group.

Interactions for Attendant Direct Trunk Group Selection

This section provides information about how the Attendant Direct Trunk Group Selection feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Direct Trunk Group Selection in any feature configuration.

- Attendant Control of Trunk Group Access

  If Attendant Control of Trunk Group Access is provided, the Attendant Direct Trunk Group Selection feature must also be provided.

- QSIG

  Attendant Direct Trunk Group Selection does not apply to QSIG trunks.

Attendant Intrusion

Use the Attendant Intrusion feature to allow an attendant to intrude on an existing call. The Attendant Intrusion feature is also called Call Offer.

Detailed description of Attendant Intrusion

This section provides a detailed description of the Attendant Intrusion feature.

The attendant uses the Attendant Intrusion feature to announce a new call or a message to a user who is already on a call.

When the attendant releases the call of the user, the source party either waits at the analog telephone of the user, or holds on an available line appearance on a digital telephone.

Note:

Only one call can be waiting at a time. If a call is already waiting on the telephone of the intruded party, the source party, once split from the attendant, cannot also wait.

Administering Attendant Intrusion

The following steps are part of the administration process for the Attendant Intrusion feature:

- Assigning an intrusion button

This section describes:

- Any prerequisites for administering the Attendant Intrusion feature
- The screens that you use to administer the Attendant Intrusion feature
- Complete administration procedures for the Attendant Intrusion feature

Prerequisites for administering Attendant Intrusion

You must complete the following actions before you can administer the Attendant Intrusion feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Intrusion

Screen name	Purpose	Fields
Attendant Console	Assign an **intrusion** button.	Any unassigned button in the **Feature Button Assignments** area.

Assigning an intrusion button

To assign an **intrusion** button:

1. Type **`change attendant n`**, where ***n*** is the number of the attendant console. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 46: Attendant Console screen on page 260).

Figure 46: Attendant Console screen

```
change attendant 1                                          Page 3 of 4
                              ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split_____                          13: __________
  2: dont-split                          14: __________
  3: act-tr-grp                          15: __________
  4: deact-tr-g                          16: __________
  5: intrusion                           17: __________
  6: hold _____ *                        18: __________
  7: __________                          19: forced-rel
  8: aux-work      RC:    Grp:           20: __________
  9: __________                          21: __________
 10: __________                          22: __________
 11: __________                          23: night-serv *
 12: __________                          24: pos-busy__ *
```

3. In the **Feature Button Assignments** area, assign **intrusion** to an available button.

   In this example, we assign **intrusion** to button 5.

4. Press **Enter** to save your changes.

Reports for Attendant Intrusion

The following reports provide information about the Attendant Intrusion feature:

- None

Considerations for Attendant Intrusion

This section provides information about how the Attendant Intrusion feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Intrusion under all conditions. The following considerations apply to Attendant Intrusion:

- None

Interactions for Attendant Intrusion

This section provides information about how the Attendant Intrusion feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Intrusion in any feature configuration.

- Intrusion is denied in when a:
  - Telephone is on a conference call with the administered maximum number of conferees
  - Call is established with Data Privacy activated
  - Call is established with Data Restriction activated
  - Telephone is a forward-to point of another telephone
  - Telephone is busy talking to another attendant
- If a call is already waiting for an intruded party, the second caller, who is split from the attendant, cannot use Call Waiting to wait for the intruded party. The attendant display shows "wait" or "busy". If an intrusion is possible, the attendant display shows "1 wait" or "1 busy".

- In Italy only, the system provides Attendant Intrusion on remote telephones through TGU/ TGE trunks.

Attendant Lockout - Privacy

Use the Attendant Lockout - Privacy feature to prevent an attendant, who drops from a multiparty conference call, from reentering the call. The attendant can be recalled only by a telephone user who is on the multiparty call.

You administer this feature on a system-wide basis. The Attendant Lockout - Privacy feature is either activated or deactivated.

Detailed description of Attendant Lockout - Privacy

This section provides a detailed description of the Attendant Lockout - Privacy feature.

The Attendant Lockout - Privacy feature provides privacy for parties on a multiparty call. The parties can hold a private conversation without interruption by the attendant. The multiparty call must be held on the attendant console.

Administering Attendant Lockout - Privacy

The following steps are part of the administration process for the Attendant Lockout - Privacy feature:

- Activating or deactivating the Attendant Lockout - Privacy feature

This section describes:

- Any prerequisites for administering the Attendant Lockout - Privacy feature
- The screens that you use to administer the Attendant Lockout - Privacy feature
- Complete administration procedures for the Attendant Lockout - Privacy feature

Prerequisites for administering Attendant Lockout - Privacy

You must complete the following actions before you can administer the Attendant Lockout - Privacy feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Lockout - Privacy

Screen name	Purpose	Fields
Console Parameters	Activate or deactivate the Attendant Lockout - Privacy feature.	**Attendant Lockout**

Activating or deactivating the Attendant Lockout - Privacy feature

To activate or deactivate the Attendant Lockout - Privacy feature:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 47: Console Parameters screen on page 264).

Figure 47: Console Parameters screen

```
change console-parameters                                    Page   1 of 3
                              CONSOLE PARAMETERS
         Attendant Group Name: 27 character name  OPERATOR
                         COS: 0                                  COR: 0
       Calls in Queue Warning: 5                    Attendant Lockout? y
        Ext Alert Port (TAAS):
                         CAS: none
              SAC Notification? n              Night Service Act. Ext.:
                  IAS (Branch)? n              IAS Tie Trunk Group No.:
          IAS Att. Access Code:                  Alternate FRL Station:
               Backup Alerting? n        DID-LDN Only to LDN Night Ext? n
TIMING
  Time Reminder on Hold (sec): 10           Return Call Timeout (sec): 10
  Time in Queue Warning (sec):
  INCOMING CALL REMINDERS
      No Answer Timeout (sec): 20                      Alerting (sec): 40
                               Secondary Alert on Held Reminder Calls? y
ABBREVIATED DIALING
     List1: group    1        List2:                  List3:

                           COMMON SHARED EXTENSIONS
            Starting Extension:                 Count:
```

2. In the **Attendant Lockout** field, perform one of the following actions:
   - Type **y** to activate this feature.
   - Type **n** to deactivate this feature.

3. Press **Enter** to save your changes.

For more information, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Interactions for Attendant Lockout - Privacy

This section provides information about how the Attendant Lockout - Privacy feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Lockout - Privacy in any feature configuration.

- Attendant Recall

  If Attendant Lockout - Privacy is activated, use Attendant Recall if you must recall the attendant.

- Individual Attendant Access

  Attendant Lockout - Privacy applies only to attendant group calls. This feature does not affect individual attendant calls.

- Trunk-to-Trunk Transfer

  Attendant Lockout - Privacy does not function when a call that uses Trunk-to-Trunk Transfer is held on the console.

Attendant Override of Diversion Features

Use the Attendant Override of Diversion Features feature to allow the attendant to bypass a call-diverting feature that a user activates. Such features include Send All Calls, Call Coverage, and Call Forwarding. An attendant can use this feature, in combination with Attendant Intrusion, to place an emergency call or an urgent call to a user.

Detailed description of Attendant Override of Diversion Features

This section provides a detailed description of the Attendant Override of Diversion Features feature.

With the Attendant Override of Diversion Features, the attendant can bypass a call-diverting feature that a user activates. Such features include Send All Calls, Call Coverage, and Call Forwarding.

Administering Attendant Override of Diversion Features

This section contains prerequisites and the screens for administering the Attendant Override of Diversion Features feature.

Prerequisites for administering Attendant Override of Diversion Features

You must complete the following actions before you can administer the Attendant Override of Diversion Features feature:

- Set up an attendant console. For information on how to set up an attendant console, see the *Administering Avaya Aura™ Communication Manager*.

Screens for administering Attendant Override of Diversion Features

Screen name	Purpose	Fields
Attendant Console	Administer the Attendant Override button.	Any available button field in the **Feature Button Assignments** area

Attendant Priority Queue

Use the Attendant Priority Queue feature to place incoming calls to an attendant, that cannot be immediately answered, into an ordered queue. With this feature, you can define 13 different categories of incoming attendant calls. Emergency calls always have the highest priority.

Detailed description of Attendant Priority Queue

This section provides a detailed description of the Attendant Priority Queue feature.

When an attendant cannot immediately answer calls, the system can place incoming calls into categories, or into a call type within a category.

With Attendant Priority Queue, attendants can answer calls by call category, such as trunk type. Attendant Priority Queue places incoming calls in a queue:

- According to the priority levels that you assign for each type of call
- In order of time stamp within each level

The calling party hears ringback until an attendant answers the call.

Attendant Priority Queue supports the following capabilities:

- Priority by Call Category
- Priority by Call Type

Priority by Call Category

Assign an Attendant Priority Queue level to each of 13 incoming attendant call categories. Each category has a default level. You can reset the priority level for any category.

Important:
Do not change the priority level for Emergency Access calls. Emergency Access calls must remain priority 1.

The attendant call categories are:

- Emergency Access. Calls from users who dial the emergency access code. The default is the highest priority level. This category must remain priority 1.
- Assistance Call. Calls from users who:

  - Dial the attendant group access code
  - Have the Manual Originating Line Service feature activated
- CO Call. Incoming central office (CO), foreign exchange (FX), or Wide Area Telecommunications Service (WATS) trunk calls to an attendant group. This category does not include trunk calls that are returned to the attendant group after a timeout or a deferred attendant recall.
- DID to Attendant. Incoming direct inward dial (DID) trunk calls to an attendant group.
- Tie Call. Incoming Tie trunk calls, including dial-repeating and direct types.
- Redirected DID Call. DID or Automatic Call Distribution (ACD) calls that time out, and are rerouted to the attendant group. The timeout can be caused by:
  - Ring/no-answer
  - Busy condition
  - Number Unobtainable
- Redirected Call. Calls that are assigned to one attendant, but redirected to the attendant group because the attendant is now busy.
- Return Call. Calls that are returned to the attendant after the calls time out. If the attendant is now busy, calls are redirected to the attendant group.
- Serial Call. Calls from the Attendant Serial Call feature. Calls fit this category when an outside trunk call, that the attendant designates as a serial call, is extended to and completed at a telephone, and then the user goes on-hook. If the attendant who extends the call is busy, the system redirects the call to the attendant group.
- Individual Attendant Access. Calls from users, incoming trunks, or a system feature, to the Individual Attendant Access (IAA) extension of a specific attendant. If the attendant is busy, the call remains in a queue until the attendant is available.
- Interpositional. Calls from one attendant to the Individual Attendant Access (IAA) extension of another attendant.
- VIP Wakeup Reminder Call. Call from the Hospitality feature that send a wake-up reminder to the attendant to call the room.
- Miscellaneous Calls. All other calls.

You can assign the same priority level to more than one category. Assigning all categories the same priority level creates a first-in first-out queue.

When at least one call appears in the Attendant Priority Queue, the Calls Waiting lamp lights steadily on all active attendant consoles. If the number of calls in the queue reaches the calls-waiting threshold for the attendant group, the Queue Warning lamp lights steadily on all active attendant consoles.

Priority by Call Type

You can further define the priority that you assign to calls in the Attendant Priority Queue by call type. Then, within each call type, you can prioritize calls by time.

The call types, in descending order of priority, are:

- Type 1 calls are outgoing public network calls that receive answer supervision when the Answer Supervision Timer of the trunk group expires, even if the trunk is still ringing. Type 1 calls are also incoming calls that the attendant answers.
- Type 2 calls are incoming external public network calls before the calls receive answer supervision, or before the Answer Supervision Timer of the trunk group expires.
- Type 3 calls are all other calls, which include internal calls, conference calls, and tie-trunk calls of any type.

Note:
External public network calls have priority over all other calls, including conference calls. Answered public network calls have priority over calls that are not yet answered.

Administering Attendant Priority Queue

The following steps are part of the administration process for the Attendant Priority Queue feature:

- Setting category priorities
- Setting the number of calls in the queue
- Assigning a Call Type button
- Translating the Call Type button into a user-defined language

This section describes:

- Any prerequisites for administering the Attendant Priority Queue feature
- The screens that you use to administer the Attendant Priority Queue feature
- Complete administration procedures for the Attendant Priority Queue feature

Prerequisites for administering Attendant Priority Queue

You must complete the following actions before you can administer the Attendant Priority Queue feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Priority Queue

Screen name	Purpose	Fields
Console Parameters	Assign priorities to queue categories.	All fields in the **Queue Priorities** area
Feature-Related System Parameters	Set the number of calls in the queue.	**Reserved Slots for Attendant Priority Queue**
Attendant Console	Assign a Call Type button.	Any unassigned button in the **Feature Button Assignments** area
Language Translations	Translate the Call Type button into a user-defined language.	**Call Type**

Setting category priorities

To set the category priorities:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen.

2. Click **Next** until you see the **Queue Priorities** area (Figure 48: Console Parameters screen on page 273).

Figure 48: Console Parameters screen

```
change console-parameters                                    Page 3 of 4

                                CONSOLE PARAMETERS
 QUEUE PRIORITIES
                 Emergency Access:1_
                  Assistance Call:2_
                          CO Call:3_
                 DID to Attendant:4_
                           Tie Call:5_
               Redirected DID Call:6_
                   Redirected Call:7_
                       Return Call:8_
                       Serial Call:9_
     Individual Attendant Access:10
                  Interpositional:11
        VIP Wakeup Reminder Call:12
              Miscellaneous Call:13

               Call-Type Ordering Within Priority Levels? y
```

3. Type a number from 1 to 13 next to each category.

   This number indicates the priority of the category. The number 1 indicates the highest priority. The number 13 indicates the lowest priority.

4. In the **Call-Type Ordering Within Priority Levels** field, perform one of the following actions:

   — If you want to order calls by call type within each category, type **y**.

   — If you do not want to order calls by call type within each category, type **n**.

5. Press **Enter** to save your changes.

Setting the number of calls in the queue

To set the number of calls in the queue:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen

2. Click **Next** until you see the **Reserved Slots for Attendant Priority Queue** field (Figure 49: Feature-Related System Parameters screen on page 274).

Figure 49: Feature-Related System Parameters screen

```
change system-parameters features                              Page 4 of 14

                      FEATURE-RELATED SYSTEM PARAMETERS

                       Reserved Slots for Attendant Priority Queue: 5_
                                        Time Before Off-Hook Alert: 10__
                            Emergency Access Redirection Extension: _____
              Number of Emergency Calls Allowed in Attendant Queue: 5_
                                          Call Pickup Alerting? n
                       Temporary Bridged Appearance on Call Pickup? y
                                    Call Pickup on Intercom Calls? y
                                            Directed Call Pickup? n
                                       Extended Group Call Pickup? n
                  Deluxe Paging and Call Park Timeout to Originator? n
     Controlled Outward Restriction Intercept Treatment: tone _______
    Controlled Termination Restriction (Do Not Disturb): tone _______
              Controlled Station to Station Restriction: tone _______

AUTHORIZATION CODE PARAMETERS           Authorization Code Enabled? y
                                         Authorization Code Length: 7
                               Authorization Code Cancellation Symbol? #
                                            Attendant Time Out Flag? n
                                       Display Authorization Code? y

                    Controlled Toll Restriction Replaces: none
```

3. In the **Reserved Slots for Attendant Priority Queue** field, type a number between 2 and 75. This number indicates how many nonemergency calls can go into the priority queue. The default is 5.
4. In the **Number of Emergency Calls Allowed in Attendant Queue** field, type a number between 0 and 75. This number indicates how many emergency calls can go into the priority queue. The default is 5.
5. Press **Enter** to save your changes.

Assigning a Call Type button

You can assign a **Call Type** button on the attendant console. When you press this button, the system displays the call type of the active call. For more information on how to set up an attendant console, see the *Administering Avaya Aura™ Communication Manager*.

Translating the Call Type button into a user-defined language

If you use a user-defined language to display messages on the attendant console, you can translate the **Call Type** button.

To translate the **Call Type** button into a user-defined language:

1. Type **`change display-messages miscellaneous-features`**. Press **Enter**.

   The system displays the Language Translations screen.

2. Click **Next** until you see the **English: Call Type** field (Figure 50: Language Translations screen on page 275).

Figure 50: Language Translations screen

```
change display-messages miscellaneous-features                  Page 5 of 6

                            LANGUAGE TRANSLATIONS

  42.     English: Add Skill: Enter number, then # sign
      Translation: ************************************

  43.     English: Remove Skill: Enter number, then # sign
      Translation: ************************************

  44.     English: Enter Skill Level, then # sign
      Translation: ************************************

  45.     English: Enter Agent LoginID
      Translation: ************************************

  46.     English: Call Type
      Translation: ***************

  47.     English: Call Charge
      Translation: ********************
```

3. In the **English: Call Type** field, translate the button label into the user-defined language.
4. Press **Enter** to save your changes.

Considerations for Attendant Priority Queue

This section provides information about how the Attendant Priority Queue feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Priority Queue under all conditions. The following considerations apply to Attendant Priority Queue:

- An incoming call that defaults to an attendant and is then redirected to the attendant group, does not change the associated Attendant Priority Queue level. The reason code that the system displays on the answering attendant console remains the same as the reason code that the system displays on the original attendant console.

Interactions for Attendant Priority Queue

This section provides information about how the Attendant Priority Queue feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Priority Queue in any feature configuration.

- Multiparty Calls

  The system always treats multiparty calls as Type 3 calls. If a multiparty call becomes a single-party call while in the queue, the multiparty call remains a Type 3 call.

- Night Service-Hunt Group

  When you use Night Service-Hunt Groups, retrieve calls from the hunt groups instead of from the Attendant Priority Queue. Since call-type prioritization does not apply to hunt groups, do not retrieve calls in order of call type, unless you designate the Attendant Priority Queue as the termination.

- Off-Premises Station

  The system always identifies calls from off-premises telephones as Type 3 calls.

Attendant Recall

Use the Attendant Recall feature to allow a user to recall the attendant while the user is on a call.

- Single-line users press the recall button or flash the switchhook to recall the attendant.
- Multi-appearance users press the conference or transfer button to recall the attendant and remain on the connection when either button is used.

Detailed description of Attendant Recall

This section provides a detailed description of the Attendant Recall feature.

With the Attendant Recall feature, users can call the attendant for assistance while the users are currently on a call. Users can activate the Attendant Recall feature only when the users are on a:

- Two-party call
- Conference call that is held at the attendant console

Administering Attendant Recall

The following steps are part of the administration process for the Attendant Recall feature:

- The system activates the Attendant Recall feature when you set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

This section describes:

- Any prerequisites for administering the Attendant Recall feature
- The screens that you use to administer the Attendant Recall feature
- Complete administration procedures for the Attendant Recall feature

Prerequisites for administering Attendant Recall

You must complete the following actions before you can administer the Attendant Recall feature:

- None

Screens for administering Attendant Recall

Screen name	Purpose	Fields
Attendant Console	Set up an attendant console.	All

End-user procedures for Attendant Recall

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Attendant Recall:

To recall the attendant:

- Single-line users press the recall button or flash the switchhook.
- Multiappearance users press the conference button or the transfer button.

Considerations for Attendant Recall

This section provides information about how the Attendant Recall feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Recall under all conditions. The following considerations apply to Attendant Recall:

- None

Interactions for Attendant Recall

This section provides information about how the Attendant Recall feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Recall in any feature configuration.

- Individual Attendant Access

  If a user is holding a hunt-group call to an individual attendant, the user who is active on the call cannot recall the attendant. However, the user can transfer calls, and make conference calls.

Attendant Serial Calling

Use the Attendant Serial Calling feature to allow the attendant to transfer trunk calls that the system routes to the attendant when the called user hangs up. The attendant can then transfer the call to another user who is on the same server.

Detailed description of Attendant Serial Calling

This section provides a detailed description of the Attendant Serial Calling feature.

You can administer the system to route calls to the attendant when the called user hangs up, but the caller does not. The attendant can then use Attendant Serial Calling to transfer the call to another user, at the request of the caller. The attendant can transfer calls only to those users on the same server.

This feature helps the attendant to use the trunks efficiently. If few trunks are available, and direct inward dialing (DID) is unavailable, a caller might make several attempts to complete a call before the caller is successful. When a caller makes a successful call to the attendant, the user can use the same line into the server for multiple telephone calls.

The attendant display shows the attendant that an incoming call is a serial call.

Administering Attendant Serial Calling

This section contains prerequisites and the screens for administering the Attendant Serial Calling feature.

Prerequisites for administering Attendant Serial Calling

You must complete the following actions before you can administer the Attendant Serial Calling feature:

- Set up an attendant console. For information on how to set up an attendant console, see the *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Serial Calling

Screen name	Purpose	Fields
Attendant Console	Administer the serial-cal button.	Any available button field in the **Feature Button Assignments** area

Attendant Split Swap

Use the Attendant Split Swap feature to allow an attendant to alternate between an active call and a split call. This feature is useful when the attendant must transfer a call, but first must talk independently with each party before completing the transfer.

Detailed description of Attendant Split Swap

This section provides a detailed description of the Attendant Split Swap feature.

With the Attendant Split Swap feature, an attendant can alternate between an active call and a split call. To activate this feature, the attendant presses a button on the attendant console.

Administering Attendant Split Swap

The following steps are part of the administration process for the Attendant Split Swap feature:

- Assigning a split-swap button

This section describes:

- Any prerequisites for administering the Attendant Split Swap feature
- The screens that you use to administer the Attendant Split Swap feature
- Complete administration procedures for the Attendant Split Swap feature

Prerequisites for administering Attendant Split Swap

You must complete the following actions before you can administer the Attendant Split Swap feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Split Swap

Screen name	Purpose	Fields
Attendant Console	Assign a split-swap button.	Any unassigned button in the **Feature Button Assignments** area.

Assigning a split-swap button

To assign a **split-swap** button:

1. Type **`change attendant n`**, where ***n*** is the number of the attendant console. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 51: Attendant Console screen on page 284).

Figure 51: Attendant Console screen

```
change attendant 1                                          Page 3 of 4
                              ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split_____                          13: split-swap
  2: dont-split                          14: __________
  3: act-tr-grp                          15: __________
  4: deact-tr-g                          16: __________
  5: __________                          17: __________
  6: hold _____ *                        18: __________
  7: __________                          19: forced-rel
  8: aux-work      RC:    Grp:           20: __________
  9: __________                          21: __________
 10: __________                          22: __________
 11: __________                          23: night-serv *
 12: __________                          24: pos-busy__ *
```

3. In the **Feature Button Assignments** area, assign **split-swap** to an available button.

   In this example, we assign **split-swap** to button 13.

4. Press **Enter** to save your changes.

Attendant Timers

Use the Attendant Timers feature to automatically alert the attendant after an administered time interval that calls remain waiting or on hold. The attendant can then reconnect with the caller, and decide whether to terminate the call, or allow the caller to continue waiting.

Detailed description of Attendant Timers

This section provides a detailed description of the Attendant Timers feature.

Attendant Timers automatically alert the attendant after an administered time interval for the following types of calls:

- Extended calls that are waiting to be answered or waiting to be connected to a busy single-line telephone
- One-party calls that are on hold at the console
- Transferred calls that are unanswered after a transfer

The Attendant Timers feature informs the attendant that a call requires additional attention. After the attendant reconnects to the call, the user can either choose to try another extension number, hang up, or continue to wait.

Communication Manager supports a variety of administrable attendant timers. Attendant timers include:

- Unanswered DID Call Timer. Specifies how long a direct inward dialing (DID) call can go unanswered before the system routes the call to the administered DID, TIE, or ISDN intercept treatment.
- Attendant Return Call Timer. Unanswered calls that the attendant extends return to the same attendant, if the attendant is available. If the same attendant is unavailable, unanswered calls return to the attendant group queue.

  The Attendant Return Call Timer is not set for calls that are extended from one attendant to another attendant. The system redirects a transferred call that times out to an attendant after the interval that is administered for the Attendant Return Call timer.
- Attendant Timed Reminder of Held Call Timer. Specifies how long a call is held. When the timer expires, the held call alerts the attendant. The message "**hc**" appears on the attendant display. You can administer either a high-pitched ring or a primary alert.

- Attendant No-Answer Timer. Specifies how long a call that terminates at an attendant console can ring with primary alerting. When the timer expires, the call rings with a secondary, higher-pitch ring. The ringing pattern of a disabled Attendant No Answer Timer does not change over from the primary pattern to the secondary pattern. If the call remains unanswered during this interval, the system routes the call to the attendant group and console where the call was placed in a Position Busy state. This timer does not apply to calls that are placed to the extension of the attendant, or to calls that the attendant originates.
- Attendant Alerting Interval (Timed Reminder). Specifies how long a call that terminates at an attendant console can ring with secondary alerting. When the timer expires, the attendant console is placed into position busy mode, and the system forwards the call to the attendant group. If the console where the alerting interval is reached is the last active day console, the system goes into Night Service, if Night Service is enabled. This timer does not apply to calls that are placed to the extension of the attendant, or to calls that the attendant originates.

  You can disable the alerting interval. In this case, a call continues to ring at the extension of the original attendant until the caller hangs up, or another feature disconnects the call. If the call reaches the timeout limit for unanswered DID calls during Night Service, for example, the Night Service feature disconnects the call.
- Line Intercept Tone Timer. Specifies how long line intercept can be. For example, LITT:10 seconds means that line intercept stops after 10 seconds.

Administering Attendant Timers

The following steps are part of the administration process for the Attendant Timers feature:

- Setting up Attendant Timers

This section describes:

- Any prerequisites for administering the Attendant Timers feature
- The screens that you use to administer the Attendant Timers feature
- Complete administration procedures for the Attendant Timers feature

Prerequisites for administering Attendant Timers

You must complete the following actions before you can administer the Attendant Timers feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Attendant Timers

Screen name	Purpose	Fields
Console Parameters	Set up the timers for the attendant.	All fields in both the **Timing** and the **Incoming Call Reminders** areas

Setting up Attendant Timers

To set up Attendant Timers:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen.

2. Click **Next** until you see the **Timing** area (Figure 52: Console Parameters screen on page 287).

Figure 52: Console Parameters screen

```
change console-parameters                                    Page   2 of 4
                              CONSOLE PARAMETERS

TIMING
  Time Reminder on Hold (sec): 10           Return Call Timeout (sec): 10
  Time in Queue Warning (sec):

  INCOMING CALL REMINDERS
      No Answer Timeout (sec): 20                      Alerting (sec): 40
                               Secondary Alert on Held Reminder Calls? y

ABBREVIATED DIALING
     List1: group    1        List2:                  List3:
            SAC Notification? n
                           COMMON SHARED EXTENSIONS
            Starting Extension:                Count:
```

3. In the **Timing** area, complete the following fields:

   - In the **Time Reminder on Hold (sec)** field, type the number of seconds before a split call returns to the console. Valid entries are a number from 10 to 1024, or blank. A split

call can be a call that the attendant extended to a user and is ringing at the user telephone, or otherwise split away from the console.

Allow 5 seconds for each ring at all points in a coverage path to ensure that the entire path is completed before the call returns to the console.

- In the **Return Call Timeout (sec)** field, type the number of seconds that a call remains on hold at the console before the system alerts the attendant. In a Centralized Attendant Service (CAS) arrangement, administer the main console and the branch consoles with the same value. Valid entries are a number from 10 to 1024, or blank.
- In the **Time in Queue Warning (sec)** field, type the number of seconds that a call can remain in the attendant queue before the system alerts the attendant. Valid entries are a number from 9 to 999.

4. In the **Incoming Call Reminders** area, complete the following fields:
   - In the **No Answer Timeout (sec)** field, type the number of seconds that a call to the attendant can remain unanswered without invoking a more insistent-sounding tone. Valid entries are a number from 10 to 1024, or blank.

     Allow 5 seconds for each ring at all points in a coverage path to ensure that the entire path is completed before the call returns to the console.
   - In the **Alerting (sec)** field, type the number of seconds after which the system disconnects a held call or an unanswered call from an attendant loop. The system routes the disconnected call either to another attendant or to Night Service. Valid entries are a number from 10 to 1024, or blank.
   - In the **Secondary Alert on Held Reminder Calls?** field, perform one of the following actions:
     - If you want to start attendant alerting for Held Reminder Calls with secondary alerting, type **y**
     - If you want to have Held Reminder Calls alert the attendant in the same way as normal calls, type **n**. Normal calls start with primary alerting, and then change to secondary alerting when the No Answer Timeout expires.
5. Press **Enter** to save your changes.

Interactions for Attendant Timers

This section provides information about how the Attendant Timers feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Timers in any feature configuration.

- Call Coverage

  If a telephone user transfers a call to an on-premises telephone, and the call remains unanswered at the expiration of the Timed Reminder Interval, the system redirects the call to an attendant. Redirection occurs even if the call redirects through Call Coverage or Call Forwarding from the transferred-to telephone.

  The system redirects an attendant-extended call to coverage instead of returning the call to an attendant if the coverage criteria is met before the Timed Reminder Interval expires. However, the system returns unanswered calls to an attendant at the expiration of the interval.

  For any call that alerts an attendant as a coverage call, that is, for any unanswered station-to-station call with the "attd" (attendant) in the Coverage Path screen of the called telephone, the secondary alerting tone does not sound.

- Centralized Attendant Service

  If an attendant at the main location transfers a call from a branch location to an extension at the main location, the timed reminder does not apply, and the call does not return to the attendant if the call is unanswered.

Return Call to (same) Attendant

Communication Manager Release 5.2 provides improvements to the existing attendant features with Return Call to (same) Attendant feature.

Generally, when an attendant offers a call to a destination that does not answer and has no coverage path, the call returns to the same attendant. If this attendant is busy or unavailable, the call returns to the attendant's group queue.

Communication Manager Release 5.2 provides individual queuing functions for each attendant supporting a multiplicity of waiting calls at a given time. When at least one call is waiting in the above queue, the Individual Calls Waiting Indicator is displayed in red. Calls queue as long as the attendant is busy.

When the feature Return Call to (same) Attendant is enabled, a call returning to a busy or now unavailable same attendant is placed into an individual waiting queue for this attendant, instead of queuing it into the attendant group. A waiting Return Call moves from the attendant's queue to the attendant group's queue after a certain period of time.

The field **Overflow timer to Group Queue** is extended to page 2 of the console-parameters screen, as shown in Figure 53.

Figure 53: Change/Display console-parameters screen (with extension)

```
display console-parameters                                    Page 2 of x
                              CONSOLE PARAMETERS

TIMING
  Time Reminder on Hold (sec): 30              Return Call Timeout (sec): 30
  Time in Queue Warning (sec):        Overflow timer to Group Queue (sec): 1024

  INCOMING CALL REMINDERS
      No Answer Timeout (sec):                          Alerting (sec):
                               Secondary Alert on Held Reminder Calls? n

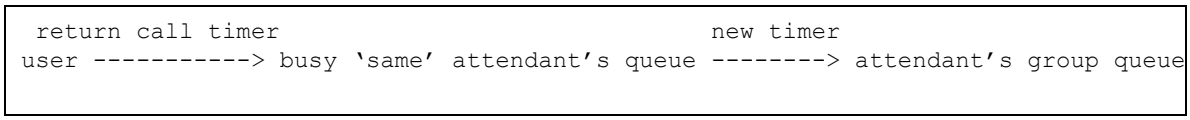
ABBREVIATED DIALING
     List1:                   List2:                   List3:
             SAC Notification? n

                           COMMON SHARED EXTENSIONS
            Starting Extension:                  Count:
   Busy Indicator for Call Parked on Analog Station Without Hardware? n
```

Attendant Overflow Timer

When a call enters the same attendant's queue, the timer in the **Attendant Overflow Timer** starts. Once the time in the timer expires, the call moves to the **attendant's group queue**, as shown in Figure 54:

Figure 54: Attendant Overflow Timer



Attendant Trunk Identification

Use the Attendant Trunk Identification feature to enable the attendant, or a user with a display, to identify a faulty trunk

Detailed description of Attendant Trunk Identification

This section provides a detailed description of the Attendant Trunk Identification feature.

With Attendant Trunk Identification, the attendant, or a user with a display, can identify a faulty trunk. When the attendant or user presses the trk-id button, the system displays the Trunk Access Code (TAC) and trunk member number of a call. The trunk can then be removed from service.

Administering Attendant Trunk Identification

This section contains the prerequisites and screens for administering the Attendant Trunk Identification feature.

Prerequisites for administering Attendant Trunk Identification

You must complete the following actions before you can administer the Attendant Trunk Identification feature:

- Set up an attendant console. For information on how to set up an attendant console, see the *Administering Avaya Aura™ Communication Manager*.

Screens for administering Attendant Trunk Identification

Screen name	Purpose	Fields
Attendant Console	Administer the trk-id button for the Attendant Trunk Identification feature.	Any available button field in the **Feature Button Assignments** area
Station	Administer the trk-id button for the Attendant Trunk Identification feature.	Any available button field in the **Feature Button Assignments** area

Attendant Vectoring

Use the Attendant Vectoring feature to provide attendants with a flexible way to manage incoming calls. For example, without Attendant Vectoring, calls that the system redirects from the attendant console to a night telephone can ring only at that telephone. These calls do not follow a coverage path. With Attendant Vectoring, Night Service calls follow the coverage path of the night telephone. The coverage path can go to another telephone, and eventually to a voice mail system. The caller can then leave a message that can be retrieved at any time.

Detailed description of Attendant Vectoring

This section provides a detailed description of the Attendant Vectoring feature.

With the Attendant Vectoring feature, you can establish an attendant vector directory number (VDN), and send attendant group calls through vector processing. This feature is useful when you want flexibility with how the system routes calls when the system is in Night Service mode.

Attendant Vectoring takes precedence over all local attendant codes that you administer. If Attendant Vectoring is enabled, the system uses call vectors instead of the normal attendant call routing to process attendant-seeking, or dial 0, calls.

For more information about vectors and VDNs, see the Meet-Me Conference feature. See also the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780

Administering Attendant Vectoring

The following steps are part of the administration process for the Attendant Vectoring feature:

- Creating a VDN extension for Attendant Vectoring
- Assigning the VDN extension for Attendant Vectoring to a console
- Assigning the VDN extension for Attendant Vectoring to a tenant

This section describes:

- Any prerequisites for administering the Attendant Vectoring feature
- The screens that you use to administer the Attendant Vectoring feature
- Complete administration procedures for the Attendant Vectoring feature

Prerequisites for administering Attendant Vectoring

You must complete the following actions before you can administer the Attendant Vectoring feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
- On the Optional Features screen, verify the values in the following fields. Your license file sets the values in these fields. You cannot manually change these values. If you have any questions, contact your Avaya representative.

To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

1. Click **Next** until you see the **Attendant Vectoring** field. Ensure that the **Attendant Vectoring** field is set to **y**.
2. You cannot use Attendant Vectoring with the Centralized Attendant Service (CAS) feature. Therefore, the **Attendant Vectoring** field cannot be set to **y** if either the **CAS Branch** field or the **CAS Main** field on the Optional Features screen is set to **y**.

On the Call Vector screen, verify that the **Attendant Vectoring** field is set to **y**. To view the Call Vector screen, type **`change vector n`**, where ***n*** is the number of a vector. Press **Enter**.

1. This field appears on the Call Vector screen only if, on the Optional Features screen, the **Attendant Vectoring** field is set to **y**.
2. The **Attendant Vectoring** field on the Call Vector screen defaults to **n**.
3. You cannot use the same vector for both Attendant Vectoring and the Meet-me Conference features. Therefore, the **Attendant Vectoring** field and the **Meet-me Conference** field cannot both be set to **y** at the same time.

Screens for administering Attendant Vectoring

Screen name	Purpose	Fields
Optional Features	Ensure that the Attendant Vectoring feature is activated.	**Attendant Vectoring**
	Ensure that fields are correctly set so that you can: • Verify the Attendant Vectoring feature on the Call Vector screen • Administer the Attendant Vectoring feature on the Console Parameters screen. See the "Prerequisites" section for the correct settings.	**Tenant Partitioning**
Call Vector	Ensure that the **Attendant Vectoring** field is set to **y**.	**Attendant Vectoring**
Vector Directory Number	Create an Attendant Vectoring VDN extension.	**Attendant Vectoring**
Console Parameters	Assign the Attendant Vectoring VDN extension to a console.	**Attendant Vectoring VDN**
Tenant	Assign the Attendant Vectoring VDN extension to a tenant.	**Attendant Vectoring VDN**

Creating a VDN extension for Attendant Vectoring

Use the Vector Directory Number screen to define vector directory numbers (VDNs) for the Call Vectoring feature. A VDN is an extension that gives you access to a call vector. Each VDN is mapped to one call vector.

VDNs are not assigned to physical equipment. You gain access to a VDN through direct dial central office (CO) trunks that are mapped to the VDN, direct inward dial (DID) trunks, and listed directory number (LDN) calls. The VDN can be a night destination for LDN.

To create a VDN extension for Attendant Vectoring:

1. Type **`change vdn n`**, where ***n*** is the VDN extension. Press **Enter**.

   The system displays the Vector Directory Number screen (Figure 55: Vector Directory Number screen on page 296).

Figure 55: Vector Directory Number screen

```
change vdn 5000                                                Page  1 of 1
                        VECTOR DIRECTORY NUMBER

                              Extension: 5000
                                   Name:
                         Vector Number: 234
                    Attendant Vectoring: y
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 59
                                    TN: 1
                              Measured: none
        Acceptable Service Level (sec):
         VDN of Origin Annc. Extension: 301
                              1st Skill:
                              2nd Skill:
                              3rd Skill:
```

2. In the **Attendant Vectoring** field, perform one of the following actions:
   - If you want this VDN to be an attendant vector, type **y**.
   - If you do not want this VDN to be an attendant vector, type **n**.

   You cannot use Attendant Vectoring with the Meet-me Conference feature. Therefore, the **Attendant Vectoring** field and the **Meet-Me Conferencing** field cannot both be set to **y** at the same time.
3. Press **Enter** to save your changes.

Assigning the VDN extension for Attendant Vectoring to a console

The **Attendant Vectoring VDN** field appears on the Console Parameters screen only if, on the Optional Features screen, the:

- **Attendant Vectoring** field is set to **y**
- **Tenant Partitioning** field is set to **n**

To assign the VDN extension for Attendant Vectoring to a console:

1. Type **`change console-parameters n`**, where ***n*** is the assigned number of the attendant console. Press **Enter**.

   The system displays the Console Parameters screen (Figure 56: Console Parameters screen on page 297).

Figure 56: Console Parameters screen

```
change console-parameters                                    Page   1 of 4
                              CONSOLE PARAMETERS
         Attendant Group Name: OPERATOR
                          COS: 0                                    COR: 0
       Calls in Queue Warning: 5                    Attendant Lockout? y
        Ext Alert Port (TAAS):
                          CAS: none
                                                Night Service Act. Ext.:
                IAS (Branch)? n                 IAS Tie Trunk Group No.:
          IAS Att. Access Code:                   Alternate FRL Station:
               Backup Alerting? n          DID-LDN Only to LDN Night Ext? n
     Attendant Vectoring VDN: 5000
```

2. In the **Attendant Vectoring VDN** field, type the VDN extension that you have created for Attendant Vectoring.
3. Press **Enter** to save your changes.

Assigning the VDN extension for Attendant Vectoring to a tenant

Use the Tenant screen to define tenants that access the system. If your server uses more than one tenant, see the "Tenant Partitioning" feature for more information.

To assign the VDN extension for Attendant Vectoring to a tenant:

1. Type **`change tenant n`**, where ***n*** is the assigned number of the tenant. Press **Enter**.

   The system displays the Tenant screen (Figure 57: Tenant screen on page 298).

Figure 57: Tenant screen

```
change tenant 18
                            Tenant 18

               Tenant Description: ____________________________________________

                  Attendant Group: 1

            Ext Alert Port (TAAS): ________ Ext Alert (TAAS) Extension: ____

                Night Destination: _____

                     Music Source: 1

          Attendant Vectoring VDN: 5000

                 Emergency Number:
```

2. In the **Attendant Vectoring VDN** field, type the VDN extension that you created for Attendant Vectoring.
3. Press **Enter** to save your changes.

Considerations for Attendant Vectoring

This section provides information about how the Attendant Vectoring feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Attendant Vectoring under all conditions. The following considerations apply to Attendant Vectoring:

- Teletypewriter device (TTY) for the hearing impaired

  Unlike fax machines and modems, a TTY has no handshake tone and no carrier tone. A TTY is silent when not transmitting. Systems cannot automatically identify TTY callers.

  However, the absence of these special tones also means that voice and TTY tones can be intermixed in prerecorded announcements. The ability to provide a hybrid voice-and-TTY announcement, when combined with the Attendant Vectoring capability, can permit a single telephone number to accommodate both voice and TTY callers.

Interactions for Attendant Vectoring

This section provides information about how the Attendant Vectoring feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Attendant Vectoring in any feature configuration.

- Centralized Attendant Service (CAS)

  You cannot use Attendant Vectoring with the Centralized Attendant Service (CAS) feature. Therefore, the **Attendant Vectoring** field cannot be set to **y** if either the **CAS Branch** field or the **CAS Main** field on the Optional Features screen is set to **y**.

- Meet-me Conference

  You cannot use Attendant Vectoring with the Meet-me Conference feature. Therefore, the **Attendant Vectoring** field and the **Meet-me Conference** field cannot both be set to **y** at the same time.

Audible Message Waiting

Use the Audible Message Waiting feature to alert a user that a message is waiting. The user hears a stutter dial tone when the user goes off hook.

The Audible Message Waiting feature is particularly useful for visually impaired people who cannot see a message waiting light.

Detailed description of Audible Message Waiting

This section provides a detailed description of the Audible Message Waiting feature.

Use the Audible Message Waiting feature to alert a user that a message is waiting. When the user goes off hook, the user hears a stutter tone just before the usual dial tone begins.

Users can access waiting messages from:

- The system memory, where a user can use a display or a voice synthesizer
- A Property Management System (PMS)
- A CM Messaging voice message system

You must ensure that your users know how to retrieve their messages.

You usually assign Audible Message Waiting on telephones without message waiting lights, such as analog telephones.

If the system loses synchronization between telephones and message-status data, use the Clear Message Waiting Indicators to turn off the message waiting indicators.

Audible Message Waiting requires a separate software right-to-use fee.

Audible Message Waiting might not be applicable in countries that restrict the characteristics of dial tones that the system provides to users.

Administering Audible Message Waiting

The following steps are part of the administration process for the Message Waiting feature:

- Administering Audible Message Waiting for a user

This section describes:

- Any prerequisites for administering the Message Waiting feature
- The screens that you use to administer the Message Waiting feature
- Complete administration procedures for the Message Waiting feature

Prerequisites for administering Audible Message Waiting

You must complete the following actions before you can administer the Audible Message Waiting feature:

- View the Optional Features screen, and ensure that the **Audible Message Waiting** field is set to **y**. If the **Audible Message Waiting** field is set to **n**, your system is not enabled for the Audible Message Waiting feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Audible Message Waiting

Screen name	Purpose	Fields
Optional Features	Enable Audible Message Waiting for your system.	**Audible Message Waiting**
Station	Administer Audible Message Waiting for a user.	**Audible Message Waiting**

Administering Audible Message Waiting for a user

To activate Audible Message Waiting for a user:

1. Type **`change station`** ***`n`***, where ***`n`*** is the extension of the user for whom you want to activate Audible Message Waiting. Press **Enter**.

   The system displays the Station screen (Figure 58: Station screen on page 303).

Figure 58: Station screen

```
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe            Auto Select Any Idle Appearance? n
          LWC Activation? y                      Coverage Msg Retrieval? y
  LWC Log External Calls? n                                Auto Answer: none
            CDR Privacy? n                           Data Restriction? n
   Redirect Notification? y                  Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                    Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n        Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: enhanced             Audible Message Waiting? y
    MWI Served User Type:                    Display Client Redirection? n
             AUDIX Name:                   Select Last Used Appearance? n
                                             Coverage After Forwarding? y
                                               Multimedia Early Answer? n
                                        Direct IP-IP Audio Connections? y
 Emergency Location Ext: 30019                    IP Audio Hairpinning? y
```

2. In the **Audible Message Waiting** field, perform one of the following actions:
   - If you want the user to the hear stutter dial tone if a message is waiting when the user goes off hook, type **y**.
   - If you do not want the user to the hear stutter dial tone if a message is waiting when the user goes off hook, type **n**.

   The system displays the **Audible Message Waiting** field only if the **Audible Message Waiting** field on the Optional Features screen is set to **y**.

   Note that the **Audible Message Waiting** field does not control the Message Waiting lamp.

Considerations for Audible Message Waiting

This section provides information about how the Audible Message Waiting feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Audible Message Waiting under all conditions. The following considerations apply to Audible Message Waiting:

- You must tell the user where to call to retrieve messages if the messages are not stored in the system memory for users to access by way of a display or a voice synthesizer.

Interactions for Audible Message Waiting

This section provides information about how the Audible Message Waiting feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Audible Message Waiting in any feature configuration.

- China Special Dial Tone. The Audible Message Waiting feature interacts with the Special Dial Tone feature. This interaction is for customers in China only. This feature plays a special dial tone whenever an analog telephone would normally receive dial tone, but the user needs to know about a feature or condition that is active at the telephone. Examples of such features or conditions include features that can be activated and deactivated by using a FAC from the telephone, and cause some rerouting of calls to that telephone.

AUDIX One-Step Recording

Use the AUDIX One-Step Recording feature to record telephone conversations by pressing a single button. The AUDIX One-Step Recording feature uses CM Messaging to record a telephone conversation. A user needs to press only one feature button on the telephone to activate this feature. AUDIX One-Step Recording then stores the recorded conversation as a message in the voice mailbox of the user. The system allows AUDIX One-Step Recording only after a call is answered.

Note:
Some countries, states, and localities have laws that determine if and under what circumstances you can record telephone conversations. Before you administer the AUDIX One-Step Recording feature, you must understand and comply with these laws.

Note:
Starting with Communication Manager Release 5.2, Intuity Audix IA770 application is called Communication Manager Messaging.

Detailed description of AUDIX One-Step Recording

This section provides a detailed description of the AUDIX One-Step Recording feature.

The AUDIX One-Step Recording feature is available with Communication Manager Release 1.3 (V11) or later.

- Communication Manager Release 1.3 supports AUDIX One-Step Recording only when the CM Messaging system is local.
- Communication Manager Release 2.0 and later supports AUDIX One-Step Recording with a local CM Messaging system or with a remote CM Messaging system. To use a remote CM Messaging system, the person recording the conversation must have Communication Manager Release 2.0 or later.

Feature button

The AUDIX One-Step Recording feature uses an administered feature button, **audix-rec**. The administrator uses the Station screen to assign this button for each telephone. When you assign the feature button, the system requires you to provide the extension for the CM Messaging hunt group of the user. Users cannot access AUDIX One-Step Recording on any telephone that does not have an administrable feature button, or on an attendant console.

Language options

Five languages are available for the feature button labels for AUDIX One-Step Recording:

- English
- Italian
- French
- Spanish
- A user-defined language

The feature button labels for AUDIX One-Step Recording are available in English, with predefined Italian, French, and Spanish translations. The administrator cannot change the text of the English, the Italian, the French, or the Spanish feature button labels.

The administrator can translate the feature button labels into a user-defined language. This translation can be any other language that the customer chooses, such as German. The administrator can use only one user-defined language throughout the system.

Periodic alerting tone

While CM Messaging records the conversation, all parties on the call might hear a periodic alerting tone. This alerting tone reminds all parties on the call that CM Messaging is recording the conversation. The tone that plays is a zip tone.

You choose the time interval to play the periodic alerting tone. If you set the time interval of the periodic alerting tone to zero, the parties hear no alerting tone.

Ready indication tone

When CM Messaging starts recording the conversation, the system plays a ready indication tone. The tone that plays is a zip tone.

The administrator can set the ready indication tone to play to:

- All the parties on the call.
- The initiator only.

  The "initiator" is the user who activates the AUDIX One-Step Recording feature.
- None of the parties on the call.

Recording delay timer

When the user presses the **audix-rec** feature button, CM Messaging answers. After CM Messaging answers, the system uses the recording delay timer to wait for CM Messaging to get ready to interpret digits. The system then sends digit 1 to tell CM Messaging to start recording.

The recording delay timer is preset to 500 milliseconds. This delay is sufficient for most recorded conversations. If you have to change this setting, see the section titled Assigning AUDIX One-Step Recording Parameters.

Administering AUDIX One-Step Recording

The following steps are part of the administration process for the AUDIX One-Step Recording feature:

- Assigning AUDIX One-Step Recording Parameters
- Translating telephone feature buttons and labels
- Assigning the feature button to a telephone
- Changing the characteristics of the zip tone

This section describes:

- Any prerequisites for administering the AUDIX One-Step Recording feature
- The screens that you use to administer the AUDIX One-Step Recording feature
- Complete administration procedures for the AUDIX One-Step Recording feature

Prerequisites for administering AUDIX One-Step Recording

You must complete the following actions before you can administer the AUDIX One-Step Recording feature:

- On the Optional Features screen, ensure that the **G3 Version** field is set to **V11** or later. If this field is not set to **V11** or later, your system is not enabled for the AUDIX One-Step Recording feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering AUDIX One-Step Recording

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 1.3 (V11) or later.	**G3 Version**
Feature-Related System Parameters	Set the time interval, in milliseconds, for the recording delay timer.	**Recording Delay Timer (msec)**
	Assign who on the call can hear the ready indication tone.	**Apply Ready Indication Tone To Which Parties In The Call**
	Set the time interval, in seconds, for the periodic alerting tone.	**Interval For Applying Periodic Alerting Tone (seconds)**
Language Translations	If needed, change the translation of the **audix-rec** feature button to a user-defined language.	**Audix Recording**
	If needed, change the translation of the **Audix Record** button label to a user-defined language.	**Audix Record**
Station	Assign the **audix-rec** feature button, and associate the hunt group extension of the user.	**Button Assignments**

Assigning AUDIX One-Step Recording Parameters

To assign the recording delay timer, the ready indication tone, and the periodic alerting tone:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **AUDIX One-step Recording** area (Figure 59: Feature-Related System Parameters screen on page 309).

Figure 59: Feature-Related System Parameters screen

```
change system-parameters features                              Page 6 of 12

                        FEATURE-RELATED SYSTEM PARAMETERS

CONFERENCE/TRANSFER

               Abort Transfer? n                  No Dial Tone Conferencing? n
        Transfer Upon Hang-Up? n        Select Line Appearance Conferencing? n
Abort Conference Upon Hang-Up? n                                    Unhold? n
   No Hold Conference Timeout: 60

ANALOG BUSY AUTO CALLBACK
                Without Flash? n


AUDIX ONE-STEP RECORDING
                            Recording Delay Timer (msec): 500
Apply Ready Indication Tone To Which Parties In The Call? all
  Interval For Applying Periodic Alerting Tone (seconds): 15
```

3. If you need to change the time between when CM Messaging answers and when CM Messaging starts recording, change the value in the **Recording Delay Timer (msec)** field. The time is measured in milliseconds in increments of 100. The default setting is 500 milliseconds.

   After CM Messaging starts recording, Communication Manager must filter out the CM Messaging tone. The user must wait longer than the Recording Delay Timer setting before the user notices that recording has started.

4. In the **Apply Ready Indication Tone To Which Parties In The Call** field, type one of the following values. These values indicate who hears the ready indication tone:

   - If you want all parties on the call to hear the ready indication tone, leave the default set to **all**. The screen displays the **Interval For Applying Periodic Alerting Tone (seconds)** field.
   - If you want only the initiator to hear the ready indication tone, right-click the field and select **initiator**. The screen does not display the **Interval For Applying Periodic Alerting Tone (seconds)** field.
   - If you want no one on the call to hear the ready indication tone, right-click the field and select **none**. The screen does not display the **Interval For Applying Periodic Alerting Tone (seconds)** field.

5. In the **Interval For Applying Periodic Alerting Tone (seconds)** field, type a value between **0** and **60** seconds. This value indicates how often all parties on the call hear the periodic alerting tone.

   The default value is **15** seconds. If you set the value to **0**, no one on the call hears the periodic alerting tone.

6. Press **Enter** to save your changes.

Translating telephone feature buttons and labels

To translate telephone feature buttons and labels for AUDIX One-Step Recording to a user-defined language, you must complete the following procedures:

- Translating the AUDIX One-Step Recording text that appears on a telephone display to a user-defined language
- Translating the AUDIX One-Step Recording button label to a user-defined language

Translating the AUDIX One-Step Recording text that appears on a telephone display to a user-defined language

To translate the text that appears on your telephone display, when this feature is recording, to a user-defined language:

1. Type **`change display-messages view-buttons`**. Press **Enter**.

   The system displays the Language Translations screen.

2. Click **Next** until you see the **Audix Recording** field (Figure 60: Language Translations screen on page 311).

Figure 60: Language Translations screen

```
change display-messages view-buttons                          Page 9 of 9

                            LANGUAGE TRANSLATIONS

English                                  Translation

1.  Station Lock                         ****************************
2.  License Error                        ****************************
3.  Conference Display                   ****************************
4.  Conf/Trans Toggle-Swap               ****************************
5.  Posted Messages                      ****************************
6.  Audix Recording                      ****************************
```

3. In the **Translation** field, type a translated name for **Audix Recording** into the user-defined language.

   Note that the language translations for the English, the Italian, the French, and the Spanish feature display are predefined. You cannot change the text for these translations.

4. Press **Enter** to save your changes.

Translating the AUDIX One-Step Recording button label to a user-defined language

The 2420 DCP telephone and the 4620 IP telephone have digital button labels instead of paper labels. If you need to translate the AUDIX One-Step Recording button labels into a user-defined language for these telephones, follow this procedure.

To translate the AUDIX One-Step Recording button label for the 2420 DCP telephone and the 4620 IP telephone to a user-defined language:

1. Type **`change display-messages button-labels`**. Press **Enter**.

   The system displays the Language Translations screen.

2. Click **Next** until you see the **Audix Record** field (Figure 61: Language Translations screen on page 312).

Figure 61: Language Translations screen

```
change display-messages button-labels                          Page 9 of 9

                              LANGUAGE TRANSLATIONS

English                                    Translation

 1. Alternate FRL                           1. *************
 2. ANI Request                             2. *************
 3. Assist                                  3. **********
 4. ASVN Halt                               4. *************
 5. AttQueueCall                            5. *************
 6. AttQueueTime                            6. *************
 7. Audix Record                            7. *************
 8. Auto Callback                           8. *************
 9. Auto Chk Halt                           9. *************
10. AutoIC                                 10. *******
11. Auto In                                11. **********
12. AutoWakeAlarm                          12. *************
13. Auto Wakeup                            13. *************
14. AuxWork                                14. ********
15. Busy                                   15. *****
```

3. In the **Translation** field, type a translated name for the **Audix Record** button label into the user-defined language.

   Note that the language translations for the English, the Italian, the French, and the Spanish feature buttons are predefined. You cannot change the text for these translations.

4. Press **Enter** to save your changes.

Assigning the feature button to a telephone

To assign the **audix-rec** feature button to an individual telephone:

1. Type **`change station n`**, where ***n*** is the extension of the telephone. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 62: Station screen on page 313).

Figure 62: Station screen

```
change station 9876                                          Page 3 of 3

                                    STATION

 SITE DATA
      Room:                                      Headset? n
      Jack:                                      Speaker? n
     Cable:                                     Mounting: d
     Floor:                                  Cord Length: 0
  Building:                                    Set Color:




ABBREVIATED DIALING
     List1:                List2:                List3:

BUTTON ASSIGNMENTS
 1. call-appr                          6.
 2. call-appr                          7.
 3. call-appr                          8.
 4. audix-rec  Ext: 9800               9.
 5.                                   10.
```

3. Right-click a button field that is not assigned to see a list of button names. Select **audix-rec** from the list.

   The screen displays an **Ext** field.

4. In the **Ext** field, type the CM Messaging hunt group extension of the user.
5. Press **Enter** to save your changes.

Changing the characteristics of the zip tone

When the AUDIX One-Step Recording feature is recording a conversation, the tone that a user hears is a zip tone. By default, a zip tone plays at a frequency of 480 Hz for 500 milliseconds, followed by silence.

If you need to change the characteristics of the zip tone, the screen that you use depends on what version of Communication Manager you have.

To change the characteristics of the zip tone if you have Communication Manager Release 2.0 (V12) or later:

1. Type **change tone-generation**. Press **Enter**.

   The system displays the Tone Generation screen.

2. Click **Next** until you see either:

   - An existing Tone Generation Customized Tones screen for the zip tone

     If a screen already exists for the zip tone, the word **zip** appears in the **Tone Name** field.

   - A blank Tone Generation Customized Tones screen (Figure 63: Tone Generation Customized Tones screen on page 314).

Figure 63: Tone Generation Customized Tones screen

```
change tone-generation                                          Page 4 of 21

                        TONE GENERATION CUSTOMIZED TONES

     Tone Name            Cadence          Tone
                           Step      (Frequency/Level)
                             1:
                             2:
                             3:
                             4:
                             5:
                             6:
                             7:
                             8:
                             9:
                            10:
                            11:
                            12:
                            13:
                            14:
                            15:
```

   If a screen already exists for the zip tone, skip the next step and go to Step 4.

3. Right-click the **Tone Name** field to see a list of options. Select **zip** from the list.
4. Right-click the **Cadence Step 1** field to see a list of options. Select a tone frequency and level combination from the list.

   The screen displays a **Duration (msec)** field.

5. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to play.

6. Right-click the **Cadence Step 2** field to see a list of options. Select **silence** from the list.

   The screen displays a **Duration (msec)** field.

7. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to remain silent after the system plays the tone.
8. Press **Enter** to save your changes.

To change the characteristics of the zip tone if you have Communication Manager Release 1.3 (V11) or earlier:

1. Type **`change system-parameters country-options`**. Press **Enter**.

   The system displays the System Parameters Country-Options screen.

2. Click **Next** until you see either:
   - An existing System Parameters Country-Options screen for the zip tone

     If a screen already exists for the zip tone, the word **zip** appears in the **Tone Name** field.

   - A blank System Parameters Country-Options screen (Figure 64: System Parameters Country-Options screen on page 315).

Figure 64: System Parameters Country-Options screen

```
change system-parameters country-options                        Page 7 of 24

                        SYSTEM PARAMETERS COUNTRY-OPTIONS

     Tone Name            Cadence          Tone
                           Step      (Frequency/Level)
                             1:
                             2:
                             3:
                             4:
                             5:
                             6:
                             7:
                             8:
                             9:
                            10:
                            11:
                            12:
                            13:
                            14:
                            15:
```

   If a screen already exists for the zip tone, skip the next step and go to Step 4.

3. Right-click the **Tone Name** field to see a list of options. Select **zip** from the list.

4. Right-click the **Cadence Step 1** field to see a list of options. Select a tone frequency and level combination from the list.

   The screen displays a **Duration (msec)** field.

5. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to play.
6. Right-click the **Cadence Step 2** field to see a list of options. Select **silence** from the list.

   The screen displays a **Duration (msec)** field.

7. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to remain silent after the system plays the tone.
8. Press **Enter** to save your changes.

End-user procedures for AUDIX One-Step Recording

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for the AUDIX One-Step Recording feature.

Recording a conversation

The user who wants to record the conversation is called the "initiator."

Note:
This procedure assumes that the initiator understands and complies with any country, state, and local laws concerning if you can record telephone conversations.

1. A user announces to the other parties on the call that he or she wants to record the conversation.

2. This user gets permission from the parties, and presses the **audix-rec** button to record the conversation.

   When the initiator presses the **audix-rec** button, the LED for the **audix-rec** button flashes. After a few seconds, the telephone displays of all internal users on the call change to **Conference**. The number of parties on the call increases by one. The LED on the telephone of the initiator stays on, and no longer flashes. This light indicates that CM Messaging is ready to record.

   CM Messaging starts to record the conversation. The system plays the ready indication tone to indicate that recording is started. Only the initiator hears any CM Messaging announcements.

3. To stop the recording at any time, the initiator can press the **audix-rec** button again. The LED on the telephone of the initiator goes out. The number of parties on the call decreases by one. The call remains active. The initiator can press the **audix-rec** button to start and stop recording the same conversation any number of times. Each time creates a separate recorded message.

   If the initiator hangs up while CM Messaging is recording the conversation, the recording ends. If the call is originally a two-party call and the other party hangs up, the recording ends. If the call is originally a multiple-party conference call and someone other than the initiator hangs up, the recording continues.

   When the recording ends, the system saves the recorded conversation in the voice mailbox of the initiator as a new voice mail message.

Considerations for AUDIX One-Step Recording

This section provides information about how the AUDIX One-Step Recording feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of AUDIX One-Step Recording under all conditions. The following considerations apply to the AUDIX One-Step Recording feature:

- Capacity constraints and feature limitations

  AUDIX One-Step Recording has the following capacity constraints and feature limitations:

  - Only one simultaneous CM Messaging recording is allowed for each call.
  - The **audix-rec** feature button works as a toggle button. When the button is active, the button is associated with only one call. A user cannot use the **audix-rec** feature button on two calls simultaneously.
  - Attendant consoles do not have an **audix-rec** feature button. Attendants cannot use the AUDIX One-Step Recording feature.
  - Service observers who are actively involved in service observing cannot use the AUDIX One-Step Recording feature.

- Denial scenarios

  The AUDIX One-Step Recording feature is denied, and the feature button flutters, if a user presses the **audix-rec** button when:

  - No call is active on the telephone
  - The user is still dialing digits
  - The connection to CM Messaging is not operating
  - All CM Messaging ports are busy
  - The number of parties on the call reaches the administered maximum
  - Another party on the call is already recording the conversation with AUDIX One-Step Recording
  - The user starts the recording from a bridged call appearance
  - Service observers are actively involved in service observing
  - The incoming or outgoing call is ringing and is not answered

- Security

  Some countries, states, and localities have laws that determine if and under what circumstances you can record telephone conversations. Before you administer the AUDIX One-Step Recording feature, you must understand and comply with these laws.

- Serviceability

  This feature depends on CM Messaging to function. The administrator is responsible for properly administering CM Messaging. CM Messaging must work for the telephone user before the administrator applies this feature to the telephone. Specifically, the administrator needs to set the appropriate **Mailbox Size** and **Voice Mail Message Maximum Length** on CM Messaging for the user.

  The **audix-rec** button requires the extension of the CM Messaging hunt group of the user. The administrator must type the correct extension on the Station screen.

Interactions for AUDIX One-Step Recording

This section provides information about how the AUDIX One-Step Recording feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of AUDIX One-Step Recording in any feature configuration. The following interactions apply to the AUDIX One-Step Recording feature:

- Bridged Call Appearance
  - A user cannot activate or deactivate the **audix-rec** feature button from a bridged call appearance.

  - If the administrator sets the ready indication tone to play to all parties, parties on bridged call appearances hear the tone. If the administrator sets the ready indication tone to play to the initiator only, parties on bridged call appearances do not hear the tone.

- Call Park

  When AUDIX One-Step Recording is active on a call, the system does not allow the user to park the call. If the user attempts to park the call, the call appearance LED flutters.

  When a call is parked, the system does not allow the user to activate AUDIX One-Step Recording. If the user attempts to activate AUDIX One-Step Recording, the feature button LED flutters.

- Conference

  When the recording request is in process, the LED is flashing. If anyone attempts to conference in another party, AUDIX One-Step Recording stops. The LED goes out.

  When the recording starts, the LED is on but not flashing. Any party on the call can conference in another party. The recording continues.

  If AUDIX One-Step Recording is in progress on two separate calls, the system does not allow the user to conference the two calls together.

- Coverage Answer Group

  An answer group contains up to eight members who act as a coverage point for another user. For example, if several attendants are responsible to answer redirected calls from a department, assign all attendants to an answer group. The administrator assigns a group number to the answer group. That group number appears in the coverage path of that department. All telephones in an answer group ring simultaneously. Any member of the group can answer the call.

  When a member of a Coverage Answer Group answers a call, any of the parties on the call can press the **audix-rec** button to record the conversation. The system stores the recorded message in the voice mailbox of the party who answers the call.

- Drop Last

  After CM Messaging starts to record, the initiator becomes the control party. If the initiator presses the **Drop** button, AUDIX One-Step Recording stops and the LED goes out. If other parties on the call press the **Drop** button, the system denies the request.

- Group Paging that uses a speakerphone

  With Group Paging, users can make an announcement over a group of digital speakerphones. Neither the group members who receive a page, nor the originator of the page, can use AUDIX One-Step Recording to record the conversation. If anyone on the call presses the **audix-rec** button, the system ignores the request. The LED flutters.

- Hunt Group

  If a member of a hunt group answers a call, the parties on the call can use AUDIX One-Step Recording to record the conversation. The system stores the recorded message in the voice mailbox of the party who answers the call.

- Hunt Group queueing

  Users cannot activate AUDIX One-Step Recording when the following conditions apply.

  - The queue is enabled for the CM Messaging hunt group
  - All the CM Messaging ports are busy

- Meet-me Conference

  Parties on a Meet-me Conference can use AUDIX One-Step Recording. Conference parties can selectively use the Display and Drop feature to drop the AUDIX One-Step Recording hunt group extension from the call. The LED goes out.

- Mode Code interface

  Voice mail connections through the Mode Code interface rely on digits that are sent over analog ports. The AUDIX One-Step Recording feature does not work with a Mode Code connection.

- Terminating Extension Group (TEG)

  Neither group members who receive TEG calls, nor the originators of TEG calls, can use AUDIX One-Step Recording to record the conversation. If anyone on the call presses the **audix-rec** button, the system denies the request. The LED flutters.

- Transfer

  When the recording request is in process, the LED is flashing. If anyone attempts to transfer the call to another party, AUDIX One-Step Recording stops. The LED goes out.

  When the recording starts, the LED is on but not flashing. Any party on the call can transfer the call to another party.

  - If the initiator transfers the call, recording automatically stops after the transfer.
  - If another party on the call transfers the call, recording continues.

  If AUDIX One-Step Recording is in progress on two separate calls, the system does not allow a user to transfer one call to the other.

- Vector Directory Number (VDN)

  When a call is answered through a VDN, any of the parties on the call can press the **audix-rec** button to record the conversation.

- Whisper Page

  With Whisper Page, no parties on the call can use AUDIX One-Step Recording to record the conversation. If anyone on the call presses the **audix-rec** button, the system denies the request. The LED flutters.

Troubleshooting AUDIX One-Step Recording

This section lists the known or common problems that users might experience with the AUDIX One-Step Recording feature.

Problem	Possible cause	Action
The user does not have the **audix-rec** button on the telephone.	The **audix-rec** button is not assigned to the telephone of the user.	Use the **`change station`** ***`n`*** command, where ***`n`*** is the extension of the telephone, to add the **audix-rec** button.
	The telephone of the user does not support buttons that can be administered.	This user cannot access the AUDIX One-Step Recording feature.
The user hears a beep every few seconds during recording.	The alerting tone interval is set too low.	Set the alerting tone interval to a number that is between 15 and 60.

Problem	Possible cause	Action
Nothing happens when the user presses the **audix-rec** button. The button light flutters.	The user was not on an active call.	Inform the user that the **audix-rec** button only works if the user is on an active call.
	The connection to CM Messaging is not operating.	Ensure that CM Messaging is operating correctly. If not, the user must wait for the system to reestablish the connection.
	The LAN connection between the CM Messaging server and the Communication Manager server is not operating.	Ensure that CM Messaging is operating correctly. If not, the user must wait for the system to reestablish the connection.
	All the CM Messaging ports are busy.	The user must wait for a CM Messaging port to be released.
	Another person on the call is already using the AUDIX One-Step Recording feature to record the conversation.	The user cannot record the conversation if someone else on the call is already using this feature.
	The user attempted to start the AUDIX One-Step Recording feature from a bridged call appearance.	The user cannot record the conversation from a bridged call appearance.
	Remote CM Messaging is configured for Communication Manager Release 1.3.	• Move the voice mail service of the user to a local CM Messaging, or • Upgrade the user to Communication Manager Release 2.0 or later.
The user does not hear a beep during recording.	The ready indication tone is set to play to only the initiator, or to no one.	Set the ready indication tone to **all**.
	The alerting tone interval is set to zero.	Set the alerting tone interval to a number between 15 and 60.
	The zip tone is set to **silence** instead of to a frequency and duration.	Reset the characteristics of the zip tone.
After the green LED is steady and the recording starts, the user hears a CM Messaging announcement.	If configured with CM Messaging, ARIA TUI might be turned on. The Recording Delay Timer is not set high enough.	Set the Recording Delay Timer to a higher number.

Authorization Codes

Use the Authorization Codes feature to control the calling privileges of system users. Authorization codes extend control of calling privileges and enhance security for remote access callers. To maintain system security, Avaya recommends that you use authorization codes.

You can use authorization codes to:

- Override a facilities restriction level (FRL) that is assigned to an originating station or trunk
- Restrict individual incoming tie trunks and remote access trunks from accessing outgoing trunks
- Track Call Detail Recording (CDR) calls for cost allocation
- Provide additional security control

Detailed description of Authorization Codes

When you dial an authorization code, the Facilities Restriction Level (FRL) that is assigned to the extension, the attendant console, the incoming trunk group, or the remote access trunk group that is in use for the call is replaced by the FRL assigned to the authorization code. The FRL that is assigned to the authorization code functions in the same way as the original FRL. However, the new FRL that is assigned to the authorization code might represent greater or lesser calling privileges than the original FRL. Access to any given facility depends on the restrictions that are associated with the FRL of the authorization code.

The following example shows how authorization codes work with FRLs.

A supervisor is at a desk of an employee. The supervisor wants to make a call that is usually not allowed by the FRL that is assigned to the extension of that employee. The supervisor, however, can still make the call if the supervisor dials an authorization code that is assigned an FRL. The FRL must be an FRL for the type of call that is allowed.

Length of authorization codes

For security reasons, authorization codes must consist of 4 to 13 digits. The number of digits in the codes must be a fixed length for a particular server that is running Communication Manager.

Once established, the number of digits (4 to 13) in the authorization code remains fixed unless all codes are removed and reentered. All authorization codes that are used in the system must be the same length.

Using authorization codes

You can administer incoming trunk groups within a system to always require an authorization code. The system applies recall dial tone to a call when the user must dial an authorization code. If the user dials a correct authorization code within 10 seconds (interdigit timeout), the system completes the call as dialed. If the user does not dial an authorization code, or dials an incorrect authorization code, the system routes to the call to an attendant. The system can also route the call to an intercept tone based on how the system was administered.

Usually, Direct Inward Dialing (DID) trunks do not require authorization codes. However, you can administer DID trunks to require an authorization code, but you must do this carefully. Different types of calls can terminate at different endpoints, and requiring an authorization code can be confuse the user.

You can also administer a Cancellation of Authorization Code Request (CACR) digit. The CACR digit cancels the 10-second interval between dialing. When the user dials the CACR digit, the system immediately routes the call according to system administration. Incoming trunk calls receive intercept tone or go to the attendant. Other calls receive intercept tone unless the user's FRL is high enough to route the call. A CACR digit from an off-premises extension over DID and Tie trunks use DID and Tie trunk intercept treatment. Internal calls receive intercept tone.

You must not program passwords or authorization codes onto auto dial buttons. Because display telephones display the programmed buttons, the potential exists for an unauthorized person to use the autodial buttons. If you must program passwords or authorization codes onto auto dial buttons, use the ~s (suppress) character to prevent displaying the codes.

AAR and ARS calls

Each authorization code is assigned a Class of Restriction (COR) that contains an associated FRL. Within a system, the FRL that is assigned to the point at which the call originates determines the access privileges that are associated with the call. When an AAR or an ARS call is dialed, the system allows or denies the call, based on the FRL of the originating station. You use COR to restrict internal or non-AAR or an ARS calls.

You can assign authorization codes to individual users to specify the level of calling privileges. Such codes work regardless of the originating facility. Once an authorization code is required and dialed on an AAR or an ARS call, the FRL assigned to the authorization code replaces the originating FRL. This new FRL controls and defines the privileges of the user.

An AAR call or an ARS call that a system user originates, or routes over an incoming tie trunk can require a dialed authorization code to continue routing.

When you administer authorization codes, ensure that the user does not have to dial the authorization code more than once. For example, if a user makes an AAR call or an ARS call, and the FRL of the user is not high enough to access any of the trunks in the routing pattern, the system prompts the user for an authorization code. If the FRL that is assigned to the authorization code is high enough to access the next trunk group in the routing pattern, the user is not prompted to dial the code again. If the system routes the call through another system, the user might be required to dial an authorization code again. This type of situation can be avoided through careful administration.

An authorization code might be required on some, but not all, trunk groups. In such cases, the system prompts for an authorization code when the originating FRL is not high enough to access the next available trunk group in the routing pattern.

Administering Authorization Codes

The following steps are part of the administration process for the Authorization Codes feature:

- Setting up Authorization Codes
- Creating Authorization Codes with a specific Class of Restriction

This section describes:

- Any prerequisites for administering the Authorization Codes feature
- The screens that you use to administer the Authorization Codes feature
- Complete administration procedures for the Authorization Codes feature

Prerequisites for administering Authorization Codes

You must complete the following actions before you can administer authorization codes:

- On the Optional Features screen, ensure that the **Authorization Codes** field is set to **y**. If the **Authorization Code** field is set to **n**, your system is not enabled for the Authorization Codes feature. Contact your Avaya representative for assistance.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Authorization Codes

Screen name	Purpose	Fields
Optional Features	Ensure that the Authorization Codes feature is enabled on the system.	**Authorization Code**
Feature-Related System Parameters	Enable the Authorization Codes feature, and set up other fields to administer the feature.	• **Authorization Code Enabled** • **Authorization Code Length** • **Display Authorization Code**
Authorization Codes - COR Mapping	Create an Authorization Code that has a specific COR.	• **AC** • **COR**
Trunk Groups	Allow the use of Authorization Code to access trunks.	• **Auth Code**

Setting up Authorization Codes

To set up authorization codes:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen (Figure 65: Feature-Related System Parameters screen on page 327).

Figure 65: Feature-Related System Parameters screen

```
change system-parameters features                              Page 3 of 8

                     FEATURE-RELATED SYSTEM PARAMETERS

                      Reserved Slots for Attendant Priority Queue: 5_
                                       Time Before Off-Hook Alert: 10__
                            Emergency Access Redirection Extension: _____
             Number of Emergency Calls Allowed in Attendant Queue: __
                                          Call Pickup Alerting? n
                       Temporary Bridged Appearance on Call Pickup? y
                                    Call Pickup on Intercom Calls? y
                                          Directed Call Pickup? n
                  Deluxe Paging and Call Park Timeout to Originator? n
Controlled Outward Toll Restriction Intercept Treatment: tone _______
    Controlled Termination Restriction (Do Not Disturb): tone _______
              Controlled Station to Station Restriction: tone _______
AUTHORIZATION CODE PARAMETERS           Authorization Code Enabled? y
                                         Authorization Code Length: 7
                               Authorization Code Cancellation Symbol? #
                                           Attendant Time Out Flag? n
                                       Display Authorization Code? _
                     Controlled Toll Restriction Replaces: station-station
          Controlled Toll Restriction Intercept Treatment: extension     3000
```

2. In the **Authorization Code Enabled** field, type **y** to enable the Authorization Codes feature on a system-wide basis.
3. In the **Authorization Code Length** field, type the number of digits that you want for the authorization code.

   This field defines the length of the Authorization Codes your users need to enter. To maximize the security of your system, Avaya recommends you make each authorization code the maximum length that the system allows.In the example shown, the authorization code has 7 digits. Avaya recommends that authorization codes must have at least 4 digits, but no more than 13.
4. In the **Authorization Code Cancellation Symbol** field, leave the default of the pound sign (**#**).

   Users must dial this symbol to cancel the 10-second wait period during which your user can enter an authorization code.
5. In the **Attendant Time Out Flag** field, leave the default of **n**.

   When you set this field to **n**, the system does not route a call to the attendant if a user does not dial an authorization code within 10 seconds, or a user dials an invalid authorization code.

6. In the **Display Authorization Code** field, type **n**.

   When you set this field to set to **n**, the authorization code does not display on the phone sets thus maximizing security.

7. Press **Enter** to save your changes.

8. Type **change authorization-code *n***, where ***n*** is the authorization code. Press **Enter**.

   The system displays the Authorization Code - COR Mapping screen (Figure 66: Authorization Code - COR Mapping screen on page 328).

Figure 66: Authorization Code - COR Mapping screen

```
change authorization-code 4285193                                Page 1 of 1

                    Authorization Code - COR Mapping

      Note: 1  codes administered. Use 'list' to display all codes.

      AC       COR        AC       COR        AC       COR        AC       COR
4285193        1    _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
_____________ ___  _____________ ___  _____________ ___  _____________ ___
```

9. In the **AC** field, type the authorization code that your users must dial.

   The number of digits in the code that you type must be the same as the number you assigned in the Feature-Related System Parameters screen in Step 3. In this example, the authorization code is **4285193**.

10. In the **COR** field, type a COR number from 0 through 95.

    In this example, the COR number is **1**.

11. Press **Enter** to save your changes.

Creating Authorization Codes with a specific Class of Restriction

You can use authorization codes that allow a callers to override the calling privileges. For example, you can give a supervisor an authorization code so that they can make calls from a telephone that is usually restricted for these calls. Since each authorization code has a Class of Restriction (COR), the system uses the COR that is assigned to the authorization code, and the FRL assigned to the COR to override the privileges associated with the restricted phone.

Authorization codes do not override dialed strings that are denied. For example, if your Automatic Route Selection (ARS) tables restrict users from placing calls to destinations that are outside of the country, a caller cannot override the restriction with an authorization code.

To create an authorization code with a specific COR:

1. Type **change authorization-code *n***, where ***n*** is the authorization code. Press **Enter**.

   The system displays the Authorization Code - COR Mapping screen (Figure 67: Authorization Code - COR Mapping screen on page 329).

Figure 67: Authorization Code - COR Mapping screen

```
change authorization-code 4285193                                Page 1 of 1

                    Authorization Code - COR Mapping

      Note: 2  codes administered. Use 'list' to display all codes.

      AC       COR        AC       COR        AC       COR        AC       COR
9260839        3     _____________ ___  _____________ ___  _____________ ___
2754609        4     _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
_____________ ___    _____________ ___  _____________ ___  _____________ ___
```

2. In the **AC** field, type the code that you want to use.
3. In the **COR** field, type the COR number.
4. Press **Enter** to save your changes.

Considerations for Authorization Codes

This section provides information about how the Authorization Codes feature behaves in certain circumstances. Use this information to ensure that you receive maximum benefits of the Authorization Codes feature under all conditions:

- From remote locations users usually access authorization from touch-tone telephones. However, users can also do so from rotary telephones at specified authorization-code-forced locations that follow appropriate trunk administration practices. Rotary station users access attendants using Listed Directory Numbers (LDN) or Remote Access Numbers (RAN), and can experience a 10-second timeout.
- The use of Authorization Codes does not limit other call-control methods, such as Toll Restriction, Miscellaneous Trunk Restriction, and Outward Restriction.
- For security reasons, do not assign authorization codes in sequential order. Assign random number barrier codes and authorization codes to users. Random codes prevent hackers from deciphering the sequential codes.
- If timeout to attendant does not occur or a Cancellation of Authorization Code Request (CACR) digit codes are dialed instead of authorization codes, the system assumes that invalid authorization codes were dialed and the caller hears intercept tones.
- Authorization codes can have an impact calling privileges. Authorization codes can:
  - Change the FRL of an outgoing call when the FRL is not high enough to access preferred that AAR/ARS assigns. An FRL is assigned to a COR that is associated with user authorization codes. No additional COR data is assigned.
  - Overrides COR for remote access calls that are assigned to barrier codes, when required. if an authorization code is required for remote access calls, the user is assigned the COR of the dialed authorization code, with all connected data, such as the FRL. This COR overrides the COR that is assigned to any required barrier code.
- Incoming trunk calls that require authorization codes do not change user privileges.

Interactions for Authorization Codes

This section provides information about how the Authorization Codes feature interacts with other features on the system. Use this information to ensure that you receive maximum benefits of the Authorization Codes feature in any feature configuration:

- AAR/ARS Partitioning

  Class of Restriction (COR) assigns partitioned group numbers and authorization codes can change CORs. Therefore, authorization codes can change Partitioned Group Numbers on incoming remote access calls. For originating calls, the COR of the user determines Partitioned Group Numbers.

- Cancellation of Authorization Code Request

If	Then
CACR =1	• Authorization = 1
Network = DEFG1, DEFG3 or DEF ECSR5	• CACR can be #
Network - S85s, DIM switch	• CACR = 1 (default)

- COR and Facilities Restriction Level (FRL)

  Authorization codes used for AAR or ARS calls override the associated FRL.

  Associated Classes of Restriction determine remote-access user privileges.

- Forced Entry of Account Codes and Call Detail Recording

  For 94A LSU and 3B2 CDRU 18-word records, authorization codes are output if administered account-code lengths are fewer than six digits. For 59-character records, authorization codes are never recorded.Note that 94A LSU and 3B2 CDRU are no longer supported.

  Authorization codes are recorded after destination addresses are dialed. Invalidly dialed authorization codes are recorded, and CDR printouts can be used to determine patterns.

Automated Attendant

Use the Automated Attendant feature to allow callers to dial an extension without the need for an attendant to connect the call.

Detailed description of Automated Attendant

This section provides a detailed description of the Automated Attendant feature.

A caller dials any extension on the system. The Automated Attendant feature uses vectors to route the call to that extension. This feature reduces the need for live attendants, which can help to reduce costs.

The Automated Attendant feature works together with the Attendant Vectoring feature. For more information, see the "Attendant Vectoring" feature. For more information about vectors and vector directory numbers (VDNs), see the "Meet-Me Conference" feature.

The *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference* contains a detailed description of Automated Attendant, and how to use the Automated Attendant feature. The guide also gives a sample vector that you can use for Automated Attendant.

Administering Automated Attendant

The following steps are part of the administration process for the Automated Attendant feature:

- Setting the prompting timeout
- Administering a vector directory number
- Administering announcements
- Controlling hunt groups by vector
- Assigning a caller information button on a multiappearance telephone
- Assigning a caller information button on a multiappearance telephone
- Assigning a caller information button on an attendant console

This section describes:

- Any prerequisites for administering the Automated Attendant feature

- The screens that you use to administer the Automated Attendant feature
- Complete administration procedures for the Automated Attendant feature

Prerequisites for administering Automated Attendant

You must complete the following actions before you can administer the Automated Attendant feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*.
- On the Optional Features screen, ensure that the **Vectoring (Prompting)** field is set to **y**. If the **Vectoring (Prompting)** field is set to **n**, your system is not set up for the Automated Attendant feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Automated Attendant

Screen name	Purpose	Fields
Optional Feature	Ensure that the Automated Attendant feature is activated.	**Vectoring (Prompting)**
Feature-Related System Parameters	Set the prompting timeout period.	**Prompting Timeout**
Vector Directory Number	Assign a VDN to an extension.	All
Announcements/Audio Sources	Complete all fields for each extension that provides an Automated Attendant announcement.	All
Hunt Group	Indicate that the system controls hunt groups with vectors.	**Vector**
Call Vector	Complete a Call Vector screen for each Automated Attendant vector.	All

Screen name	Purpose	Fields
Station	Assign a **callr-info** display button for multiappearance telephones.	Any blank field in either the **Button Assignments** area or the **Feature Button Assignments** area
Attendant Console	Assign a **callr-info** display button for attendant consoles.	Any blank field in the **Feature Button Assignments** area

Setting the prompting timeout

To set the prompting timeout:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Vectoring** area (Figure 68: Feature-Related System Parameters screen on page 335).

Figure 68: Feature-Related System Parameters screen

```
change system-parameters features                                Page 7 of 8

                          CALL CENTER SYSTEM PARAMETERS

EAS
        Expert Agent Selection (EAS) Enabled? n
       Minimum Agent-LoginID Password Length:
         Direct Agent Announcement Extension: _____              Delay: ___
   Message Waiting Lamp Indicates Status For: station

VECTORING
                   Converse First Data Delay: 0       Second Data Delay: 2
              Converse Signaling Tone (msec): 100          Pause (msec): 70_
                    Prompting Timeout (secs): 10
                Interflow-qpos EWT Threshold: 2

SERVICE OBSERVING
              Service Observing Warning Tone? n

ASAI
 Call Classification After Answer Supervision? n      Send UCID to ASAI? n
```

3. In the **Prompting Timeout (sec)** field, type the number of seconds before the **collect digits** command times out for callers who use rotary dialing. This value must be a number from 4 to 10. The default is 10.

   The **Prompting Timeout (sec)** field appears only if the **Vectoring (Prompting)** field on the Optional Features screen is set to **y**.

4. Press **Enter** to save your changes.

Administering a vector directory number

To administer a vector directory number (VDN), see the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*.

See also the Attendant Vectoring feature.

Administering announcements

To administer announcements for the Automated Attendant, see the Announcements feature.

Controlling hunt groups by vector

To control hunt groups by vector:

1. Type **change hunt-group *n***, where ***n*** is the number of the hunt group that you want to control by vector. Press **Enter**.

   The system displays the Hunt Group screen (Figure 69: Hunt Group screen on page 337).

Figure 69: Hunt Group screen

```
change hunt-group 12345                                      Page 1 of 3

                                    HUNT GROUP

           Group Number: ___                                      ACD? n
             Group Name: _____________________________          Queue? y
        Group Extension: ____                                   Vector? y
             Group Type:
                     TN:
                    COR:                                 MM Early Answer?
          Security Code: ____
       ISDN Caller Disp: ________

           Queue Length: ___
Calls Warning Threshold: ___   Port: x      Extension: ____
 Time Warning Threshold: ___   Port: x      Extension: ____
```

2. In the **Vector** field, type **y** to indicate that this hunt group is vector controlled.

   You can change the **Vector** field to **y** only if the **Vectoring (Basic)** field on the Optional Features screen is set to **y**. For more information on setting up hunt groups, see the "Hunt Group" feature.

3. Press **Enter** to save your changes.

Assigning a caller information button on a multiappearance telephone

You can administer any multiappearance display telephone to have a caller information (**callr-info**) button. This button displays digits that were collected for the last **`collect digits`** command.

To assign a **callr-info** button on a multiappearance telephone:

1. Type **`change station n`**, where ***n*** is the extension of the telephone that you want to change. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 70: Station screen on page 338).

   If all the buttons are assigned in this area, click **Next** until you see The **Feature Button Assignments** area.

Figure 70: Station screen

```
change station 60006                                          Page 3 of 5
                                      STATION
     SITE DATA
          Room: _______                                  Headset? n
          Jack: ___                                      Speaker? n
         Cable: ___                                     Mounting: d
         Floor: _______                             Cord Length: 0_
      Building: _______                               Set Color: _____


ABBREVIATED DIALING
     List1: ________          List2: _________          List3: _________

BUTTON ASSIGNMENTS
 1: call-appr                          4: cpn-blk
 2: call-appr                          5: cpn-unblk
 3: call-appr                          6: callr-info
```

3. In the **Button Assignments** area or in the **Feature Button Assignments** area, assign **callr-info** to an available button.

   In this example, we assign **callr-info** to button 6 in the **Button Assignments** area.

4. Press **Enter** to save your changes.

Assigning a caller information button on an attendant console

You can administer an attendant console to have a caller information (**callr-info**) button. This button displays digits that were collected for the last **`collect digits`** command.

To assign a **callr-info** button on an attendant console:

1. Type **`change attendant`** ***`n`***, where ***`n`*** is the number of the attendant console to which you want to assign a **callr-info** button. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 71: Attendant Console screen on page 339).

Figure 71: Attendant Console screen

```
change attendant 1                                          Page 3 of 4
                              ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split_____                          13: callr-info
  2: dont-split                          14: __________
  3: act-tr-grp                          15: __________
  4: deact-tr-g                          16: __________
  5: __________                          17: __________
  6: hold _____ *                        18: __________
  7: __________                          19: forced-rel
  8: aux-work      RC:    Grp:           20: __________
  9: __________                          21: __________
 10: __________                          22: __________
 11: __________                          23: night-serv *
 12: __________                          24: pos-busy__ *
```

3. In the **Feature Button Assignments** area, assign **callr-info** to an available button.

   In this example, we assign **callr-info** to button 13.

4. Press **Enter** to save your changes.

Considerations for Automated Attendant

This section provides information about how the Automated Attendant feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Automated Attendant under all conditions. The following considerations apply to Automated Attendant:

- Automated Attendant competes with several features for ports on the call classifier - detector circuit pack or an equivalent circuit pack.

Interactions for Automated Attendant

This section provides information about how the Automated Attendant feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Automated Attendant in any feature configuration.

- CM Messaging

  Automated Attendant gives the caller the option to leave a message or wait in a queue for an attendant.

- Authorization Codes

  The system does not prompt for an authorization code, and the **route-to** command fails if:

  — Authorization codes are enabled

  — A **route-to** command in a prompting vector accesses either Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS)

  — The Facility Restriction Level (FRL) of the vector directory number (VDN) does not have the permission to use the chosen routing preference

- CallVisor Adjunct-Switch Application Interface (ASAI)

  The Call Vectoring feature can collect ASAI-provided digits through the **collect vector** command as dial-ahead digits. The system passes CINFO to CallVisor ASAI.

- Hold

  If a call is put on hold during the processing of a collect command, the command restarts at the announcement prompt when the call is taken off hold. All dialed-ahead digits are lost. Similarly, if a call to a vector is put on hold, vector processing is suspended when a collect command is encountered. When the call becomes active, the collect command resumes.

- Inbound Call Management (ICM)

  You can use Automated Attendant to collect information that an adjunct might later use to handle a call.

- Transfer

  If a call to a VDN is transferred during a collect command, the collect command restarts when the transfer is complete. All dialed-ahead digits are lost. Similarly, if a call to a vector is transferred, vector processing is suspended when a collect command is encountered. When the transfer is complete, the collect command resumes. Attendant-extended calls suspend vector processing in the same way as transferred calls.

Automatic Callback

Use the Automatic Callback (ACB) feature to allow internal users who place a call to a busy or an unanswered internal telephone to be called back when the called telephone becomes available. When a user activates Automatic Callback, the system monitors the called telephone. When the called telephone becomes available to receive a call, the system automatically originates the Automatic Callback call. The originating party receives priority ringing. The calling party then lifts the handset, and the called party receives the same ringing that the system provided on the original call.

When you place a call from an analog telephone, and the line is busy, an announcement prompts you to either:

- Enter the digit 1 to activate Automatic Callback.
- Enter the digit 2 to route the call to a hunt group extension.

Important:
Use the Automatic Callback and Ringback Queuing features to allow internal users who place a call to a busy or unanswered destination to be called back when the destination becomes available. Automatic Callback applies to stations, Ringback Queuing provides the same function for calls directed to a busy trunk group.

Detailed description of Automatic Callback

With the Automatic Callback feature, when a caller places a call to a busy or an unanswered internal telephone, the system calls the caller back when the called telephone becomes available. Upon hearing a busy signal, a user activates Automatic Callback, and hangs up. The system monitors the called telephone. When the called telephone becomes available to receive a call, the system automatically originates the Automatic Callback call. The originating party receives priority ringing. The calling party then lifts the handset, and the called party receives the same ringing that the system provided on the original call.

To activate this feature, the user of a single-line telephone presses the Recall button, or flashes the switchhook. The user then dials the Automatic Callback Feature Access Code (FAC). A single-line user can activate Automatic Callback for only one call at a time.

The number of calls for which a user of a multiappearance telephone can activate Automatic Callback depends on the number of Automatic Callback buttons that you assign to the telephone. After the user places a call to a telephone that is busy or unanswered, the user presses an idle Automatic Callback button, and hangs up.

If the original caller answers an Automatic Callback call, and for some reason the called extension cannot accept the Automatic Callback call, the caller hears a confirmation tone and then silence. The call is still queued.

Users cannot activate Automatic Callback for calls to:

- A telephone that is assigned Termination Restriction
- An extension toward which Automatic Callback is already activated
- A data terminal or a data module
- An attendant console group
- A Terminating Extension Group (TEG)
- An extension for a hunt group, a split, or a skill
- The login ID of an EAS agent
- A Vector Directory Number (VDN) extension

Automatic Callback supports the following capabilities:

- Ringback Queuing
- Called Party Queuing
- Analog Busy Automatic Callback Without Flash
- QSIG Call Completion - Administrable TSC Signaling Connection
- ISDN CCBS Supplementary Service on Busy
- CCBS for Incoming Calls

Ringback Queuing

You can administer your system to call users back if users try to place an outgoing call over a trunk group when all trunks are busy. Ringback Queuing places outgoing calls in an ordered queue (first-in, first-out) when all trunks are busy. The system automatically places the callback call to the telephone when a trunk becomes available, and the user hears a distinctive three-burst signal, which indicates an Automatic Callback call from the system. When the user answers the callback call, the original call automatically continues. Redialing is not required. Ringback queuing is also called Automatic Callback for busy trunks.

If a user with a multiappearance telephone has an idle Automatic Callback button and tries to access an all-trunks-busy trunk group, the call queues automatically. The lamp that is associated with the Automatic Callback button lights, and the user hears a confirmation tone.

Ringback Queuing is automatic for a single-line telephone. After dialing is complete, the user hears a confirmation tone if the queue is available. No action is required. The system queues as many calls as are allowed, based on the value in the **Queue Length** field on the Trunk Group screen. The system checks the busy or idle status of the trunk group only once. If all trunks are busy, the call queues, even if a trunk has become available by the time that the caller finishes dialing. In this case, a caller might be called back immediately after the caller receives a confirmation tone and hangs up.

You can specify queuing for any outgoing-only trunk group that is not part of a distributed communications system (DCS), or for the outward direction of a non-DCS two-way trunk group.

Called Party Queuing

In Communication Manager Release 5.2, Automatic Callback is enhanced to allow queuing of called parties. This feature works on analog, DCP, IP (H.323) and IP (SIP) telephones. In Communication Manager Release 5.2, Automatic Callback allows:

- Multiple active callbacks for an extension, subject to the limitation on the total number of callbacks within the system
- Callbacks for softphones, provided the softphone has at least one bridged call appearance on a physical station

A called telephone can have multiple active automatic callbacks. The callbacks are processed in the order in which they were activated.

If a calling station uses multiple call appearances, the number of automatic callbacks depends on the number of Automatic Callback buttons assigned to the station.

Automatic Callback works the same way as it does on a local server, on the following networks:

- On a Distributed Communication Server (DCS) network, Automatic Callback (ACB) requests from or to a station located on a different Communication Manager are queued and processed.
- If your public service network provider supports ISDN Call Completion Busy Subscriber (CCBS), the CCBS requests are queued and processed.
- On a QSIG network, ACB requests from or to a station located on a different Communication Manager are queued.

Analog Busy Automatic Callback Without Flash

With Analog Busy Automatic Callback Without Flash, callers who place a call from an analog station to a station that is busy and has no coverage path or forwarding, hear an announcement and are presented with options. Depending on the selection that the caller makes, the call is queued to Automatic Callback, routed to an extension, or dropped. No switchhook flash is required for Analog Busy Automatic Callback.

QSIG Call Completion - Administrable TSC Signaling Connection

This capability covers auto callback within a private corporate network only, for example, through QSIG. Communication Manager Release 4.0 or later provides an administrable option on the Trunk Group screen to allow users to specify the method of signaling connection the system uses while waiting for a busy station to become idle.

The **TSC Method for Auto Callback** field on the QSIG Trunk Group Options page of the Trunk Group screen allows customers to administer whether or not to retain the Temporary Signaling Connection (TSC) when QSIG Call Completion (QSIG-CC) is activated with other Communication Manager servers, or with non-CM servers (like the I55 or Siemens Hicom). The default value for the **TSC Method for Auto Callback** is **drop-if-possible**. The other option is to set the value to **always-retain**.

Older QSIG-CC standards require Path Reservation, which is not supported by Communication Manager. QSIG-CC can fail if the QSIG TSC is dropped when connected to a server that does not support the latest version of the QSIG-CC standards. In order for Communication Manager to work with servers based on old QSIG-CC standards, this retaining option is needed.

Currently, the preferred QSIG-CC signaling connection method used by Communication Manager is the signaling connection release. In other words, Communication Manager populates the element *retain-sig-connection* in CCBS/CCNR invoke APDUs with the hard-coded value FALSE.
With Communication Manager 4.0 or later, the new administration option on the Trunk Group screen controls:

- the element *retain-sig-connection* in CCBS/CCNR invoke APDUs, when CM is the originating PINX
- the signaling connection method for the QSIG-TSC when CM is the terminating or the outgoing gateway PINX

For more information, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

ISDN CCBS Supplementary Service on Busy

In EMEA, the public network service providers support the ISDN Call Completion Busy Subscriber (CCBS) capabilities where the service provider allows automatic callback for a busy subscriber. By implementing ISDN CCBS Supplementary Services, Communication Manager Release 5.0 enables automatic callback to the public network.

Note:
The CCBS feature is not supported by all service providers.
The Call Completion on No Reply (CCNR) feature is defined by the ETSI standards. But the CCNR feature is not supported by Communication Manager, or by service providers for new customers.

The following settings must be administered to use this feature:

1. On the ISDN Trunk Group screen, set **Supplementary Service Protocol** to option **c** (which is usually already set for ETSI public network trunks).
2. Also on the ISDN Trunk Group screen, set **NCA-TSC Trunk Member** to the trunk member whose D-channel will be used to route the ETSI CCBS request.
3. To enable ETSI for BRI, you must set the **Interface** column to **user** or **network** to enable option **c** (stated in step 1) in the **TSC SS Protocol** column on the BRI-Trunk-Board screen. Also, the maximum number for the **NCA-TSC** field has to be a value > 0.
4. For PRI, you must set the **TSC Supplementary Service Protocol** field on the Signaling Group screen to **c** to enable ETSI.
   Also, the maximum number of **NCA-TSC** field on the Signaling Group screen has to be set to a value > 0.

For more information, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

CCBS for Incoming Calls

The Call Completion to Busy Subscriber (CCBS) feature is based on the existing auto callback and supplementary service - completion of calls (QSIG SS-CC) features. It provides the auto callback functionality to be used on calls to or from the public network. The server informs the caller as soon as the busy subscriber becomes available.

This feature supports the following:

- ETSI-TSC (Temporary Signaling Connection) for incoming calls. In Communication Manager Release 5.0 and earlier releases, TSC is available for ETSI only for outgoing calls. TSC is currently available in both directions for QSIG.
- ETSI-CCBS for incoming calls. In Communication Manager Release 5.0 and earlier releases, CCBS is only fully available for internal users and for users on systems interconnected by DCS, QSIG, or SIP trunks. On the ETSI interface, CCBS is supported for outgoing calls only. Starting with Communication Manager Release 5.1, CCBS on the ETSI interface is fully available in both directions (incoming and outgoing).

Restriction: ETSI-TSC and ETSI-CCBS are implemented without gateway functionality (ETSI - QSIG/DCS/SIP).

The supplementary service Completion of Calls has been added as new ETSI ISDN functionality. This feature is supported only in countries where the ETSI ISDN protocol is supported.

This feature must be supported by the service provider. Some service providers offer Call Completion without any additional charge, but you need to apply for it.

Completion of Calls is known as "Auto callback" at the user side.

CCBS Call Flow Scenarios

As an analog voice terminal user, you can activate supplementary service - Call Completion to Busy Subscriber (SS-CCBS) by pressing the Recall button or flashing the switch hook, then dialing the Automatic Callback Activation Feature Access Code. You can activate only one Automatic Callback call at any given time.

As a multi-appearance voice terminal user, you can activate SS-CCBS for the number of Automatic Callback buttons assigned to the terminal. After placing a call to a voice terminal over the DSS1 network that is busy, you can activate SS-CCBS by pressing an idle Automatic Callback button.

In the above two scenarios, the called station is located in the public network. The public network access must be located in the same switch as the station.

When you request a CCBS supplementary service it remains active until the Call Completion is performed or until the Service Duration timer expires. The default for the timer is set to 40 minutes. The terminal must be located in the same switch as the public network access.

When SS-CCBS is activated towards the busy station on the terminate side (public network or PBX), the terminating side monitors the called voice terminal. When the called voice terminal becomes available to receive a call, the terminating side notifies the originating side of the possibility of executing a Call Completion call attempt. The originating side then originates the Call Completion call.

A busy voice terminal becomes available when the user hangs up after completing the current call.

A SS-CCBS request is canceled for any of the following user-related reasons:

- The Call Completion call is successful.
- The called party at the terminating PBX does not become available within 40 minutes.
- The called party is busy again.

CCBS Routing issue

CCBS requests using the ETSI ISDN network require a special view to the routing in Communication Manager. It may be necessary to add an additional routing entry to allow an incoming ETSI CCBS request to reach the dedicated station.

In an incoming ETSI basic call, the called number is always supplied by the network provider. With CCBS, the called number is supplied by the requesting user. If the requesting user encodes the number in a different way than the network provider does, CCBS will fail. In this case, an additional routing entry is necessary to allow the ETSI CCBS request to reach the called number.

For example, station 7001 has a PBX access code of 53608. The national destination code (also known as the city code) is 211.

On an incoming basic call, the called number may be presented as 536087001. In this example, the call can be routed to the dedicated station because 53608 is configured in the ars digit-conversion table.

In an incoming ETSI CCBS request, the called number may be presented as 211563087001. Keep in mind this number is provided by the requesting user, not by the network provider. The CCBS request will fail if only 53608 is entered in the ars digit-conversion table. To make CCBS work, the digit sequence 21153608 must be added to the ars digit-conversion table.

Figure 72 shows the entries for this example:

Figure 72: ars digit-conversion table

```
display ars digit-conversion 0                                  Page 1 of 2
                      ARS DIGIT CONVERSION TABLE
                                Location: all                 Percent Full: 0

  Matching Pattern    Min   Max   Del   Replacement String   Net    Conv ANI Req

  53608               5      9    5                          ext    n        n
  21153608            8     12    8                          ext    n        n
```

Administering Automatic Callback

The following steps are part of the administration process for the Automatic Callback feature:

- Assigning a FAC for Automatic Callback
- Enabling Automatic Callback With Called Party Queuing
- Setting the no-answer timeout interval
- Assigning a feature button for Automatic Callback
- Setting the queue length for Ringback Queuing
- Enabling CCBS

This section describes:

- Any prerequisites for administering the Automatic Callback feature
- The screens that you use to administer the Automatic Callback feature
- Complete administration procedures for the Automatic Callback feature

Screens for administering Automatic Callback

Screen name	Purpose	Fields
Feature Access Code (FAC)	Assign a Feature Access Code (FAC) with which to activate or deactivate Automatic Callback.	**Automatic Callback Activation/ Deactivation**
Feature-Related System Parameters	Set the number of times that the callback call rings at the calling station before the system cancels the callback call.	**Automatic Callback With Called Party Queuing-No Answer Timeout Interval**
Station (multiappearance)	Assign a feature button for the Automatic Callback feature.	**Buttons/Feature Button Assignments - auto-cback**
Trunk Group	Set the queue length for Ringback Queuing.	**Queue Length**
	Enable CCBS	**Supplementary Service Protocol** **NCA-TSC Trunk Member**

Assigning a FAC for Automatic Callback

To assign a Feature Access Code (FAC) for Automatic Callback:

1. Type **`change feature-access codes`**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen (Figure 73: Feature Access Code (FAC) screen on page 349).

Figure 73: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 1 of 7
                                FEATURE ACCESS CODE (FAC)
            Abbreviated Dialing List1 Access Code: ____
            Abbreviated Dialing List2 Access Code: ____
            Abbreviated Dialing List3 Access Code: ____
   Abbreviated Dial - Prgm Group List Access Code: ____
                        Announcement Access Code: ____
                         Answer Back Access Code: ____
                           Attendant Access Code: ____
       Auto Alternate Routing (AAR) Access Code: ____
        Auto Route Selection (ARS) Access Code1: ____  Access Code 2: ____
                  Automatic Callback Activation: ____   Deactivation: ____
   Call Forwarding Activation Busy/DA: ____   All: ____   Deactivation: ____
                           Call Park Access Code: ____
                         Call Pickup Access Code: ____
   CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                     CDR Account Code Access Code: ____
                           Change COR Access Code: ____
                      Change Coverage Access Code: ____

                     Data Origination Access Code: ____
                         Data Privacy Access Code: ____
                 Directed Call Pickup Access Code: ____
```

2. In the **Automatic Callback Activation** field, type the digits of the access code that you want to use to activate the Automatic Callback feature.
3. In the **Deactivation** field, type the digits of the access code that you want to use to deactivate the Automatic Callback feature.
4. Press **Enter** to save your changes.

Enabling Automatic Callback With Called Party Queuing

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the **Feature-Related System Parameters** screen.
2. Set **Automatic Callback With Called Party Queuing** to **y**.

   (Figure 74: Feature-Related System Parameters screen)
3. Press **Enter** to save your changes.

Setting the no-answer timeout interval

You can administer the number of times that the callback call rings at the calling station before the callback call is canceled.

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen (Figure 74: Feature-Related System Parameters screen).

Figure 74: Feature-Related System Parameters screen

```
change system-parameters features                          Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: none
              Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: none
             Music (or Silence) on Transferred Trunk Calls? no
                      DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? y
    ACA Referral Calls: local      ACA Referral Destination:
               ACA Short Holding Time Originating Extension:
               ACA Long  Holding Time Originating Extension:
Treat ISDN Call to Busy User as ACA Short Holding Time Call? n
             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

2. In the **Automatic Callback - No Answer Timeout Interval (rings)** field, enter the number of times that you want a callback call to ring at the calling station before the callback call is canceled. In this example the number of rings is set to 3.
3. Press **Enter** to save your changes.

Assigning a feature button for Automatic Callback

To assign one or more feature buttons for Automatic Callback:

1. Type **change station *n***, where ***n*** is the extension of the station for which you want to assign a feature button. If you are adding a new station, type **add station next**.

   The system displays the Station screen (Figure 75: Station screen on page 351).

Figure 75: Station screen

```
add station 1014                                          Page 3 of X
                                   STATION

     SITE DATA
          Room: _______                                  Headset? n
          Jack: ___                                      Speaker? n
         Cable: ___                                     Mounting: d
         Floor: _______                              Cord Length: 0_
      Building: _______                                Set Color: _____


ABBREVIATED DIALING
     List1: ________           List2: _________          List3: _________

BUTTON ASSIGNMENTS
 1: call-appr                5:
 2: call-appr                6:
 3: call-appr                7:
 4: auto-cback               8:
```

2. In the **Button Assignments** area, type **auto-cback** in a blank field.
3. Repeat Step 2 for as many buttons as you want to assign for Automatic Callback.
4. Press **Enter** to save your changes.

Setting the queue length for Ringback Queuing

To set the queue length for Ringback Queuing:

1. Type **change trunk-group *n***, where ***n*** is the number of an existing trunk group for which you want to set the queue length. If you are adding a new trunk group, type **add trunk-group next**.

   The system displays the Trunk Group screen.

2. In the **Queue Length** field, type the number of outgoing calls that you want to be held waiting when all trunks are busy.
3. Press **Enter** to save your changes.

Enabling CCBS

To enable a trunk to support Completion of Calls, set the **Supplementary Service Protocol** field on Page 2 of the **Trunk Group** screen to **c**.
(Figure 76: Supplementary Service Protocol field).

Also, set the **NCA-TSC Trunk Member** field on Page 3 of the **Trunk Group** screen.
(Figure 77: Trunk Group screen (page 3)).

Figure 76: Supplementary Service Protocol field

```
Group Type: ISDN                                              Page 2 of x

TRUNK PARAMETERS
        Codeset to Send Display:  6      Codeset to Send National IEs:  6
      Max Message Size to Send:  260     Charge Advice: automatic
 Supplementary Service Protocol:  c      Digit Handling (in/out): overlap/overlap

           Trunk Hunt: cyclical
                                                   Digital Loss Group: 13

 Incoming Calling Number - Delete:        Insert:       Format:
            Bit Rate: 1200               Synchronication: async   Duplex: full
 Disconnect Supervision - In? y Out? n
 Answer Supervision Timeout: 0
                                     CONNECT Reliable When Call Leaves ISDN? n
```

Figure 77: Trunk Group screen (page 3)

```
add trunk-group next                                          Page 3 of x
                              TRUNK FEATURES
           ACA Assignment? _          Measured: ____     Wideband Support? _
 Long Holding Time(hours): _                            Maintenance Tests? _
  Short Holding Time(sec): _  Data Restriction? _     NCA-TSC Trunk Member: _
  Short Holding Threshold: __        Send Name: _     Send Calling Number: _
             Used for DCS? _                          Send EMU Visitor CPN?

Suppress # Outpulsing? _  Numbering Format: _______
Outgoing Channel ID Encoding: _________     UUI IE Treatment: _______
                                       Maximum Size of UUI IE Contents: ___
                                             Replace Restricted Numbers? _
                                           Replace Unavailable Numbers? _
                                                Send Connected Number: _
                                             Hold/Unhold Notifications? _

        Send UUI IE? _
          Send UCID? _                BRS Reply-best DISC Cause Value: __
                                                Ds1 Echo Cancellation? _

                                       US NI Delayed Calling Name Update? _
Show ANSWERED BY on Display? y
                           Network (Japan) Needs Connect Before Disconnect? _
```

Considerations for Automatic Callback

This section provides information about how the Automatic Callback feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Automatic Callback under all conditions. The following considerations apply to Automatic Callback:

- The system cancels an Automatic Callback request if the:
  - Called party is unavailable within 30 minutes.
  - Calling party does not answer the callback call within the administered interval. This interval consists of two to nine ringing cycles, and is set in the **Automatic Callback-No Answer Timeout Interval** field on the Feature-Related System Parameters screen.
  - Calling party decides not to wait, and presses the same Automatic Callback button a second time on a multiappearance telephone, or dials the Automatic Callback cancellation code on a single-line telephone.

- Automatic Callback is administered for individual telephones by Class of Service (COS), and cannot be assigned to attendants. Multiappearance telephones must have an Automatic Callback button to activate the feature.
- Automatic Callback works differently, depending on whether the called party is busy or does not answer the call. For a busy call, Automatic Callback occurs as soon as the called party hangs up. For an unanswered call, the telephone must be used for another call, and then hung up before Automatic Callback occurs.

  Note:
  If the user who originates an Automatic Callback originator has all line appearances occupied when the Automatic Callback call comes in, the user hears priority ringing once, and the Automatic Callback lamp blinks. However, if the user presses the Automatic Callback button to answer the Automatic Callback call, the system drops one of the other calls.
- Queuing can reduce the number of trunks that are required.
- On a multiappearance telephone, one callback call can be associated with each Automatic Callback button that is assigned to the terminal.
- On a single-line telephone, only one Automatic Callback call can wait at a time.
- Queue requests are canceled when:
  - A trunk is unavailable within 30 minutes.
  - The user does not answer the callback call within the administered interval.
  - The telephone is busy when the callback call is attempted.
  - The user dials the Ringback Queuing cancellation code, or presses the Automatic Callback button that is associated with the queued call.
- Incoming tie-trunk calls cannot queue on an outgoing trunk group. The system does not know the calling number, and cannot originate the callback call.
- The system checks the busy or idle status of the trunk group only once. If all trunks are busy, the call queues, even if a trunk becomes available by the time that the caller finishes dialing. In this case, a caller might be called back immediately after the caller receives a confirmation tone and hangs up.
- A trunk might appear to be available, yet outgoing calls are queued. The trunk is not free, because the trunk is reserved for a previous Automatic Callback request.
- The Automatic Callback feature works correctly even if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.

Interactions for Automatic Callback

This section provides information about how the Automatic Callback feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Automatic Callback in any feature configuration.

- Attendant Call Waiting and Call Waiting Termination

  If a user activates Automatic Callback to or from a single-line telephone, Call Waiting Termination is denied.

- Attendant Intrusion

  Attendant Intrusion does not work if a user has activated Automatic Callback.

- Automatic Route Selection (ARS)

  If a user with a multiappearance telephone that has an Automatic Callback button makes an ARS call, and all trunks are busy, the system activates Ringback Queuing automatically.

- Bridged Call Appearance

  Users cannot activate Automatic Callback from a bridged call appearance. If a user activates Automatic Callback from a primary extension number, the return-call notification rings at all bridged call appearances.

- Busy Verification

  If a user has activated Automatic Callback on a telephone, you cannot perform Busy Verification of that telephone.

- Call Coverage

  If the calling station has Call Coverage active, the callback terminates at the called station and does not follow the coverage path.

- Call Forwarding

  If the calling party has activated Call Forwarding on a telephone, the calling party is able to activate Automatic Callback. If the called party activates Call Forwarding on a telephone before the caller trying to use Automatic Callback, the calling party is not able to activate Automatic Callback. Also, if Automatic Callback was activated before the called telephone user activated Call Forwarding, the system redirects the callback call attempt toward the callback party, not to the forwarded-to party.

  - If the calling station has Call Forwarding active, the callback is forwarded *only* if the forwarded station is local to the calling station. You cannot activate Automatic Callback if the forwarded station is remote to the calling station.
  - If a forwarded station that has active automatic callback has any activity going on, callback is not generated till one of the following conditions is met:
    - the forwarded station goes on hook

    - the forwarding is removed and the user goes on and off hook
  - Automatic callback cannot be activated if the called party is forwarded to a station that is forwarded to another station.
- Call Pickup

  A group member cannot answer a callback call for another group member.
- Class of Restriction (COR)

  Telephones with origination restriction cannot activate Automatic Callback.
- Conference and Transfer

  A user of a single-line telephone can activate conference or transfer if Automatic Callback is activated.
- Distributed Communication System (DCS)

  Automatic Callback operates over a DCS network in the same way that Automatic Callback operates on a local server.
- Expert Agent Selection (EAS)

  Users cannot activate Automatic Callback to the login ID of an EAS agent. Users can activate Automatic Callback to the telephone where the agent is logged in.
- Hold

  A user of a single-line telephone cannot receive Automatic Callback calls if the user has placed a call on hold.
- Hot Line Service

  Telephones that are administered for Hot Line Service cannot activate Automatic Callback.
- Intercom - Automatic and Dial

  Intercom calls are not eligible for Automatic Callback.
- Internal Automatic Answer (IAA)

  IAA does not automatically answer Automatic Callback calls.
- Manual Originating Line Service

  Telephones with Manual Originating Line Service cannot activate Automatic Callback.
- Personal Station Access

  You cannot activate automatic callback to a disassociated PSA extension unless that extension is bridged to another physical station. If callback was activated before the disassociation, the callback remains in queue till the activation timer expires or the callback is explicitly canceled.

  You cannot activate automatic callback from a disassociated PSA extension.

- Public Network Trunks: Automatic Callback works on outgoing public network trunks in some countries. The call must be dialed using AAR, ARS, or UDP. Automatic Callback cannot be activated on a public network trunk call if the call was dialed using a Trunk Access Code (TAC).
- QSIG: Automatic Callback operates over a QSIG network in the same way as on a local server. The call must be dialed using AAR, ARS, or UDP. Automatic Callback cannot be activated on a QSIG call if the call was dialed using a Trunk Access Code (TAC).
- Remote Access

  Callback calls cannot be made to Remote Access users, because the system does not know the calling number.
- Ringback Queuing

  Users can press an Automatic Callback button to activate Ringback Queuing.
- Send All Calls

  You cannot activate automatic callback on a station that uses the Send All Calls redirection option.
- Telephone Display

  When the system generates an Automatic Callback call, the display of the originating telephone displays Automatic Callback, or the equivalent translated phrase for Administrable Language Displays.

Automatic Circuit Assurance

Use the Automatic Circuit Assurance (ACA) feature to identify possible trunk malfunctions. When you enable ACA, the system measures the holding time of each trunk call. If the measurements show calls with either extremely long or extremely short holding times, Communication Manager places a referral call to an attendant or a telephone.

Detailed description of Automatic Circuit Assurance

This section provides a detailed description of the Automatic Circuit Assurance feature (ACA).

The system records the holding time from when a trunk is accessed to when the trunk is released. You set short and long holding-time limits for each trunk group. The system then compares the recorded holding times against these limits.

You enable ACA for the entire system, and administer thresholds for individual trunk groups. You can measure all trunks, or only certain trunks.

Communication Manager deals with long-holding and short-holding calls differently. For every call that is shorter than the administered short holding time, the system increases the short-holding counter by one. For calls over the same trunk that are within the normal range, the system decreases the short holding counter by one. Thus, trunks that handle a normal variety of call lengths are not singled out as faulty. If the counter reaches the administered short holding limit, the system places a referral call.

If one long call exceeds the long holding time, the system makes a referral call.

You cannot measure personal central office (CO) lines, out-of-service trunks, or trunks that are undergoing maintenance testing.

The referral call

An ACA call includes a display message or a voice-synthesized message that states:

- That this call is an ACA call
- The access code, the trunk group number, and the trunk group member number
- The type of referral, either short holding time or long holding time

If the referral call is answered, the system displays this information until the call is released. If the call is unanswered within 3 minutes, the system ends the call. The system places the call again after one hour, and continues to place the call hourly until someone answers.

The attendant or the telephone user who receives the referral call can press the **aca-halt** button to stop further calls. The **aca-halt** button is a toggle button, and turns off the ACA feature until the user presses the button again.

The audit trail

When the system makes a referral call, the system also adds a record to an audit trail. Audit trail records are available on the ACA Measurements Report. Each record contains the:

- Time and the date of referral
- Trunk group number, the trunk access code, and the trunk group member
- Type of referral, either short holding time or long holding time

Administering Automatic Circuit Assurance

This section describes the screens required to administer the Automatic Circuit Assurance feature.

Screens for administering Automatic Circuit Assurance

Screen name	Purpose	Fields
Feature-Related System Parameters	Enable the ACA feature.	• **Automatic Circuit Assurance Enabled** • **ACA Referral Calls** • **ACA Referral Destination** • **ACA Short Holding Time Originating Extension** • **ACA Long Holding Time Originating Extension**
Trunk Features	Set assignments and thresholds.	• **ACA Assignment** • **Short Holding Threshold** • **Long Holding Time (hours)** • **Short Holding Time (seconds)**

Screen name	Purpose	Fields
Attendant Console	Set the **aca-halt** feature button.	Any available button in the **Feature Button** area
Station	Set the **aca-halt** feature button.	Any available button in the **Feature Button** area

Reports for Automatic Circuit Assurance

The following reports provide information about the Automatic Circuit Assurance (ACA) feature:

- The ACA Measurements Report shows the audit trail for ACA calls.

For detailed information on these reports and the associated commands, see *Avaya Aura™ Communication Manager Reports*.

Considerations for Automatic Circuit Assurance

This section provides information about how the Automatic Circuit Assurance (ACA) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Automatic Circuit Assurance under all conditions. The following considerations apply to Automatic Circuit Assurance:

- None

Interactions for Automatic Circuit Assurance

This section provides information about how the Automatic Circuit Assurance feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Automatic Circuit Assurance in any feature configuration.

- Administrable Language Displays

  You cannot administer languages for ACA messages.

- CM Messaging

  Do not set the referral-call extension to a telephone that covers to a CM Messaging voice messaging system. You can overload CM Messaging with the volume of calls, because ACA calls remain active for up to three minutes.

- Busy Verification

  Once you identify a potentially defective trunk, you can use Busy Verification to check that trunk.

- Centralized Attendant Services (CAS)

  When CAS is activated, the referral-call destination must be on the local switch. The system interprets a referral destination of 0 as the local attendant, if a local attendant exists. The CAS attendant cannot activate or deactivate ACA referral calls at a branch location.

- Distributed Communications System (DCS)

  Referral calls can be placed across a DCS network. The primary switch is administered to receive ACA referred calls from remote nodes for all switches within the network. You must administer the **ACA Remote PBX Identification** field on the Feature-Related System Parameters screen with the PBX ID of the node that is designated as primary.

  If ACA referral calls are sent off the switch that generates the referral, the display and voicing information that indicates the failed trunk is lost, even if the referral call is made over a DCS network.

- Night Service

  The system does not place referral calls to the attendant if the system is in Night Service mode.

- Visually Impaired Attendant Service (VIAS)

  If the attendant presses the Display Status button and an ACA call has not been answered, the words "Automatic Circuit Assurance" are voiced.

  If a visually-impaired attendant presses the Display Status button and the ACA call has been answered, the words Automatic Circuit Assurance and the extension that is assigned to the ACA call are voiced.

  If the switch contains a voice-synthesis board, ACA referral calls are also accompanied by an audible message that identifies the type of ACA infraction encountered. The message is "Automatic circuit assurance <long> or <short> holding time threshold has been exceeded for trunk group <#> member number <#>."

- Voice Message Retrieval

  If you use Voice Message Retrieval, you can assign a nondisplay telephone as a referral destination.

- Wideband Switching

  ACA treats wideband-trunk calls as a single-trunk call, and therefore triggers a single referral call. The call information shows the lowest B-channel trunk member that is associated with the wideband channel.

Automatic Number Identification

Use the Automatic Number Identification (ANI) feature to display telephone number of the calling party on your display telephone. The system uses ANI to interpret calling party information that is signaled over multifrequency (MF) or Session Initiation Protocol (SIP) trunks.

Detailed description of Automatic Number Identification

This section provides a detailed description of the Automatic Number Identification (ANI) feature.

ANI displays calling party information on your display telephone that is signaled over MF or SIP trunks.

- For a description about calling party information that is signaled over ISDN or H.323 trunks to your display telephone, see the "Caller ID" feature.
- For a description about calling party information that is signaled over Centralized Automatic Message Accounting (CAMA) trunks to your local emergency rapid response organization, see the "E911" feature.

Incoming Automatic Number Identification

Use inband signaling for information, such as the address digits for the called party, that is delivered over the same trunk circuit that is used for the voice or data connection. Use out-of-band or ISDN signaling when signaling information passes through a different signaling path than the path that is used for the voice or data connection.

For example, when a call is made from 555-3800 to your display telephone at extension 81120, and the **Incoming Tone (DTMF) ANI** field is set to ***ANI*DNIS*** on the Trunk Group screen, your trunk group receives *5553800*81120*. If the same field is set to **ANI*DNIS***, your trunk group receives 5553800*81120*. In both cases, *call from 555-3800* appears on your telephone display.

If you do not use inband ANI, the incoming trunk group name appears on your telephone display.

Outgoing Automatic Number Identification

Outgoing ANI applies to outgoing Russian MF ANI, R2-MFC ANI, China #1 MF ANI, and Spain Multi Frequency España (MFE) ANI trunks only.

Use Outgoing ANI to specify the type of ANI to send on outgoing calls. You can define MF ANI (the calling party number, sent through multifrequency signaling trunks) prefixes by COR. This allows a system to send different ANIs to different central offices (COs).

For a tandem call that uses different types of incoming and outgoing trunks, the server uses:

- The COR-assigned call type of the incoming trunk for Russian or R2-MFC outgoing trunks
- Automatic Route Selection (ARS) call types for MFE outgoing trunks

Administering Automatic Number Identification

The following steps are part of the administration process for the Automatic Number Identification (ANI) feature:

- Setting up ANI on a multifrequency trunk
- Displaying incoming ANI calling party information
- Setting up outgoing ANI
- Setting up an ANI request button

This section describes:

- Any prerequisites for administering the Automatic Number Identification (ANI) feature
- The screens that you use to administer the Automatic Number Identification (ANI) feature
- Complete administration procedures for the Automatic Number Identification (ANI) feature

Prerequisites for Automatic Number Identification

You must complete the following actions before you can administer the Automatic Number Identification (ANI) feature:

- None

Screens for administering Automatic Number Identification

Screen name	Purpose	Fields
Multifrequency-Signaling-Related Parameters	Set up ANI on an MF trunk.	• **Incoming Dial Type** • **Incoming Tone (DTMF) ANI**
Trunk Group	Set up incoming ANI so that the system displays the calling party information from either an MF or a SIP trunk.	• **Incoming Dial Type** • **Incoming Tone (DTMF) ANI**
• AAR Digit Analysis Table • ARS Digit Analysis Table • AAR Digit Conversion Table • ARE Digit Conversion Table	Set up outgoing ANI for Russian MF ANI, R2-MFC ANI, China #1 MF ANI, and Spain Multi Frequency España (MFE) ANI trunks.	• **ANI Reqd** • ANI Req
Station	Assign an **ani-requst** button to the telephone of a user.	Any available button field in the **Button Assignments** area.

Setting up ANI on a multifrequency trunk

An ANI request button on the telephone of a user allows the user to display the telephone number of the calling party during the voice state of the call. The trunk must support this functionality.

To set up ANI for multifrequency signaling:

1. Type **`change multifrequency-signaling n`**, where ***n*** is a number between 1 and 8. Press **Enter**.

   The system displays the Multifrequency-Signaling-Related Parameters screen (Figure 78: Multifrequency-Signaling-Related Parameters screen on page 368).

Note:

The number of pages and the fields on the screen that the system displays is based on the value in the **Outgoing Call Type** field.

– If the value in the **Outgoing Call Type** field is **group-ii-mfc**, the system displays four pages. The system also displays the **ANI Prefix**, **Default ANI**, **Next ANI Digit Incoming**, and **Next ANI Digit Outgoing** fields.

- If the value in the **Outgoing Call Type** field is **mfe**, the system displays two pages. The system also displays the **ANI Prefix**, and **Default ANI** fields.
- If the value in the **Outgoing Call Type** field is **none**, the system displays three pages. The system also displays the **Next ANI Digit Incoming** field.

Figure 78: Multifrequency-Signaling-Related Parameters screen

```
change multifrequency-signaling 1                              Page  1 of  X

            MULTIFREQUENCY-SIGNALING-RELATED SYSTEM PARAMETERS 1

         Incoming Call Type:                        ANI Prefix:
         Outgoing Call Type:                      Default ANI:
      Maintenance Call Type:            NEXT ANI DIGIT
                                                      Incoming:
    Maximum Resend Requests:                          Outgoing:
  Received Signal Gain (dB):
Transmitted Signal Gain (dB):

                         Request Incoming ANI (non-AAR/ARS)?
                   Outgoing Forward Signal Present Timer (sec):
                    Outgoing Forward Signal Absent Timer (sec):
MF Signaling Intercept Treatment - Incoming? _  Outgoing: ____________ _____
                             Collect All Digits Before Seizure?
                  Overlap Sending on Link-to-Link Tandem Calls?
          Private Group II Permissions and Public Interworking?
                             Convert First Digit End-of-ANI To: _
                            Use COR for All Group II Responses? _
                                Group II Called Party Category:
                            Use COR for Calling Party Category?
```

For a thorough description of the Multifrequency-Signaling-Related Parameters screen and the values for the fields see the *Administering Avaya Aura™ Communication Manager*, 03-300509.

2. When you are finished, press **Enter** to save your changes.

Displaying incoming ANI calling party information

A display telephone might display either the telephone number and name of the calling party, or the incoming trunk group name. You set the **ANI** field on the Trunk Group screen.

To display ANI calling party information on a trunk:

1. Type **`change trunk group n`**, where ***n*** is the number of the trunk that you want to change. Press **Enter**.

   The system displays the Trunk Group screen.

2. Click **Next** until you see the **Incoming Dial Type** field.
3. In the **Incoming Dial Type** field, type **tone**.
4. Click **Next** until you see the **Incoming Tone (DTMF) ANI** field.
5. In the **Incoming Tone (DTMF) ANI** field, type ***ANI*DNIS**.

Note:
The **Incoming Tone (DTMF) ANI** field only appears if the **Incoming Dial Type** field on the previous page is set to **tone**.

6. Press **Enter** to save your changes.

Setting up outgoing ANI

Prerequisites

You must complete the following actions before you can set up ANI for outgoing calls:

1. View the Feature-Related System Parameters screen.

   To view the Feature-Related System Parameters screen, type **`change system-parameters features`**. Press **Enter**.
2. Click **Next** until you see the **Allow ANI Restriction on AAR/ARS** field.
3. Ensure that the **Allow ANI Restriction on AAR/ARS** field is set to **y**.
4. Press **Enter** to save your changes.

To set up ANI for outgoing calls:

1. Type **`change aar analysis`**. Press **Enter**.

   The system displays the AAR Digit Analysis Table screen (Figure 79: AAR Digit Analysis Table screen on page 370).

Note:
The system uses AAR routing information to route calls within your company over your own private network. The software converts the number that the user dials. The software then analyzes the number, and routes the call as a private-network call.

Figure 79: AAR Digit Analysis Table screen

```
change aar analysis                                          Page 1 of X

                          AAR DIGIT ANALYSIS TABLE
                                                  Percent Full:  ___

     Dialed          Total    Route    Call   Node  ANI
     String        Min Max  Pattern   Type   Num   Reqd
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
_________________  __  __   _____    ____   ___    n
```

2. For each appropriate dialed string on your plan, set the **ANI Reqd** field as follows:

ANI Reqd

The following are the valid entries and usage for the **ANI Reqd** field:

1. Press **Enter** to save your changes.

   If necessary, repeat steps 1 through 3 for the ARS Digit Analysis Table screen.

2. To view the ARS Digit Analysis Table screen, type **`change ars analysis`**. Press **Enter**.

Note:

The system uses ARS routing information to route calls that go outside your company over public networks. The system also uses ARS routing information to route calls to remote company locations if you do not have a private network. The software converts the number that the user dials. The software then analyzes the number, and routes the call as a public network call.

If necessary, repeat steps 1 through 3 for the AAR Digit Conversion Table screen, and the ARS Digit Conversion Table screen.

3. To view the AAR Digit Conversion Table screen, type **change aar digit-conversion**. To view the ARS Digit Conversion Table screen, type **change ars digit-conversion**. Press **Enter**.

Valid entries	Usage
y/n	Enter **y** if ANI is required on incoming R2-MFC or Russian MF ANI calls. This field applies only if the **Request Incoming ANI (non-AAR/ARS)** field on the Multifrequency-Signaling-Related System Parameters screen is **n**.
r	This value is allowed only if the **Allow ANI Restriction on AAR/ARS** field on the Feature Related System Parameters screen is **y**. The system uses this value to drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails. Other types of trunks treat **r** as **y**.

Setting up an ANI request button

An ANI request button on the telephone of a user allows the user to display the telephone number of the calling party during the voice state of the call. The trunk must support this functionality.

To set up an ANI request button on the telephone of a user:

1. Type **change station *n***, where ***n*** is the extension that you want to change. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 80: Station screen on page 372).

Figure 80: Station screen

```
change station 10                                          Page 3 of 4

                                  STATION

SITE DATA
      Room:                                          Headset? n
      Jack:                                          Speaker? n
     Cable:                                         Mounting: d
     Floor:                                     Cord Length: 0
  Building:                                       Set Color:



ABBREVIATED DIALING
     List1:               List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          5:
 2: call-appr                          6:
 3. call-appr                          7:
 4. ani-requst                         8:
```

3. In an available button field, type **ani-requst**.
4. Press **Enter** to save your changes.
5. Notify the user of the button assignment.

Reports for Automatic Number Identification

The following reports provide information about the Automatic Number Identification (ANI) feature:

- None

Considerations for Automatic Number Identification

This section provides information about how the Automatic Number Identification (ANI) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of ANI under all conditions. The following considerations apply to ANI:

- None

Interactions for Automatic Number Identification

This section provides information about how the Automatic Number Identification (ANI) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of ANI in any feature configuration.

- Attendant Console

  If an attendant extends a call, the attendant's Class of Restriction (COR) is used to select the ANI prefix.

- Authorization Codes

  The authorization code COR is used to select the ANI prefix. The extension's ANI is used if an extension originates the call. The ANI for the server is used if the originating endpoint is an incoming MF or SIP trunk.

- Bridged Call Appearance

  A call from a bridged call appearance uses the ANI of the primary extension.

- Call Vectoring

  The ANI of the originating party is used, not the ANI of the call vector, when a call vectoring route-to command routes a call over an outgoing trunk.

- Distributed Communications System (DCS)

  In a DCS, the ANI that is sent to the CO is determined by the **ANI for PBX** field, but the category sent to the CO is determined by the **Category for MF ANI** field on the Class of Restriction screen for the incoming DCS trunk or by the type of call.

- Expert Agent Selection (EAS)

  The EAS agent's login extension and COR is used to determine the ANI prefix.

- Hunt Groups and Automatic Call Distribution (ACD) Splits

  The phone's extension and the COR is used to determine the ANI prefix for a hunt group or ACD split.

- Multimedia Call Handling (MMCH)

  For call origination, multimedia complexes use the COR assigned to their phones.

- Remote Access

  A remote access barrier code COR is not used for ANI. The extension's ANI is used if an extension originates the call. The ANI for the server is used if the originating endpoint is an incoming trunk.

- Separation of Bearer and Signaling

  The Separation of Bearer and Signaling feature can provide ANI while the media stream is going over a type of trunk that cannot provide ANI.

Avaya Video Telephony Solution

Use the Avaya Video Telephony Solution to enable videoconferencing for your desktop and group video communications.

Detailed description of Avaya Video Telephony Solution

The Avaya Video Telephony Solution enables Communication Manager to merge a set of enterprise features with Polycom's videoconferencing adjuncts. It unifies Voice over IP with video, Web applications, Avaya's video enabled IP softphone, third-party gatekeepers, and other H.323 endpoints.

The following components are part of the Avaya Video Telephony Solution feature:

- Polycom VSX3000, VSX7000 and VSX8000 conferencing systems with Release 8.03 or later
- Polycom V500 video calling systems
- Polycom RMX 2000 video bridge is supported beginning with Communication Manager Release 4.1. For more specific information on the RMX 2000 product, see: http://www.polycom.com/usa/en/products/products.html
- Polycom MGC video conferencing bridge platforms with Release 8.0.1 are supported, but with some limitations. Release 7.5 of the MGC is not supported.
- Third-party gatekeepers, including Polycom Path Navigator

You also need a system running Communication Manager Release 3.1.3, and Avaya IP Softphone Release 5.2 with video integrator.

For more information, see also:

Avaya Video Telephony Solution Release 4.0 Networking Guide, 16-601423, Issue 3
Video Telephony Solution Release 4.0 Quick Setup, 16-300310, Issue 4
IP Softphone and Video Integrator Getting Started, 16-600748, Issue 3

Note:
To configure the Polycom MGC-25 Video Conferencing Bridge Platforms with Avaya S8300, S8500 and S87xx Servers, see the procedures stated in the *Video Telephone Solution R4.0 Quick Set Up Guide, 16-300310, Issue 4.*

The following table shows the compatible Polycom and Tandberg products that you can use with Communication Manager as part of the Avaya Video Telephony feature:

Vendor	Product	Version	Communication Manager version	
			4.0.3+	5.0 SP3+
Avaya	Avaya IP Video Softphone	R6 SP4+ [1]	Yes	Yes
	C-LAN	FW26+ [2]	Yes	Yes
	Meeting Exchange	5.0.2.00(4.13.0.2)	No	Yes
Polycom	PathNavigator	7.00.08.0407+ [6]	Yes	Yes
	SE200	3.00.02.ER019+ [6]	Yes	Yes
	iPower	6.0.0.315+	Limited [3, 4]	Limited [3, 4]
	ViewStationFX	V6.0.5+	Limited [3, 4]	Limited [3, 4]
	ViewStation	V7.5.4+	Limited [3]	Limited [3]
	VSX/V500	8.7.1	Yes	Yes
		9.0+	Yes	Yes
	MGC	8.0.0.27	Yes	Yes
		9.0.1.8+	Yes	Yes
	RMX	2.0.2.25+		Yes
	HDX	2.0.2-2461+	Yes [5]	Yes
	RSS2000		No	No
Tandberg	T150	L5.0 [7]	Yes	Yes

Key:

Blank=Unverified; Yes=Verified; No=Does not work; +=Later firmware

Notes:

1. IPSP R6 video not backward compatible with CM3.1.2 and earlier
2. C-LAN FW11 has known issues with VSX registration.
3. Telephony features and IPSP video mute are not supported.
4. Internal MCU calls from an iPower to an IPSP, or Communication Manager connected VSX do not connect.
5. CM4.0.1 SP1 required for HD video.
6. Inter-gatekeeper call rate management will require CM4.0.4 or CM5.1.1 SP1 minimum.

7. Until L5.2 is available, T150 requires a dedicated ip-network-region with IP-IP Direct Audio set to no.

Bridged Call Appearance

Use the Bridged Call Appearance feature to give single-line and multiappearance telephones an appearance of another telephone number. With Bridged Call Appearance, the user can originate, answer, and bridge onto calls to or from the telephone number of another user.

The terms "primary number," "primary telephone," and "primary station" all mean the same thing. The primary number is the extension that you want other extensions to bridge onto. For example, if you want extension A as the primary number to also have call appearances on extensions B, C, and D, the administrator must access extensions B, C, and D using the Station screen, and bridge each extension to extension A.

The Bridged Call Appearance feature works on the following telephones:

- Single-line telephone

  A single-line telephone can be the primary number, meaning that it can have a bridged appearance on another telephone. A single-line telephone can also have a bridged appearance of either another single-line telephone or a multiappearance telephone.

- Multiappearance telephone

  A multiappearance telephone can be the primary number, meaning that it can have a bridged appearance on another telephone. A multiappearance telephone can have a bridged appearance of a single-line telephone or one or more appearances of a multiappearance telephone. A multiappearance telephone can also have bridged appearances of multiple telephone numbers.

Detailed description of Bridged Call Appearance

The primary number of a telephone is the extension assigned when the telephone is administered. The primary number appears in the **Extension** field on the Station screen. On a multiappearance telephone, multiple appearances of this primary number can exist.

A Bridged Call Appearance is an appearance of a primary number on a different telephone. In most ways, the bridged call appearance acts like the primary number appearance. For example, when someone calls the primary number, you can answer that number at the primary telephone or at all bridged appearances of that number. When a call is received, the primary number and all bridged appearances alert visually, with audible ringing as an administrable option. Likewise, a call that is placed from a bridged call appearance carries the display information and the Class of Restriction (COR) of the primary number.

You can use a bridged call appearance like a primary call appearance for most features. For example, Conference, Transfer, Hold, Drop, and Priority Calling from a bridged appearance, just as from a primary call appearance.

Sample uses

The following list describes some situations in which you might want to use bridged call appearances:

- A secretary making or answering calls on the primary number of an executive

  These calls can be placed on hold for later retrieval by the executive, or the executive can bridge onto the call. In all cases, the executive handles the call as if he or she had placed or answered the call. It is never necessary to transfer the call to the executive.

- For visitor telephones

  An executive can have another telephone in their office for use by visitors. It might be desirable that the visitor can bridge onto a call that is active on the executive's primary number. A bridged call appearance makes this possible.

- In service environments

  It might be necessary that several people be able to handle calls to a particular extension. For example, several users might be required to answer calls to a hot line number in addition to their normal functions. Each user might also be required to bridge onto existing hot line calls. A bridged call appearance provides this capability.

- For a user who frequently uses telephones that are in different locations

  A user might not spend all of their working hours in the same place. For this type of user, it is convenient to have their extension bridged at several different telephones.

Administrable buttons and lamps for multiappearance telephones

You can administer the message lamp and some feature buttons to apply to the primary number rather than to the number of the telephone they reside on.

- You can administer the message lamp to light on the bridged user's telephone when messages are waiting for the primary telephone.
- You can administer the call forwarding all calls and call forwarding busy/don't answer buttons to activate Call Forwarding for any extension that is on the telephone, even if this extension is a bridged appearance. In addition, you can administer the lamp associated with the call forwarding button to track the call forwarding status of any extension. Thus, a bridged user can activate or deactivate Call Forwarding from the telephone with the bridged call appearance for all primary and bridged appearances of the extension. The bridged appearance telephone shows the call forwarding status of the specified extension.

- You can administer the send all calls button to activate Send All Calls for any administered extension. The lamp associated with Send All Calls tracks the status of the administered extension. Thus, a bridged user can activate Send All Calls for the primary extension user.

Administering Bridged Call Appearance

The following steps are part of the administration process for the Bridged Call Appearance feature:

- Creating a bridged call appearance on a single-line telephone
- Creating a bridged call appearance on a multiappearance telephone

This section describes:

- Any prerequisites for administering the Bridged Call Appearance feature
- The screens that you use to administer the Bridged Call Appearance feature
- Complete administration procedures for the Bridged Call Appearance feature

Prerequisites for administering Bridged Call Appearance

You must complete the following actions before you can administer the Bridged Call Appearance feature:

- If Data Privacy for data or voice calls is administered, you can prohibit bridging onto voice or data calls with Data Privacy. To prohibit bridging onto Data Privacy calls, type **y** in the **Prohibit Bridging Onto Calls with Data Privacy** field on the Feature-Related System Parameters screen.

  To view the Feature-Related System Parameters screen, type **`display system-parameters features`**. Press **Enter**.

- For each coverage path that includes a telephone with bridged appearances you must administer whether you want a call to skip a coverage point if that telephone has already alerted as a bridged appearance. Enter **n** to skip the coverage point in the **Terminate to Coverage Pts. with Bridged Appearance?** field on the Coverage Path screen. Enter **y** to alert both a bridged call and a redirected call.

  To view the Coverage Path screen, type **`change coverage path n`**, where ***n*** is the number of the coverage path you want to change. Press **Enter**.

Screens for administering Bridged Call Appearance

Screen name	Purpose	Fields
Feature-Related System Parameters	Ensure data privacy.	**Prohibit Bridging Onto Calls with Data Privacy**
Coverage Path	Skip a coverage point.	**Terminate to Coverage Pts. with Bridged Appearance**
Station	Create a bridged call appearance on a single-line telephone	• **Bridged Call Alerting** • **Line Appearance** • **Btn** • **Ext**
	Create a bridged call appearance on a multiappearance telephone	• **Per Button Ring Control** • **Bridged Call Alerting** • **Bridged Idle LIne Appearance** • **Auto Select Any Idle Appearance** • **Button Assignments** • **Btn** • **Ext** • **Ring**

Creating a bridged call appearance on a single-line telephone

To create a bridged call appearance on a single-line (analog) telephone:

1. Type **`change station`** ***`n`***, where ***`n`*** is the extension of the single-line (analog) telephone on which you want to create the bridged call appearance. Press **Enter**.

   The system displays the Station screen for a single-line telephone.

2. Click **Next** until you see the **Bridged Call Alerting?** field (Figure 81: Station screen (single-line) on page 383).

Figure 81: Station screen (single-line)

```
change station n                                              Page 2 of 3
                                    STATION

FEATURE OPTIONS
           LWC Reception? none
          LWC Activation? y                      Coverage Msg Retrieval? y
  LWC Log External Calls? n                                Auto Answer: none
            CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                       Call Waiting Indication: n
 Per Button Ring Control? n                  Att. Call Waiting Indication: n
   Bridged Call Alerting? n                     Distinctive Audible Alert? y
        Switchhook Flash? n                           Adjunct Supervision? n
    Ignore Rotary Digits? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number? _
       Service Link Mode: as-needed
         Multimedia Mode: basic                    Audible Message Waiting? n
    MWI Served User Type: _______
              AUDIX Name: _______
                                                 Coverage After Forwarding? _

                                              Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001                           IP Audio Hairpinning? n
Precedence Call Waiting? y
```

3. In the **Bridged Call Alerting?** field, perform one of the following actions:
   - If you want the bridged appearance to ring when a call arrives at the primary telephone, type **y**.
   - If you want the bridged appearance to flash but not ring when a call arrives at the primary telephone, leave the default set to **n**.
4. Click **Next** until you see the **Line Appearance** field (Figure 82: Station screen (single-line) on page 384).

Figure 82: Station screen (single-line)

```
                                    STATION
 SITE DATA
      Room: _______                                      Headset? n
      Jack: _______                                      Speaker? n
     Cable: _______                                     Mounting? d
     Floor: _______                                  Cord Length: 0
  Building: _______                                    Set Color: ______

ABBREVIATED DIALING
     List1: ___________       List2: _________         List3: _________

HOT LINE DESTINATION

         Abbreviated Dialing List Number (From above 1, 2 or 3):
                                                      Dial Code:
      Line Appearance:  brdg-appr   Btn:     Ext:
```

5. In the **Line Appearance** field, perform one of the following actions:
   - Type **abrdg-appr** to create a bridged appearance of a single-line telephone.
   - Type **brdg-appr** to create a bridged appearance of a multiappearance telephone.
6. Press **Enter**.

   The system displays the **Btn** and **Ext** fields.
7. In the **Btn** field, type the button number from the primary telephone that you want to use for the bridged call appearance.
8. In the **Ext** field, type the extension of the primary telephone.
9. Press **Enter** to save your changes.

Creating a bridged call appearance on a multiappearance telephone

To create a bridged call appearance on a multiappearance telephone:

1. Type **`change station`** ***`n`***, where ***`n`*** is the extension of the multiappearance telephone on which you want to create the bridged call appearance. Press **Enter**.

   The system displays the Station screen for a multiappearance telephone.
2. Click **Next** until you see the **Per Button Ring Control?** field (Figure 83: Station screen (multiappearance telephone) on page 385).

Figure 83: Station screen (multiappearance telephone)

```
change station n                                              Page 2 of 4
                                    STATION

FEATURE OPTIONS
           LWC Reception? spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                       Coverage Msg Retrieval? y
  LWC Log External Calls? n                                 Auto Answer: none
            CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? y
   Bridged Call Alerting? n                    Restrict Last Appearance? y
  Active Station Ringing: single          Conf/Trans On Primary Appearance? n

        H.320 Conversion? n          Per Station CPN - Send Calling Number? _
       Service Link Mode: as-needed       Busy Auto Callback without Flash? y
         Multimedia Mode: basic
    MWI Served User Type: ______                 Display Client Redirection? n
         Automatic Moves:
              AUDIX Name:                       Select Last Used Appearance? n
                                                  Coverage After Forwarding? _
     Recall Rotary Digit? n                         Multimedia Early Answer? n

Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001      Always use? n        IP Audio Hairpinning? n
Precedence Call Waiting? y
```

3. Perform one of the following actions:
   - To assign ringing separately to each bridged appearance, type **y**.
   - To assign all bridged appearances to either ring or not ring as determined by the **Bridged Call Alerting** field, leave the default set to **n**.
4. In the **Bridged Call Alerting?** field, perform one of the following actions:
   - If you want the bridged appearance to ring when a call arrives at the primary telephone, type **y**.
   - If you want the bridged appearance to flash but not ring when a call arrives at the primary telephone, leave the default set to **n**.
5. In the **Bridged Idle Line Preference?** field, perform one of the following actions:
   - If you want the user to lift the telephone receiver, then press the lighted bridged appearance button to connect to the call, type **y**.
   - If you want the user to just lift the telephone receiver to connect to the call, leave the default set to **n**.
6. In the **Auto Select Any Idle Appearance?** field, perform one of the following actions:

- To allow automatic selection of an alternate idle appearance for transferred or conferenced calls when another appearance of the bridged number is unavailable, type **y**.
- To prevent this automatic selection, leave the default set to **n**.

7. Click **Next** until you see the **Button Assignments** area (Figure 84: Station screen (multiappearance set) on page 386).

Figure 84: Station screen (multiappearance set)

```
change station n                                              Page 3 of 4
                                    STATION
    SITE DATA
          Room: _______                                 Headset? n
          Jack: _____                                   Speaker? n
         Cable: _____                                  Mounting: d
         Floor: _______                              Cord Length: 0
      Building: _______                                Set Color: ______



   ABBREVIATED DIALING
        List1: ________          List2: ________          List3: ________

   BUTTON ASSIGNMENTS
     1: brdg-appr  Btn:   Ext:
     2: brdg-appr  Btn:   Ext:
```

8. In the **Button Assignments** area next to any available button number, perform the following actions:
   - Type **abrdg-appr** to create a bridged appearance of a single-line telephone.
   - Type **brdg-appr** to create a bridged appearance of a multiappearance telephone.
9. Press **Enter**.

   The system displays the **Btn** and **Ext** fields.
10. In the **Btn** field, enter the button number from the primary phone that you want to use for the bridged call appearance.
11. Enter the extension of the primary telephone.
12. Press **Enter** to save your changes.

Considerations for Bridged Call Appearance

This section provides information about how the Bridged Call Appearance feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Bridged Call Appearance feature under all conditions.

The following considerations apply to single-line telephones:

- A bridging user cannot have more than one bridged appearance for a particular primary telephone. However, a multiappearance bridging user can have bridged appearances of more than one single-line telephone on their telephone (a multiappearance bridging user, by use of different buttons, can bridge onto several different primary telephones).
- If the primary single-line telephone is correctly administered, but not in service, calls can still be placed by the bridging users, and received on the bridged appearances of the telephone.
- If more than one user goes off-hook on a bridged appearance at the same time, only the user who was the first to go off-hook can dial.
- The Privacy-Manual Exclusion feature can be activated by the bridging user only, while active on a call, to prevent accidental bridging of an active call.
- If a call terminates at a telephone on an extension other than the primary extension (for example, terminating extension group (TEG), UCD group, call coverage answer group, or DDC group extension), a bridged call appearance is not maintained. Therefore, the primary telephone should not be made a member of such a group.
- If two parties are bridged together on an active call with a third party, and if the conference tone feature is enabled, conference tone is heard.

The following considerations apply to multiappearance telephones:

- On multiappearance telephones, a bridged call appearance can be assigned to any 2-lamp button. It does not require the use of a regular call appearance. The number of bridged call appearances allowed at each telephone is limited only by the number of 2-lamp buttons available on the telephone.
- Up to six parties can be off-hook and involved in a conversation on a bridged appearance of an extension.
- A bridging telephone might have a bridged call appearance corresponding to each call appearance of the primary extension at the bridged telephone. For example, if a primary telephone has three call appearances, a bridging telephone should have three bridged call appearances of that primary extension. This allows users to refer to the individual call appearances when talking about a specific call.
- Bridged call appearances may result in the reduction of available feature buttons, thereby reducing a user’s capabilities. You can use a Call Coverage module or expansion module to provide additional bridged call appearances.

- If a call terminates at a telephone on an extension other than the primary extension, a bridged call appearance is not maintained. Examples of such termination points can be TEG, UCD group, call coverage answer group, or DDC group extensions. Therefore, the primary telephone should not be made a member of such a group.
- You can administer conference tone, which, when enabled, is heard when two parties are bridged together on an active call with a third party.
- You can administer a telephone with zero call appearances of its primary extension. In this way, a telephone can be administered to have only bridged appearances.

Interactions for Bridged Call Appearance

This section provides information about how the Bridged Call Appearance feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Bridged Call Appearance in any feature configuration.

- Abbreviated Dialing

  A user, accessing Abbreviated Dialing while on a bridged call appearance, accesses their own Abbreviated Dialing lists. The user does not access the Abbreviated Dialing lists of the primary extension associated with the bridged call appearance.

  A user cannot use an abbreviated dialing Feature Access Code (FAC) after using a priority calling FAC.

- Adjunct Switch Applications Interface (ASAI)

  If you are using ASAI, do not administer more than 16 bridged appearances.

- Attendant display and telephone display

  A call from the primary extension or from a bridged call appearance of the primary extension is displayed as a call from the primary extension. That is, the call is displayed as coming from the primary extension regardless of which appearance placed the call.

  On multiappearance telephones, the display at the primary telephone shows the same information for a bridged call appearance as the information for a nonbridged call. For calls to the primary extension, the display at a zero call appearance bridging telephone shows a call from the originator to the primary with no "redirection reason" character.

- Automatic Call Distribution (ACD)

  Bridged appearances cannot be accessed using non-ACD hunt groups (although administrable).

- Automatic Callback

  Automatic Callback calls cannot originate from a bridged call appearance. However, when Automatic Callback is activated from the primary telephone. The callback call rings at all bridged appearances of the extension and at the primary telephone. This ring is set with priority call distinctive ringing signal. It displays at all telephones and shows that it is a callback call.

- Busy Indicator (multiappearance telephones only)

  A user presses a Busy Indicator button to call the extension associated with the Busy Indicator button. When a user presses a Busy Indicator button on a zero primary call appearance telephone, the system uses the first available bridged call appearance to place the call.

- Call Coverage

  - Single-line telephones

    When a single-line telephone is administered as a bridged call appearance, the telephone user cannot invoke Send All Calls for the extension of their telephone. The user does not have a send all calls button, and the call appearance is associated with another extension. When the user dials a FAC, Send All Calls is activated for the extension associated with the call appearance.

  - Multiappearance telephones

    Coverage criteria for bridged call appearances is based entirely on the criteria of the primary extension associated with bridged appearance. A call to the primary extension that requires call coverage treatment follows the coverage path of the primary extension. Such a call does not follow the path of any of the bridged appearances. Bridged call appearances do not receive redirection notification.

    A user with bridged call appearances can activate or deactivate Send All Calls for a primary telephone from the bridged appearance.

    The primary telephone should not be a member of a call coverage group. This is because calls to the primary telephone as a member of the group are not bridged.

    You can administer the system so a call can appear at a telephone as both a bridged call and a redirected call. In this way, if the bridged user is the first coverage point, the call redirects to that telephone when the coverage criteria are satisfied.

    If the primary telephone is a single-line telephone with a bridged call appearance on a multiappearance telephone, an incoming call to the single-line telephone that goes to coverage terminates at a primary call appearance on the bridging user's telephone as a coverage call. If the bridging user is a zero primary call appearance telephone, the call cannot redirect to the bridging user. This is because there are no primary call appearances. Therefore, the call redirects to the next available coverage point.

- Call Detail Recording (CDR)

  If a bridging user originates or answers a call on a bridged appearance, the extension of the bridge is recorded as the calling/called telephone. A conference or transfer by a bridging user also appears like it was performed by the telephone user.

  On multiappearance telephones, when a call originated from a bridged call appearance on a telephone administered for zero primary call appearance is recorded by CDR, the extension associated with the appearance is recorded as the calling party. A conference or transfer by a bridged call appearance on a zero primary call appearances telephone also appears as performed by the extension associated with the appearance.

- Call Forwarding All Calls, Call Forward Busy/Don't Answer

  Call Forwarding can be activated or canceled for the primary extension from any bridged call appearance of that number. When activated, calls to the primary extension do not terminate at the bridged call appearances, but go to the designated forwarding destination. Bridged call appearances do not receive redirection notification of the call to the primary extension when it is forwarded unless Ringing - Abbreviated and Delayed is administered.

- Call Park

  When a call is parked from a bridged call appearance, it is parked on the primary extension.

- Call Pickup

  Calls that are made to a primary telephone, alerting at bridged appearances of the primary telephone, can only be answered by pickup group members of the primary number.

  - If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to **n**, the primary appearance and all bridged appearances of the call are dropped after Call Pickup is used to answer the call.
  - If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to **y**, the primary and bridged call appearance lamps stay lit after Call Pickup is used to answer the call.
  - If the primary telephone and the bridged telephone are both in the same pickup group, members in the pickup group can answer a call that is made to the primary telephone that is ringing at the bridging user's telephone. This can be done instead of selecting the bridged appearance button.

  - If the primary telephone and the bridged call appearance are not in the same pickup group, members who are in the same pickup group as the bridged call appearance telephone can answer a call that is made to the primary telephone.

  When a user dials the the Call Pickup FAC on a bridged call appearance, the system interprets the action as an attempt to answer a call from the call pickup group of the primary telephone. When operating this way, the covering user can act as the primary user and provide the same call pickup coverage if desired.

  If a telephone has bridged call appearances of numerous telephones, for example, sales, service, and warehouse, and you want calls to be answered only by the primary telephone users or the bridging users, do not assign the primary and bridging users to a pickup group.

- Call Waiting Termination (single-line telephones only)

  Call Waiting Termination applies only to an active call on the primary telephone that has no one else bridged on. If one or more bridging users are active on a call, call waiting calls are denied even if the primary user is also off-hook on the call. A bridging user can bridge onto a call with the primary user if there is also a call waiting.

- Class of Restriction (multiappearance telephone users only)

  The COR assigned to a telephone's primary extension also applies to calls originated from a bridged call appearance.

- Conference - Attendant, Conference

– Single-line telephones

  A bridged call cannot be conferenced if more than one user is active on that call. This is because the bridging user has no access to the call after the primary telephone user places the call on soft hold, and the primary telephone user has no access to the bridging user's call appearance used for conference/transfer attempts.

  You can place a call on hold using normal single-line conference procedures when the primary telephone user is active on a call, and no other bridging user is active on the call. Any attempt by a bridging user to bridge onto the call during a successful conference attempt is denied.

  A single bridging user can conference the call using the normal multiappearance telephone conference procedures. Any attempt by the single-line primary telephone user to bridge onto the call during a successful conference attempt is ignored. Any attempt by other bridging users is denied (standard denial response is returned to the bridged appearance).

  If a conference is not allowed because of the preceding limitations, the user can accomplish a transfer by asking an internal nonbridged party in the connection to create the conference. The user can also ask the remaining bridging users and primary user to disconnect so that the conference can be completed. At completion of the conference, the parties that left the call can reenter the call if control of the conference remains with the primary telephone. If conference control does not remain with the primary telephone, the bridging user must conference the primary telephone and the bridging user back into the call as required.

  If the bridging user has no other available bridged appearances of the primary extension (other than the one he or she is currently on), the bridging user, after pressing the conference/transfer button, must select a call appearance to be used for the conference, before dialing the number.

– Multiappearance telephones

Conferences can be set up on bridged appearances using the usual conference operations. Either a primary extension button or a bridged appearance button can be used to make the calls for adding to the conference.

You can administer the system to automatically select the first idle appearance if there is no idle appearance with an extension matching the extension that is conferencing the call.

When the user presses the conference button (the second time) to connect the parties together, the newly formed conference call appears on the primary or bridged appearance to which the user was connected at the time of that last conference button depression. The other appearance is disassociated from the conference call. Therefore, if the original call is on a bridged appearance, and the conference is formed on a primary appearance at that same telephone, the bridged extension becomes disassociated from the conference call. In this case, the primary user can no longer bridge onto the conference.

This disassociation of the conference from the bridged extension can be avoided by setting up the conference in the opposite order. To do this, the user:

a. Presses the hold button to hold the original call on the bridged appearance

b. Selects a call appearance and calls the party to be added

c. Presses the conference or transfer button

d. Selects the held bridged appearance

e. Presses the conference button (again)

When this procedure is used, the conference is formed on the bridged appearance so that the primary user can still bridge onto the conference call.

If the primary user and the bridged user are both on the call when one user transfers the call, the user performing the transfer becomes the controlling user for the participation of both users on the conference. To disassociate the appearance from the call, the controlling user must be the latter of the two users to hang up from the call. If the controlling user hangs up first, the appearance goes on soft hold when the noncontrolling party hangs up. In this case, one of two things must occur to disassociate the appearance from the call: all other parties on the call hang up, or the controlling user rejoins the call and hangs up again.

The display shows the number of other active parties in a call, including active bridged appearances.

- Consult (multiappearance telephones only)

  Bridged call appearances of the primary extension do not ring on a consult call to the primary extension.

- Coverage Answer Group

- Single-line telephones

  Calls to the primary telephone as a member of a Coverage Answer Group are not bridged.

  If the primary telephone is made a member of a coverage group, coverage criteria is based entirely on the criteria of the primary telephone. This means that a call to the primary telephone that requires call coverage treatment follows the path of the primary telephone and not the path of any of the telephones with bridged appearances of the primary telephones.

- Multiappearance telephones

  Bridged call appearances of a primary extension do not ring when there is a Coverage Answer Group (CAG) call to the primary extension. Bridged call appearances cannot bridge onto the call.

- Data Privacy, Data Restriction

  When Data Privacy is activated or Data Restriction is assigned to a telephone involved in a bridged call and the primary telephone and/or bridging user attempts to bridge onto the call, Data Privacy and Data Restriction are automatically overridden (or deactivated in the case of Data Privacy).

- Emergency calls

  If a user dials an emergency call from a bridged appearance, the Calling Party Number that is sent to the public safety answering point for US E911 locations is the extension of the physical telephone from which the call is made.

- Hold - Automatic

  - Single-line telephones

    A call cannot be put on hold if more than one user is active on that call.

    The primary telephone user, when no other bridges are active on the call, can put the call on hold, using normal single-line hold procedures. If the primary telephone user successfully soft holds the call, the status lamp at all of the bridged appearances shows the hold indication; and then the call can be put on hard hold by dialing the hard hold FAC. The hard held call is no longer accessible to the bridging users until it is taken off hold by the primary telephone user. After the call is put on hard hold, any new call to the primary telephone is tracked by the bridged appearances.

    A bridging user can place an active call on hold (if the primary telephone or any other bridges are not active on the call) by using normal multiappearance hold procedures. Any attempt to enter the held call returns it to the status of an active call that can then be accessed using bridging procedures.

  - Multiappearance telephones

    Any user (primary or bridged appearance) can place an active call on hold. If only one user is active on a call and places that call on hold, the indicator lamp at both the primary's appearance button and the bridged appearance button show that the call is on hold. If more than one user is bridged onto the active call, and one of the users activates Hold, the activator receives "hold" indication for the call and status lamp of all other bridged users remains active.

- Hotline Service (single-line telephones)

  If a single-line telephone is administered for Hotline Service, bridged appearances of that telephone's extension also place a hot line call automatically when a user goes off-hook on that bridged appearance.

- Hunt Group (DDC or UCD)

  Bridged call appearances cannot be used in conjunction with DDC or UCD hunt groups.

  Although you can assign a bridged extension to a hunt group, Avaya does not recommend such assignment because DDC/UCD calls do not terminate at any bridged appearances of that extension on other telephones.

- Intercom (multiappearance telephones only)

  Bridged appearances of a primary extension are not rung for intercom calls. Furthermore, if a telephone has no primary call appearances it can never be rung for an intercom call. Therefore, if someone is screening all calls for the primary telephone, and is indicating who is calling through intercom, the primary telephone must have a call appearance on which to receive and send intercom calls.

- Internal Automatic Answer (IAA)

  Calls terminating to a bridged appearance of an IAA-eligible telephone are not eligible for IAA.

- Last Number Dialed (LND)

  Activation of the LND feature causes the last number dialed from the activating telephone to be redialed, regardless of the extension used (primary or bridged call appearance).

- Leave Word Calling (LWC)

  A LWC message left by a user on a bridged call appearance leaves a message for the called party to call the primary extension assigned to the bridged call appearance.

  When a user calls a primary extension, and activates LWC, the message is left for the primary extension, even if the call was answered at a bridged call appearance.

  LWC messages left by the primary user can be canceled by a bridged appearance user.

- Personal Central Office Line

  - Single-line telephones

    A single-line primary telephone cannot be a member of a Personal Central Office Line (PCOL) group.

  - Multiappearance telephones

    If a user is active on his or her primary extension on a PCOL call, bridged call appearances of that extension cannot be used to bridge onto the call. The call can only be bridged onto the call if another telephone is a member of the same PCOL group and has a PCOL button.

- Personal Status Access (PSA)

  PSA allows a user to execute a dissociate request from a bridged appearance. However, when a user executes a dissociate command at telephone B, the user dissociates from telephone B. This is the case, even if the user is on a bridged appearance that belongs to telephone A.

- Priority Calling

  The primary telephone user or the bridging user can make a priority call. If a priority call is made to an idle telephone, the primary telephone and all bridging users are alerted by priority alerting.

- Privacy-Manual Exclusion

  Activation of exclusion by any user (primary or bridged appearance) before placing a call, prevents any other user from bridging onto the call. Activation of exclusion by any user active on a call, while the primary user and/or any other bridging users are active on the call, drops all other users from the call (including the primary user), leaving only the activator and the calling/called party on the call.

- Redirection Notification (multiappearance telephones only)

  Redirection Notification is not provided at bridged appearances unless Ringing - Abbreviated and Delayed is administered to give notification.

- Ringback Queuing

  Ringback Queuing is not provided on calls originated from a bridged call appearance. However, after the primary user of the bridged extension has activated Ringback Queueing, the resulting callback call alerts at bridged appearances as well as at the primary user’s telephone. The call can be answered from the primary user’s telephone or from any bridged appearance.

- Ringer Cutoff (multiappearance telephones only)

  Ringer Cutoff prevents any nonpriority (or nonintercom) incoming call from ringing at that telephone. This is independent of whether the call is to the telephone’s primary extension or to any of the bridged appearances’ extensions.

- Service Observing

  You observe calls on a primary extension and all bridged appearances of that extension. You cannot observe bridged appearances on the extensions phone. For example, if you are observing extension 3082 and this telephone also has a bridged appearance for extension 3282, you cannot observe calls on the bridged call appearance for 3282. But if you observe extension 3282, you can observe activity on the primary and all of the bridged call appearances of 3282.

  The primary telephone user or bridging user can bridge onto a service observed call of the primary at any time. A bridging user cannot activate Service Observing using a bridged call appearance.

  If the primary is service observing on an active call, a bridged call appearance cannot bridge onto the primary line that is doing the service observing.

- Terminating Extension Group (TEG)

  TEG calls to the primary extension do not ring at the associated bridged appearances. TEG calls cannot be answered or bridged onto from a bridged appearance. The primary telephone should not be assigned to a TEG.

- Terminal Translation Initialization (TTI)

  If a user is on a bridged appearance, the user cannot use TTI to separate from the telephone.

- Transfer

  – Single-line telephones

    A call cannot be transferred by a single-line telephone if more than one user is active on that call.

    The primary telephone user, when no other bridges are active on the call, can transfer the call using normal single-line transfer procedures. Any attempt by a bridging user to bridge onto this call during a successful transfer attempt is denied.

    A single-line bridging user, alone on a bridged call, can transfer the call, using normal transfer procedures. Any attempt by the primary telephone user to bridge onto this call during a successful transfer attempt is ignored; and any attempt to bridge on by a bridging user is denied.

    If the bridging user has no other available bridged appearances of the primary extension (other than the one he or she is currently on), the bridging user, after pressing the conference/transfer button, must select a call appearance to be used for the transfer, before dialing the number.

- Multiappearance telephones

  If the bridging user has at least one available bridged appearance of the primary extension (other than the one he or she is currently on), the system automatically selects a bridged call appearance for the transfer when the conference/transfer button is pressed.

  You can administer the system to automatically select the first idle appearance if there is no idle appearance with an extension matching the extension that is transferring the call.

  If the primary user and the bridged user are both on the call when one user transfers the call, the user performing the transfer becomes the controlling user for the participation of both users on the conference. The controlling user is immediately dropped from the call. When the noncontrolling user hangs up, the appearance goes on soft hold. In this case, one of two things must occur to disassociate the appearance from the call: all other parties on the call hang up, or the controlling user rejoins the call and hangs up again.

- Videophone 2500 (single-line telephones)

  A user may not use a single-line bridge to a Videophone 2500 principal that is on a video call.

- Voice Message Retrieval

  A voice message to the primary extension can be retrieved on a bridged appearance by the bridged appearance user. If a security code is required to retrieve the message, the bridging user must use the security code of the primary telephone.

- Voice Paging

  The use of Voice Paging automatically invokes exclusion. Therefore, interactions for this feature are the same as for Privacy-Manual Exclusion.

Bulletin Board

Use the Bulletin Board feature to post information and retrieve messages from other users on the server. Avaya personnel can also leave high-priority messages on the bulletin board. The system displays the high-priority messages as the first 10 lines on the bulletin board.

Detailed description of Bulletin Board

This section provides a detailed description of the Bulletin Board feature.

Use the Bulletin Board feature to post information and retrieve messages from other users on the server. Anyone with an init or an inad login can add or change messages on the bulletin board. Avaya personnel can also leave high-priority messages on the bulletin board. The system displays the high-priority messages as the first 10 lines on the bulletin board.

When you log in to the system, the system alerts you to any messages that are on the bulletin board, and gives you the date of the last message.

If an Avaya employee enters a high-priority message while you are logged in, you receive the notification the next time that you enter a command. This high-priority message disappears after you enter a command. The system displays the high-priority message again each time that you log in, until you remove the message.

The bulletin board provides three pages of message space. You can write on any available line other than the high-priority lines.

You must maintain the bulletin board. If your bulletin board exceeds 80% capacity, the system displays the capacity that remains when you log in. If the bulletin board is full, the new messages overwrite the old messages.

Administering Bulletin Board

The following steps are part of the administration process for the Bulletin Board feature:

- Setting user permissions
- Changing bulletin board information

This section describes:

- Any prerequisites for administering the Bulletin Board feature

- The screens that you use to administer the Bulletin Board feature
- Complete administration procedures for the Bulletin Board feature

Screens for administering Bulletin Board

Screen Name	Purpose	Fields
Command Permission Categories	Give permission to users to type nonpriority information on the Bulletin Board screen.	• **Display Admin and Maint Data** • **Administer Features**
Bulletin Board	Add or change priority, or nonpriority, information in the system.	All

Setting user permissions

To give a user permission to type nonpriority information on the Bulletin Board screen:

1. Type **`change permissions`** ***`login ID,`*** where ***`login ID`*** identifies the user who is to use the Bulletin Board feature. Press **Enter**.

   The system displays the Command Permission Categories screen (Figure 85: Command Permission Categories screen on page 401).

Figure 85: Command Permission Categories screen

```
                                                              Page 1 of 3

                        COMMAND PERMISSION CATEGORIES
                              Login Name: Sup3ru

COMMON COMMANDS
                  Display Admin. and Maint. Data? y
                              System Measurements: y

ADMINISTRATION COMMANDS
       Administer Stations? y                Administer Features? y
         Administer Trunks? y             Administer Permissions? y
  Additional Restrictions? n

MAINTENANCE COMMANDS
         Maintain Stations? n     Maintain Switch Circuit Packs? n
           Maintain Trunks? n    Maintain Process Circuit Packs? n
          Maintain Systems? n              Maintain Enhanced DS1? n
```

2. In the **Display Admin. and Maint. Data?** field, perform one of the following actions:
   - Type **y** if you want the user to:
     - Type nonpriority messages on the bulletin board
     - Use the display, list, monitor, status commands
     - Change his or her password
     - Schedule reports
3. In the **Administer Features** field, perform one of the following actions:
   - Type **y** if you want the user to:
     - Type nonpriority messages on the bulletin board
     - Administer the feature-related parameters, such as coverage paths, class of service, class of restriction, system parameters, authorization codes, and security
4. Press **Enter** to save your changes.

Changing bulletin board information

To change bulletin board information:

1. Type **`change bulletin-board`**. Press **Enter**.

   The system displays the Bulletin Board screen (Figure 86: Bulletin Board screen on page 402).

Figure 86: Bulletin Board screen

```
change bulletin-board                                          Page 1 of 3

              Message (* indicates high-priority)                  Date
          *Avaya is in the process of                           03/02/2004
          *investigating your trunk lockup problem.             03/02/2004
          *The Bulletin Board will be updated as                03/02/2004
          *we find information.                                 03/02/2004
          *  We have identified the problem.                    03/02/2004
          *The trunk you added does not provide                 03/02/2004
          *disconnect supervision. However, the                 03/02/2004
          *trunk group was administered as such.                03/02/2004
          *Please call Pat J. for details.                      03/02/2004

          We recently added a new trunk group (14)              03/02/2004
          and have had many of the members getting              03/02/2004
          locked up.                                            03/02/2004
          We see the error - thanks for checking.               03/02/2004
```

The **date** field is a display-only field that contains the date that someone added or changed the line of information.

2. Type the bulletin board information.

   Those who have an init or an inads login, including Avaya personnel, can type high-priority information in Line 1 through Line 10. High-Priority messages have an asterisk (*) at the beginning of the line. When someone with an init or an inads login types the high-priority information, the system displays the high-priority message the next time that you log into the system.

   Those with an init or an inads login can type any of the following characters, number, and symbols:

Table 5: Bulletin board entries

Character, number, or symbol	Symbol Name
A through **Z**	
a through **z**	
Blank	
0 through **9**	
!	Exclamation mark

1 of 3

Table 5: Bulletin board entries (continued)

Character, number, or symbol	Symbol Name
@	At sign
#	Pound sign
$	Dollar sign
%	Percent sign
^	Circumflex
&	Ampersand
*	Asterisk
_	Underscore
+	Plus sign
-	Minus sign or dash
=	Equal sign
[	Left bracket
]	Right bracket
{	Left brace
}	Right brace
|	Bar or pipe
\	Back slash
‘	left single-quotation mark
’	right single-quotation mark or apostrophe
~	Tilde
;	Semi-colon
:	Colon
,	Comma

2 of 3

Table 5: Bulletin board entries (continued)

Character, number, or symbol	Symbol Name
"	Right double-quotation mark
<	Left angle-bracket
>	Right angle-bracket
.	Period
/	Forward slash
?	Question mark
	3 of 3

3. Type the bulletin board information.

   Those with permission, as defined on the Command Permission Categories screen, can type message information in:

   — Line 11 through Line 19 of Page 1

   — Line 1 through Line 20 of Page 2

   — Line 1 through Line 20 of Page 3

   Type any of the characters, numbers, or symbols shown in Table 5: Bulletin board entries on page 402. Press **Enter** to save your changes.

Considerations for Bulletin Board

This section provides information about how the Bulletin Board feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Bulletin Board under all conditions. The following considerations apply to Bulletin Board:

- Only users with an init or an inads login can add or edit high-priority messages.
- Only one user can change a message at a time.
- The bulletin board does not lose information during a system reset at level 1 or level 2. If you save translations, you can restore the information if a system reset occurs at levels 3, 4, or 5.

Busy Indicator

Use the Busy Indicator feature to provide multiappearance telephone users and attendants with a visual indicator of the busy or the idle status of one of the following system resources:

- An extension number
- A trunk group
- A terminating extension group (TEG)
- A hunt group, either direct department calling (DDC) or uniform call distribution (UCD)
- Any loudspeaker paging zone, including all zones

Detailed description of Busy Indicator

This section provides a detailed description of the Busy Indicator feature.

You can assign extension numbers, trunk group access codes, and Loudspeaker Paging access codes to a Busy Indicator button.

The Busy Indicator button provides the attendant or the user with direct access to the extension number, the trunk group, or the paging zone.

The Facility Busy lamp indication for a Vector Directory Number (VDN) does not light when the VDN is being used. You can use the associated button to place a call to a VDN.

Busy Indicator supports the following capabilities:

- Busy Tone Disconnect

Busy Tone Disconnect

In some regions of the world, the Central Office (CO) sends a busy tone for the disconnect message. With Busy Tone Disconnect (BTD), the switch disconnects analog loop-start CO trunks when the CO sends a busy tone.

A call that originates from or terminates to a telephone that uses a BTD-enabled trunk has a Call Classifier port connected to the trunk. The Call Classifier port connects after the call is answered and stays connected on the trunk until the station hangs up, or a BTD signal is received from the CO. If only one BTD trunk is on a call when the BTD signal is received, the call is dropped. If the call is a conference call, only the trunk is dropped. The rest of the parties stay connected.

Interactions for Busy Indicator

This section provides information about how the Busy Indicator feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Busy Indicator in any feature configuration.

- Answer Supervision

  If Answer Supervision is enabled, set the **Answer Supervision timeout** field to 0 (zero).

Busy Verification

Use the Busy Verification feature (Verify button) to allow attendants and specific multiappearance telephone users to make test calls to trunks, telephones, and hunt DDC and UCD groups. Attendants and multiappearance telephone users can distinguish between a telephone that is truly busy and one that only appears busy because of some trouble condition. Users can also use this feature to quickly identify faulty trunks.

Detailed description of Busy Verification

This section provides a detailed description of the Busy Verification feature.

An attendant or multiappearance telephone user can activate Busy Verify by pressing the Verify button. If they want to verify a telephone or hunt group, they enter an extension number. If they want to verify a trunk, they dial a trunk-access code, followed by the 2- or 3-digit number of the trunk-group member to be verified. If the trunk-group member number is less than 10, the system requires a leading zero (01 or 001 rather than 1).

Note:
For DEFINITY SI or DEFINITY CSI, the member number is a 2-digit number; for DEFINITY R, the member number is a 3-digit number.

After an attendant or multiappearance telephone user has activated Busy Verification, the system checks the validity of the extension or trunk-access code and member number. If the number is not a telephone extension, DDC/ UCD group-extension, ACD split number, or trunk access code with a valid member number, the system denies Verify and returns intercept tone.

When you use Verify to check a valid extension (one that is in the dial plan and assigned to a telephone), the system initiates a priority call to that extension. Table 6: Verification of a telephone on page 407 describes the process.

Table 6: Verification of a telephone

Telephone Status	System Response	Result
Idle	• Generates priority ringing at the telephone. • Processes the call as a normal telephone-originated or attendant-originated call	• Verification is complete. • Anyone can place a call to the telephone.

Table 6: Verification of a telephone

Telephone Status	System Response	Result
Active on a call and has an idle call appearance	• Generates priority ringing at the first idle appearance. • Processes the call as a normal attendant-originated call.	• Verification is complete. • Anyone can place a call to the telephone extension.
Active on a call and has no idle call appearances or has only one line appearance	• Bridges the attendant onto the call. • Generates a warning tone to all active parties and repeats the tone every 15 seconds while the attendant remains bridged onto the call.	• Verification is complete. • The attendant can determine if the telephone is actually in use.
Out of service	• Generates reorder tone.	• Verification is denied.

When you use Verify to check a valid ACD split, UCD group, or DDC group, the system initiates a priority call to that group. (Valid in this case means the split or group is translated and at lease one member is logged in.) Table 7: Verification of an ACD Split, UCD Group, or DDC Group on page 408 describes the process.

Table 7: Verification of an ACD Split, UCD Group, or DDC Group

Split or Group Member Status	System Response	Result
Available for an incoming call	• Generates priority ringing at the member's telephone. • Processes the call as a normal attendant-originated call.	• Verification is complete. • Anyone can place a call to the member's telephone.
All activated Make Busy	• Generates reorder tone.	• Verification is denied.
Not available for incoming calls	• The system does not queue the call even if a queue is available. • Generates reorder tone.	• Verification is denied.

When you use Verify to check a valid trunk, the system checks the status of that trunk. (Valid in this case means the trunk is translated with members and is not in an out-of-service state.) Table 8: Verification of a Trunk on page 409 describes the process.

Table 8: Verification of a Trunk

Trunk Status	System Response	Result
The trunk is idle and incoming.	• The system generates confirmation tone.	• Verification is complete. • Anyone can use the trunk.
The trunk is idle and outgoing.	• The system generates dial tone.	• Verification is complete. • Anyone can use the trunk.
The trunk is busy with an active call.	• The system bridges the Verify originator onto the call. • The system generates a warning tone to all active parties and repeats the tone every 15 seconds while the Verify originator remains bridged onto the call.	• Verification is complete. • The trunk is in use.
The trunk is out of service.	• The system generates reorder tone.	• Verification is denied.

Administering Busy Verification

The following steps are part of the administration process for the Busy Verification feature:

- Using Busy Verification

This section describes:

- Any prerequisites for administering the Busy Verification feature
- The screens that you use to administer the Busy Verification feature
- Complete administration procedures for the Busy Verification feature

Prerequisites for administering Busy Verification

You must complete the following actions before you can administer the Busy Verification> feature:

- View the Trunk Group screen, ensure that the **Dial Access** field is **y**. If this field is not set to **y**, contact your Avaya representative before you continue with this procedure.

Screens for administering Busy Verification

Screen name	Purpose	Fields
Station	Set up busy verify extension.	**Feature Button Assignments**

Using Busy Verification

To use Busy Verification:

1. Type **change station *n***, where ***n*** is the station to be assigned the busy verify button. Press **Enter**.

   For this example, enter extension **1014**.

   The system displays the Station screen (Figure 87: Station screen on page 410).

Figure 87: Station screen

```
 Page 3 of X
                                    STATION
     SITE DATA
          Room: _______                                  Headset? n
          Jack: ___                                      Speaker? n
         Cable: ___                                     Mounting: d
         Floor: _______                           Cord Length: 0_
      Building: _______                             Set Color: _____


ABBREVIATED DIALING
     List1: ________          List2: _________          List3: _________

BUTTON ASSIGNMENTS
 1: call-appr                  4: verify__
 2: call-appr                  5: ________
 3: call-appr
```

2. In the **Feature Button Assignments** field, type **verify**.
3. Press **Enter** to save your changes.

4. To activate the feature, press the **Verify** button on the phone and then enter the Trunk Access Code and member number to be monitored.

Considerations for Busy Verification

This section provides information about how the Busy Verification feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Busy Verification under all conditions. The following considerations apply to Busy Verification:

- A busy verification cannot be made to an analog extension that is waiting to be answered at another extension. A call must be answered before it can be verified.
- If your country requires a tone other than 440 Hz, use the Intrusion feature rather than Verify to verify telephones.
- The system does not provide bridging when you verify UCD and DDC groups or RLTs.
- You cannot make outgoing test calls on DID trunks.
- You can verify an extension that is administered without hardware (X-ported). In this case, the system generates reorder tone.

Interactions for Busy Verification

This section provides information about how the Busy Verification feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Busy Verification in any feature configuration.

- Automatic Callback

  Once the called party in an Automatic Callback call hangs up, neither extension can be busy-verified until both the calling and called parties are connected or the callback attempt is canceled (by the activating party or by time-out of the callback interval).

- Call Coverage

  Since the busy-verification call to an extension is originated as a priority call, the call does not go to coverage.

- Call Forwarding

  Busy verification made to an extension with call forwarding activated, does not busy verify the forwarded-to extension. Only the called extension is busy verified.

- Call Waiting Termination

  You cannot verify an extension that called an active telephone and is receiving call-waiting ringback tone unless the extension has an idle call appearance.

- Conference

  The system denies busy verification of any extension involved in a conference call of more than five people. However, the system does allow a busy verification of any extension involved in a conference call of 5 or fewer parties. The system also denies busy verification of a trunk on a 6-party call.

- Data Privacy

  Busy verification is denied if it would cause a bridging attempt on a telephone that has activated Data Privacy.

- Data Restriction

  The system denies Verify if Data Restriction is active on a call, and a busy verification bridging attempt is made on that call.

- Hold

  Busy verification of a multiappearance telephone is denied if all call appearances have calls on hold.

- Individual Attendant Access

  An attendant cannot make a busy verification of another individual attendant console or of the attendant group.

- Loudspeaker Paging Access

  The system denies busy verification if the telephone or trunk to be verified is connected to paging equipment.

- Transfer

  Once the originator of busy verification has bridged onto a call, any attempt to transfer the call is denied until the originator drops from the call.

- Telephone Origination Restriction

  A telephone that is origination restricted can be assigned a Busy Verify button. However, the button cannot be used.

- Telephone Termination Restriction

  The system denies busy verification of telephones that are termination restricted.

Call Charge Information

Use the Call Charge Information feature to determine the approximate charge for calls that are made on outgoing trunks.

Detailed description of Call Charge Information

This section provides a detailed description of the Call Charge Information feature.

Communication Manager provides two ways to know the approximate charge for calls made on outgoing trunks.

Call Charge Information supports the following capabilities:

- Advice of Charge
- Periodic Pulse Metering
- Charge Display

Advice of Charge

For ISDN trunks, Advice of Charge (AOC) collects charge information from the public network for each outgoing call. Charge advice is a number that represents the cost of a call. The system records the charge information as either a charging unit or a currency unit.

Periodic Pulse Metering

For non-ISDN trunks, Periodic Pulse Metering (PPM) accumulates pulses that are transmitted from the public network at periodic intervals during an outgoing trunk call. At the end of the call, the number of pulses collected is the basis on which charges are determined.

Call-charge information helps you to account for the cost of outgoing calls before you receive the call charges from your network provider. The ability to account for the cost of outgoing calls before you receive the call charges from your network provider is especially important in countries where telephone bills are not itemized.

You can also use the information about the cost of outgoing calls to give the cost of telephone calls to employees. The cost information of outgoing telephone calls can help users to better manage their use of company telecommunications facilities. Note, however, that you cannot necessarily use the call charge information that the Call Charge Information feature provides to reconcile telephone bills with your network provider.

You must request either AOC service or PPM service from your network provider. In some areas, your selection is limited. Note that the public network does not offer AOC service and PPM service in some countries, including the US. In some countries, AOC information is received automatically for each call. In other countries, the system must request AOC information for each call. Your Avaya representative can help you determine the type of service that you need.

In some countries, the public network sends call-charge information only at the end of a call. In other countries, the public network sends information both at the end of the call and while the call is in progress. PPM is available over the following trunk types:

- Central office (CO)
- Direct inward and outward dialing (DIOD)
- Foreign exchange (FX)
- Personal Central Office Line (PCOL)
- Wide Area Telecommunications Service (WATS)

Charge Display

With Communication Manager, you can view call charge information on a telephone display, or on a Call Detail Recording (CDR) report.

Charge Display at a user telephone

You can allow users to view call charges on telephone displays. From a display, a user can see the cost of an outgoing call, both while the call is in progress and at the end of the call. If you want users to control when the display of the call charge information, you can assign a display button that the user can press to see the current call charges. You can also administer the system so that the system displays call charges automatically whenever a user places an outgoing call.

Charge Display on a CDR report

You can administer the system to display call charges on CDR reports. For more information, see the "Call Detail Recording" feature.

Either the **ISDN C C** field or the **PPM** field in the CDR record contains the last cumulative charge received from the network. If Call Splitting or Attendant Call Recording is enabled, and a call is transferred for the first time, the **ISDN Call Charge** field contains the cumulative charge that was most recently received from the network.

For all subsequent transfers, the **ISDN Call Charge** field contains the difference between the cumulative charge that was most recently received and the value that was generated in the previous CDR record for the same call.

A zero appears in the **Call Charge** field when:

- No AOC information is received
- A value of zero is the last charge information that was received
- The outgoing trunk group is not administered for AOC or PPM

Administering Call Charge Information

The following steps are part of the administration process for the Call Charge Information feature:

- Administering the charge display
- Administering AOC for ISDN trunks
- Administering PPM for non-ISDN trunks
- Administering PPM for DS1 circuit packs

This section describes:

- Any prerequisites for administering the Call Charge Information feature
- The screens that you use to administer the Call Charge Information feature
- Complete administration procedures for the Call Charge Information feature

Prerequisites for administering Call Charge Information

You must complete the following actions before you can administer the Call Charge Information feature:

- Defining CDR to support Call Charge Information
- Specifying the frequency of the call charge displays
- Translating the text "Call Charge"
- Assigning a COR for charge displays

Defining CDR to support Call Charge Information

To define Call Detail Recording (CDR) to support Call Charge Information:

1. Type **change system-parameters cdr**. Press **Enter**.

   The system displays the CDR System Parameters screen (Figure 88: CDR System Parameters screen on page 416).

Figure 88: CDR System Parameters screen

```
change system-parameters cdr                                    Page   1 of 2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 18                    CDR Date Format: month/day
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
Modified Circuit ID Display? n                  Remove # From Called Number? y
                 Record Outgoing Calls Only? n            Intra-switch CDR? y
  Suppress CDR for Ineffective Call Attempts? y     Outg Trk Call Splitting? y
      Disconnect Information in Place of FRL? n       Outg Attd Call Record? y
                                                   Interworking Feat-flag? y
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                   Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
      Record Call-Assoc TSC? n  Digits to Record for Outgoing Calls: outpulsed
   Privacy - Digits to Hide: 0              CDR Account Code Length: 4
```

2. Administer the CDR System Parameters screen. For more information, see the "Call Detail Recording" feature.

Specifying the frequency of the call charge displays

To specify the frequency of the charge display:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen (Figure 89: Feature-Related System Parameters on page 417).

Figure 89: Feature-Related System Parameters

```
display system-parameters features                              Page   9 of 14
                        FEATURE-RELATED SYSTEM PARAMETERS

                 Pull Transfer: n           Update Transferred Ring Pattern? n
         Outpulse Without Tone? y             Wait Answer Supervision Timer? n
         Misoperation Alerting? n              Repetitive Call Waiting Tone? n
    Allow Conference via Flash? y
 Vector Disconnect Timer (min):      Network Feedback During Tone Detection? y
                                     ystem Updates Time On Station Displays? y
      Intercept Treatment On Failed Trunk Transfers? n
                    Station Tone Forward Disconnect: silence
                              Level Of Tone Detection: precise
          Charge Display Update Frequency (seconds): 30
        Date Format on 607/2420/4600/6400 Terminals: mm/dd/yy
Onhook Dialing on 607/2420/4600/6400/8400 Terminals? n



ITALIAN DCS PROTOCOL
  Italian Protocol Enabled? n
```

2. In the **Charge Display Update Frequency (seconds)** field, type the number of seconds between the charge update information displays that a user sees.

   The valid entries are **10** through **60,** and blank.

   Note that frequent display updates can have an impact on the performance of the system. If the duration of a call is less than the value in the **Charge Display Update Frequency (seconds)** field, the display does not automatically show the charge information.

   If you want a user to see the charge information, you must assign a **disp-chrg** feature button on the Station screen for a user.

3. Press **Enter** to save your changes.

Translating the text "Call Charge"

To translate the text for "Call Charge:"

1. Type **`change display-messages miscellaneous-features`**. Press **Enter**.

   The system displays the Language Translations screen (Figure 90: Language Translations screen on page 418).

Figure 90: Language Translations screen

```
change display-messages miscellaneous-features                    Page 5 of 8
                            LANGUAGE TRANSLATIONS

   42.     English: Add Skill: Enter number, then # sign
       Translation: ************************************

   43.     English: Remove Skill: Enter number, then # sign
       Translation: ************************************

   44.     English: Enter Skill Level, then # sign
       Translation: ************************************

   45.     English: Enter Agent LoginID
       Translation: ************************************

   46.     English: Call Type
       Translation: ***************

   47.     English: Call Charge
       Translation: ********************
```

2. Click **Next** until you see the translation number **47**.
3. In the **Translation** field, type the translation for "Call Charge" if you need a translation for the text.
4. Press **Enter** to save your changes.

Assigning a COR for charge displays

To assign a Class of Restriction (COR) for automatic charge display:

1. Type **change cor *n***, where ***n*** is the number of the COR to which you want to assign an automatic charge display. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 91: Class of Restriction screen on page 419).

Figure 91: Class of Restriction screen

```
display cor 1                                                Page   1 of 4
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 7                                APLT? y
  Can Be Service Observed? n            Calling Party Restriction: none
Can Be A Service Observer? n             Called Party Restriction: none
        Time of Day Chart: 2         Forced Entry of Account Codes? n
         Priority Queuing? n                 Direct Agent Calling? n
     Restriction Override: none         Facility Access Trunk Test? n
     Restricted Call List? y                  Can Change Coverage? n

            Access to MCT? y              Fully Restricted Service? n
Group II Category For MFC: 7
         Send ANI for MFE? n               Add/Remove Agent Skills? n
            MF ANI Prefix:                Automatic Charge Display? y
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                         Can Be Picked Up By Directed Call Pickup? n
                                     Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

2. In the **Automatic Charge Display** field, perform one of the following actions:
   - If you want the user to automatically see the call charges during a call and at the end of a call, type **y**.
   - If you want the user to press the disp-chrg feature button to see the call charges. To see the call charges, the user must press the disp-chrg feature button before the system drops the call, type **n**.
3. Press **Enter** to save your changes.

Screens for administering Call Charge Information

Screen name	Purpose	Fields
Attendant Console	Assign a feature button for the attendant to display charges.	**Feature Button Assignments** area • **disp-chgs**
CDR System Parameters	Define Call Detail Recording (CDR) for the system.	All

Screen name	Purpose	Fields
Class of Restriction	Specify a Class of Restriction (COR) that allows the users to have charges displayed automatically.	**Automatic Charge Display**
DS1 Circuit Pack	Specify the values and the increments for Periodic Pulse Metering (PPM).	• **Received Digital Metering Pulse Maximum** • **Received Digital Metering Pulse Minimum** • **Received Digital Metering Pulse value**
Feature-Related System Parameters	Specify the frequency of the system displays for charge information.	**Charge Display Update Frequency**
Language Translations	Specify a translation of the "Call Charge" text display.	**Call Charge**
Station	Assign a feature button for the user to display charges.	**Feature Button** • **disp-chrg**
	Assign a COR for an automatic display of call charges.	**COR**
Trunk Group (all types)	Specify charge information that controls Call Charge Information processes and displays.	• **Charge Conversion** • **Charge Type** • **Currency Symbol** • **Decimal Point**

Screen name	Purpose	Fields
Trunk Group • central office (CO) • Direct inward and outward dialing (DIOD) • foreign exchange (FX) • Personal Central Office Line (PCOL) • Wide Area Telecommunications Service (WATS)	Administer PPM for a non-ISDN network.	• **CDR Reports** • **Direction** • **Frequency** • **Outgoing Glare Guard (msec)** • **PPM**
Trunk Group-ISDN-PRI	Administer Advice of Charge (AOC) for an ISDN network.	• **Charge Advice** • **Service Type** • **Supplementary Service Protocol** • **CDR Reports**

Administering the charge display

To administer the charge display, you must complete the following procedures:

- Administering a trunk group for call charge displays
- Assigning a call charge display button for a user
- Assigning a call charge display feature button for an attendant

Administering a trunk group for call charge displays

To administer a trunk group for call charge displays:

1. Type **change trunk-group *n***, where ***n*** is the number of the trunk group for which you want to administer call charge display information. Press **Enter**.

   The system displays the Trunk Group screen.

2. Click **Next** until you see the **Charge Conversion** field.

3. In the **Charge Conversion** field, type the charge unit for the currency that you use.

   Valid entries are **1** to **64,500**.

   The software multiplies the number of charge units by the value of the **Charge Conversion** field, and displays the result as a currency. If the **Charge Conversion** field is blank, the software displays the number of charge units, but does not convert the charge units to a currency.

   - The system displays the **Charge Conversion** field for central office (CO), direct inward and outward dialing (DIOD), foreign exchange (FX), and Wide Area Telecommunications Service (WATS) trunk groups when the **Direction** field on the Trunk Group screen is set to **outgoing** or **two-way**.
   - The system displays the **Charge Conversion** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not set to **none**.

4. In the **Charge Type** field, type the words or the characters that you want the system to display after the system displays the call charge amount.

   You can leave the field blank, or you can type one to seven characters. The system counts a leading space, or an embedded space, as a character.

   - The system displays the **Charge Type** field for CO, DIOD, FX, and WATS trunk groups when the **Direction** field on the Trunk Group screen is set to **outgoing** or **two-way**.
   - The system displays the **Charge Type** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not set to **none**.

5. In the **Currency Symbol** field, type the symbol that you want the system to display before the system displays the call charge amount.

   You can leave the field blank or you can type one to seven characters. The system counts a leading space, or an embedded space, as a character.

   - The system displays the **Currency Symbol** field for CO, DIOD, FX, and WATS trunk groups when the **Direction** field on the Trunk Group screen is set to **outgoing** or **two-way**.
   - The system displays the **Currency Symbol** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not set to **none**.

6. In the **Decimal Point** field, type the representation of a decimal point that is appropriate for your currency.

   You can type **comma**, **period**, or **none**.

   If you type **comma** or **period**, the system divides the call charge amount by 100.

   - The system displays the **Decimal Point** field for CO, DIOD, FX, and WATS trunk groups when the **Direction** field on the Trunk Group screen is set to **outgoing** or **two-way**.
   - The system displays the **Decimal Point** field for ISDN trunk groups when the **Charge Advice** field on the Trunk Group screen is not **none**.

7. Press **Enter** to save your changes.

Assigning a call charge display button for a user

To assign a call charge display button for a user:

1. Type **change station** *n*, where *n* is the extension of the user to whom you want to assign a call charge display feature button. Press **Enter**.

   The system displays the Station screen (Figure 92: Station screen on page 423).

Figure 92: Station screen

```
change station 1014                                          Page 1 of X
                              STATION

Extension: 1014               Lock Messages? n                    BCC: 0
     Type:                    Security Code:                       TN: 1
     Port:                  Coverage Path 1:                      COR: 1
     Name:                  Coverage Path 2:                      COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                          Message Lamp Ext: 1014
           Speakerphone: 2-way                   Mute button enabled? y
       Display Language? English                    Expansion Module?
                   Model:

 Survivable GK Node Name:                            Media Complex Ext:
                                                          IP Softphone? y
                                                   Remote Office Phone? y
```

2. In the **COR** field, type the number of the COR that supports the automatic display of call charges.
3. Click **Next** until you see the **Button Assignments** area (Figure 93: Station screen on page 424).

Figure 93: Station screen

```
change station 1014                                          Page   3 of 4
                                    STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                       Cord Length: 0
   Building:                                         Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                             7:disp-chrg
 2: call-appr                             8:
 3: call-appr                             9:
 4:                                      10:
 5:                                      11:
 6: headset                              12: release
```

4. In the **Button Assignments** area, type **disp-chrg** next to the feature button number that you want the user to use to display a call charge amount.
5. Press **Enter** to save your changes.

Assigning a call charge display feature button for an attendant

To assign a call charge display feature button for an attendant:

1. Type **change attendant *n***, where ***n*** is the number of the attendant console to which you want to assign a charge display feature button.

   The system displays the Attendant Console screen.
2. Click **Next** until you see the **Feature Button Assignments** area (Figure 94: Attendant Console screen on page 425).

Figure 94: Attendant Console screen

```
change attendant 1                                          Page 3 of 4
                              ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split_____                          13: disp-chrg_
  2: __________                          14: __________
  3: __________                          15: __________
  4: __________                          16: __________
  5: __________                          17: __________
  6: hold _____ *                        18: __________
  7: __________                          19: forced-rel
  8: aux-work      RC:    Grp:           20: __________
  9: __________                          21: __________
 10: __________                          22: __________
 11: __________                          23: night-serv *
 12: __________                          24: pos-busy__ *
```

3. In the **Feature Button Assignments** area, type **disp-chrg** next to the feature button number that you want the attendant to use to display a call charge amount.
4. Press **Enter** to save your changes.

Administering AOC for ISDN trunks

To administer Advice of Charge (AOC) for an ISDN trunk:

1. Type **add trunk-group *next***. Press **Enter**.

   The system displays the Trunk Group screen.
2. Click **Next** until you see the **Charge Advice** field.
3. In the **Charge Advice** field, perform one of the following actions:
   - If your public network sends AOC automatically, type **automatic**.
   - If the system must request charge information for each call, and you want to receive only the final call charge, type **end-on-request**.
   - If the system must request charge information for each call, and you want the system to display call charges both during the call and at the end of the call, type **during-on-request**.

   You can change this field from the default value of none, only if the **CDR Reports** field is set to **y**.
4. In the **Service Type** field, type **public-ntwrk**.

5. In the **Supplementary Service Protocol** field, type the supplementary service protocol that this trunk uses. Table 9: Supplementary service protocols on page 426 shows the valid entries for this field. You can type only one entry.

Table 9: Supplementary service protocols

Valid entries	Usage
a	National
b	ISO/ETSI QSIG Private Network. Also used for the separation of bearer and signaling (SBS) signaling trunks.
c	ETSI public network.
d	European Computer Manufacturer's Association (ECMA) QSIG private network. Supports only Name Identification and Additional Network Feature Transit Counter (ANF-TC).
e	Distributed Communications System (DCS) with Rerouting • Do not use this option if the **Service Type** field is set to **dmi-mos** or **sddn**. Set the **Used for DCS** field to **y**.
f	ISDN Feature Plus Public network feature plus signaling.
g	American National Standards Institute (ANSI). Available only if the **ISDN-PRI** field or the **ISDN-BRI** field on the Optional Features screen is set to **y**.

6. In the **CDR Reports** field, type the entry that provides the CDR information that you want for your system. Table 10: CDR report entries on page 426 shows the valid entries for this field.

Table 10: CDR report entries

Valid entries	Usage
y	All outgoing calls on this trunk group generate call detail records. If the **Record Outgoing Calls Only** field on the CDR System Parameters screen is set to **n**, incoming calls on this trunk group also generate call detail records.

Table 10: CDR report entries

Valid entries	Usage
n	Calls over this trunk group do not generate call detail records.
r	The system generates call detail records for both incoming and outgoing calls. The system also generates the following ringing interval call detail records: • Abandoned calls. The system creates a record with condition code *H*. Condition code *H* indicates the time until the call was abandoned. • Answered calls. The system creates a record with condition code *G*. Condition code *G* indicates the interval between when the call starts to ring and the user answers the call. • Calls to busy stations. The system creates a record with condition code *I*. Condition code *I* indicates a recorded call interval of zero.

7. Press **Enter** to save your changes.

Administering PPM for non-ISDN trunks

To administer Periodic Pulse Metering (PPM) for non-ISDN trunks:

1. Type **change trunk-group *n***, where ***n*** is the number of the trunk-group for which you want to administer PPM. Press **Enter**.

   The system displays the Trunk Group screen.

2. In the **CDR Reports** field, type the entry that specifies the circumstances under which you want the system to generate CDR report information. Table 11: CDR report entries on page 427 shows the valid entries for this field.

Table 11: CDR report entries

Valid entries	Usage
y	All outgoing calls on this trunk group generate call detail records. If the **Record Outgoing Calls Only** field on the CDR System Parameters screen is set to **n**, incoming calls on this trunk group also generate call detail records.

Table 11: CDR report entries

Valid entries	Usage
n	Calls over this trunk group do not generate call detail records.
r	The system generates call detail records for both incoming and outgoing calls. The system also generates the following ringing interval call detail records: • Abandoned calls. The system creates a record with condition code *H*. Condition code *H* indicates the time until the call was abandoned. • Answered calls. The system creates a record with condition code of *G*. Condition code *G* indicates the interval between when the call starting to ring and the user answers the call. • Calls to busy stations. The system creates a record with condition code *I*. Condition code *I* indicates a recorded call interval of zero.

3. In the **Direction** field, perform one of the following actions:
   - If you want this trunk to be used for incoming traffic, type **incoming**.
   - If you want this trunk to be used for outgoing traffic, type **outgoing**.
   - If you want this trunk to be used to network call redirection, type **two-way**.

   The system displays this field for all trunk groups except direct inward dialing (DID) and customer-premises equipment (CPE).

4. In the **Glare** field, type the minimum acceptable interval, in milliseconds, between the time that the server sends an outgoing seizure request and when the server receives a seizure acknowledgment. If the interval in which the server receives an acknowledgment is less than the interval that you specify in this field, glare is assumed. Valid entries are the numbers **40** to **100**, in increments of 10.

   Only TN2140 ports receive this timer.

   You can administer this field only if the **Trunk Type** field is set to **cont**, and the **Direction** field is set to **two-way** or **outgoing**.

5. In the **Frequency** field, type the PPM pulse frequency that the public network requires. Table 12: PPM pulse frequencies on page 429 shows the valid entries for this field.

   The system displays this field only if the **Direction** field is set to **outgoing** or **two-way**, and the **PPM** field is set to **y**.

Table 12: PPM pulse frequencies

Valid entries	Usage
12k	The TN465B, or later, circuit pack and the TN2184 circuit pack can detect only 12k and 16 kHz **PPM**. If you type **12k** in the **Frequency** field, the circuit pack is set to detect 12 kHz.
16k	The TN465B, or later, circuit pack and the TN2184 circuit pack can detect only 12k and 16kHz **PPM**. If you type **16k** in the **Frequency** field, the circuit pack is set to detect 16kHz.
50	The TN465B, or later, circuit pack and the TN2184 circuit pack can detect only 12k and 16kHz **PPM**. If you type **50** in the **Frequency** field, the circuit pack is set to detect 16kHz.
50/12k	The TN465B, or later, circuit pack and the TN2184 circuit pack can detect only 12k and 16kHz **PPM**. If you type **50/12k** in the **Frequency** field, the circuit pack is set to detect 12kHz.
50/16k	The TN465B, or later, circuit pack and the TN2184 circuit pack can detect only 12k and 16kHz **PPM**. If you set the **Frequency** field to **50/16k**, the circuit pack is set to detect 16kHz.

6. In the **PPM** field, type **y**.
7. Press **Enter** to save your changes.

Administering PPM for DS1 circuit packs

To administer PPM for DS1 circuit packs:

1. Type **`change ds1 n`**, where ***n*** is the number of the DS1 circuit pack for which you want to administer PPM. Press **Enter**.

   The system displays the DS1 Circuit Pack screen (Figure 95: DS1 Circuit Pack screen on page 430).

Figure 95: DS1 Circuit Pack screen

```
                              DS1 CIRCUIT PACK

            Location: ______                          Name: ____________
            Bit Rate: ______                    Line Coding: ____

      Signaling Mode: __________

        Interconnect: ____                Country Protocol: ______

Interface Companding: ____
           Idle Code: ____

              Received Digital Metering Pulse Minimum (ms):
              Received Digital Metering Pulse Maximum (ms):
                     Received Digital Metering Pulse Value:
      Slip Detection: __                  Near-end CSU Type: ______
                                                Block Progress Indicator? n
```

2. In the **Received Digital Metering Pulse Maximum (ms)** field, type the number that your network service provider recommends. Valid entries are **20** to **1000**, in increments of 10. The number that you type in this field must be greater than the number that you type in the **Received Digital Metering Pulse Minimum (ms)** field.

   The system displays this field only when the **Signaling Mode** field is set to **cas**, the **Interconnect** field is set to **co** or **pbx**, and the **Country Protocol** field is set to a protocol that uses PPM as defined in Table 13: Country protocol codes for incoming digital PPM signaling on page 431.

3. In the **Received Digital Metering Pulse Minimum (ms)** field, type the number the number that your network service provider recommends. Valid entries are **20** to **1000**, in increments of 10. The number that you type in this field must be less than the number that you type in the **Received Digital Metering Pulse Maximum (ms)** field.

   The system displays this field only when the **Signaling Mode** field is set to **cas**, the **Interconnect** field is set to **co** or **pbx**, and the **Country Protocol** field is set to a protocol that uses PPM as defined in Table 13: Country protocol codes for incoming digital PPM signaling on page 431.

4. In the **Received Digital Metering Pulse Value** field, type the number that your network service provider recommends. Valid entries are **1** and **2**.

   The system displays this field when the **Signaling Mode** field is set to **cas**, the **Country Protocol** field is set to **21**, and the **Interconnect** field is set to **co** or **pbx**.

Table 13: Country protocol codes for incoming digital PPM signaling

Code	Country	PPM Min. (ms)	PPM Max. (ms)	PPM value
0	null	NA	NA	NA
1	US	NA	NA	NA
2	Australia	80	180	0
3	Japan	NA	NA	NA
4	Italy	120	150	1
5	Netherlands	90	160	0
6	Singapore	NA	NA	NA
7	Mexico	20	180	1
8	Belgium	20	180	1
9	Saudi Arabia	NA	NA	NA
10	UK	NA	NA	NA
11	Spain	20	220	0
12	France	NA	NA	NA
13	Germany	NA	NA	NA
14	Czech Republic	20	420	1
15	Russia CIS	NA	NA	NA
16	Argentina	10	180	1
17	Greece	100	180	1
18	China	NA	NA	NA
19	Hong Kong	NA	NA	NA
20	Thailand	20	180	1
21	Macedonia Croatia	120 20	180 80	1 1

1 of 2

Table 13: Country protocol codes for incoming digital PPM signaling (continued)

Code	Country	PPM Min. (ms)	PPM Max. (ms)	PPM value
22	Poland	100	150	0
23	Brazil	NA	NA	NA
24	Nordic	NA	NA	NA
25	South Africa	160	240	0, 1
				2 of 2

5. Press **Enter** to save your changes.

End-user procedures for Call Charge Information

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Call Charge Information:

Displaying call charge information

To display call charge information:

1. Press the disp-chrg button before the call drops.

   If you press the:

   - Elapsed-timer button, the elapsed-timer information can overwrite part of the call charge information.
   - Local-directory-number button, the call charge information overwrites the directory number information.
   - Exit or Normal button, the directory number information no longer overwrites the local directory number information.

Considerations for Call Charge Information

This section provides information about how the Call Charge Information feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Charge Information under all conditions. The following considerations apply to Call Charge Information:

- Performance impact

  Call Charge Information can have an impact on system performance in several ways. The information that comes in over ISDN trunks takes up bandwidth, and reduces the maximum amount of traffic that the ISDN D-channel can handle. This is especially true in countries such as Germany and France, where the network sends charging information updates as often as every 3 to 10 seconds for each active international call.

  The number of telephones that display charge information and the frequency of updates also affect performance. Usually, the update frequency matches the average rate at which call charge updates are received from the public network.

  CAUTION:
  When users update displays too frequently, unnecessary system performance degradation can occur. If performance slows to an unacceptable rate, you can lengthen the amount of time between updates.

Interactions for Call Charge Information

This section provides information about how the Call Charge Information feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call Charge Information in any feature configuration.

- Attendant Features

  Attendant consoles cannot have an automatic charge display. If you want the attendant to see call charges, you must assign a disp-chrg button to the attendant console. If the attendant transfers an outgoing call, the display returns to normal mode. If the transfer is not completed, or the call remains at the attendant console, the attendant must press the disp-chrg button again to view call charges.

- Automatic Incoming Call Display

  If a user has charges displayed for an existing call, and a second call rings on another line appearance, the display returns to normal mode for a short time to show the identity of the caller. The user must press the disp-chrg again to view call charges. Or if automatic charge display is enabled, the user must wait for the Charge Display Update Frequency interval to expire.

- Bridged Appearance

  If a user uses a bridged call appearance to place a call, the system displays the call charges on the telephone from which the call is made. If Automatic Charge Display is part of the Class of Restriction (COR) for that telephone, the system displays the charges automatically. The system displays the actual charge for the call on the Call Detail Recording (CDR) report as if the call was made from the principal extension, and not from the bridged appearance.

- Call Coverage or Call Forwarding

  Call charges for a call to an extension that the system redirects over a public network trunk, are charged to the called extension, not the calling extension. However, if the call is placed from an internal telephone that has charge display capability, the caller sees the charges for the redirected call.

- Call Park

  When a user parks a call, the display mode returns to normal. If a user retrieves a parked, outgoing call from another display telephone, the display on that set shows the current call charges if the user presses the disp-chrg button. The display also shows the charges if the Class of Restriction (COR) of the user allows Automatic Charge Display. If call splitting is enabled, the display shows the charges that accumulated since the user unparked the call.

- Call Transfer

  Advice of Charge (AOC) administration for the outgoing trunk group controls whether AOC information is requested or recorded for the call, when the system routes a transferred call over a public network ISDN-PRI trunk group. If two or more outgoing trunks are connected through trunk-to-trunk transfer, the software can receive AOC information from the network for each outgoing trunk that is involved in the call.

- Call Detail Recording (CDR) Adjuncts

  The software does not tandem AOC information through a private network to other switches. The CDR adjunct that records AOC information must receive its input from software that is directly connected to the public network.

- CDR Call Splitting
  - The system generates a separate call record, whenever the system transfers a call, if you administered CDR Call Splitting for outgoing trunks.
  - Attendant Call Recording, which is a form of Call Splitting, generates a CDR record when an attendant drops from a call.
  - Incoming Trunk Call Splitting has no effect on charge information.
  - If you rely on Call Splitting or Attendant Call Recording, request call charge information during the call. However, if you use AOC, a request for call charge information during a call increases message activity on the signaling channel, and reduces Busy Hour Call Capacity.

  - In some countries, or with specific protocols, AOC information is unavailable during a call. If AOC information in unavailable during a call, you can use the Elapsed Time in the CDR records to allocate the charges among the call participants.
  - You must use CDR Call Splitting if you want the charge display to restart at zero when a call is transferred.

- Centralized Attendant Services

  In any configuration where a branch system has no direct connection to the public network, the private network does not pass call-charge information to these branches.

- Conference

  If a user adds a third party to a call that is in charge-display mode, the display returns to normal. The system does not display call charges when more than two parties are on the call.

- Distributed Communications System (DCS)

  In any configuration where a branch system has no direct connection to the public network, the private network does not pass call-charge information to these branches.

- Electronic Tandem Network (ETN)

  In any configuration where a branch system has no direct connection to the public network, the private network does not pass call-charge information to these branches.

- Hold

  If a user places a call on hold, the display returns to normal mode. The user must press the disp-chrg button again to view call charges. If the automatic charge display is enabled, the user must wait for the system to refresh the display.

- Last Number Dialed

  When a user is active on a call, a user can view the last number that the user dialed. To view the last number that was dialed, the user presses the stored-numb button, and then presses the
  last-numb button. To view call charges again, the user must press the disp-chrg button, or the Normal button if Automatic Charge Display is part of the COR of the user.

- QSIG

  In any configuration where a branch system has no direct connection to the public network, the private network does not pass call charge information to these branches.

- System resets

  If you perform a warm reset while calls are active with charge display, the charge display stops operating. To resume call charge updates, users must press the Normal button.

Call Coverage

Use the Call Coverage feature to automatically reroute incoming calls to alternate telephone numbers.

Detailed description of Call Coverage

This section provides a detailed description of the Call Coverage feature.

Use Call Coverage to:

- Reroute incoming calls to alternate telephone numbers when the called party is unavailable to answer calls
- Establish the order in which calls are redirected to alternate destinations
- Establish up to six alternate destinations for an incoming call
- Establish redirection criteria that govern when the system redirects a call
- Establish multiple coverage paths that the system can select from based on redirection criteria
- Redirect calls based on the time of day
- Redirect calls to a local telephone number or to a telephone number in the public network
- Allow users to change their lead coverage path from both onsite and off-site locations

When a call meets the redirection criteria for a called telephone number, the system attempts to route the call sequentially to one of the points in a coverage path. Users can have a maximum of six points in the coverage path. If no coverage points are available, the call might revert to the original called number. If any point in the path is available, the call either rings at the individual telephone, an available member of a coverage group, or queues to the coverage group. Once a call is ringing or queued at any point in a coverage path, the call neither reverts to the original number, nor to the previous coverage point.

A call continues to ring at a coverage point for the interval that is administered for Coverage Subsequent Redirection. At the end of this interval, the system attempts to route the call to any points that remain in the coverage path. If no other point is available to accept the call, the call remains queued, or continues to ring at the current coverage point.

What is a Call Coverage path?

A call coverage path is a list of one to six alternate answering positions. The system sequentially accesses the coverage points when the called party or the called group is unavailable to answer the call.

When a call meets the redirection criteria for a called telephone number, the system attempts to route the call sequentially to one of the points in a coverage path. Users can have a maximum of six points in the coverage path. If no coverage points are available, the call might revert to the original called number.

You can assign a coverage path to any of the following entities:

- An automatic call distribution (ACD) split
- An agent login ID
- A personal central office line (PCOL) group
- A Terminating Extension Group (TEG)
- A hunt group
- A telephone that can be either on site or off site

You define the coverage paths and establish the redirection criteria. You can include any of the following entities as points in a coverage path:

- A telephone number
- A voice messaging system
- An announcement
- An attendant group
- A uniform call distribution (UCD) hunt group
- A direct department calling (DDC) hunt group
- An ACD hunt group
- A coverage answer group (CAG)
- A vector directory number (VDN)

Multiple coverage paths

The system can select from multiple coverage paths that you define for a single destination. However, the system uses only one coverage path per call. The system first considers *Coverage Path 1*, the lead coverage path, when the system directs a call to coverage.

When the system redirects a call to coverage, the system checks the lead coverage path to determine whether the coverage redirection criteria of the path match the call status. If the criteria match, the system uses the lead coverage path. If the redirection criteria of the lead coverage path does not match, the system moves in sequence from point to point in the coverage path to find a coverage path with redirection criteria that matches the call status. If the system does not find a match, the call remains at the called extension. Once the system selects a coverage path, that path is used throughout the duration of the call.

Call Coverage supports the following capabilities:

- Call Coverage

  The system reroutes incoming calls to alternate telephone numbers when the called party is unavailable to answer calls.

- Call Coverage Off Network

  You can administer and use an external number in a coverage path. The system can monitor the call to determine whether the external number is busy or does not answer. If necessary, the system can redirect a call to coverage points that follow the external number.

- Call Coverage Time of Day

  You can administer the redirection of calls to different lead coverage paths based on the day of the week and the time of day.

- Call Coverage Changeable Coverage Paths

  Users can use a Feature Access Code (FAC) to modify coverage points.

- Consult

  Users can answer a coverage call, and then communicate with the called user without the caller hearing the conversation.

- Extended User Administration of Redirected Calls

  Users can change their lead coverage path from both onsite and off-site locations.

Time-of-Day Coverage

Use the Time-of-Day Coverage capability to redirect calls to different lead coverage paths at different times of the day, and on different days of the week.

For example, a user might want incoming calls to go to coverage based on the following schedule:

- To a co-worker at the office during normal business hours
- To an off-network destination, such as home, in the early evening
- To a voice messaging, such as CM Messaging, at all other times

To provide the user with the requested coverage, you administer the information in Table 14: Example of a Time-of-Day coverage table on page 440.

Table 14: Example of a Time-of-Day coverage table

Day of the week	Time 1 directed to	Time 2 directed to	Time 3 directed to	Time 4 directed to
Monday	00:00 CovPath3 (CM Messaging)	08:00 CovPath1 (Office)	17:30 CovPath2 (Home)	20:00 CovPath3 (CM Messaging)
Tuesday	00:00 CovPath3 (CM Messaging)	08:00 CovPath3 (Office)	17:30 CovPath3 (Home)	20:00 CovPath3 (CM Messaging)
Wednesday	00:00 CovPath3 (CM Messaging)	08:00 CovPath1 (Office)	17:30 CovPath2 (Home)	20:00 CovPath3 (CM Messaging)
Thursday	00:00 CovPath3 (CM Messaging)	08:00 CovPath3 (Office)	17:30 CovPath3 (Home)	20:00 CovPath3 (CM Messaging)
Friday	00:00 CovPath3 (CM Messaging)	08:00 CovPath1 (Office)	17:30 CovPath2 (Home)	20:00 CovPath3 (CM Messaging)
Saturday	00:00 CovPath3 (CM Messaging)			
Sunday	00:00 CovPath3 (CM Messaging)			

The Time-of-Day Coverage table represents time in 24-hour format. Activation times are ascending from the earliest to the latest. The activation times cover the entire day. If you do not assign a lead coverage path to a specific time interval, no coverage exists from that time until the next activation time.

When a call arrives at an extension, the system determines the lead coverage path that is in effect at that time. The system uses the information to redirect the call. If you change call coverage for a user while the user has a call in progress, your changes do not affect the call in progress.

Off-network Call Coverage

You can use standard remote coverage to an external number to send a call to an external telephone. However, the system does not monitor the call once the call leaves your system. Therefore, if the call is busy or not answered at the external number, the call cannot be directed back to the system.

The Coverage of Calls Redirected Off Net (CCRON) capability, however, allows you to use an external number in a coverage path. The system monitors the call to determine whether the external number is busy or unanswered. If necessary, the system can redirect a call to coverage points that follow the external number. Any coverage point can be an off-network destination.

This capability allows a call to follow a coverage path that:

1. Starts at the called extension
2. Redirects to the home telephone, and if unanswered at home
3. Returns to the voice mail box of the called extension

Note that the call does not return to the system if the external number is the last point in the coverage path, except when no trunks are available to route the call. In that case, the system attempts to again terminate the call at the original called extension.

When the system redirects an incoming trunk call off the network, a timer is set. The timer prevents the system from redirecting other incoming trunk calls from redirecting off the network until the timer either expires or is cancelled. The timer prevents calls that were redirected off the network from being routed back to the original telephone number from the off-network destination. Calls that are routed back to the original telephone number in this situation effectively create a loop that seizes trunks until trunks are no longer available.

The system provides the means to perform call classification on an off-network coverage call to determine the disposition of the call. If the off-network call is carried completely over ISDN facilities to the final destination, ISDN trunk signaling is used to monitor the call. If ISDN trunk signaling is not used to monitor the call, a call classifier port is used to cancel the call.

When the system tries to use a call classifier port to classify an off-network coverage call, the system introduces an unavoidable cut-through delay while the call classifier port attempts to identify an answered call. Neither the originating party nor the answering party hears each other during the 1-second or less delay. A call classifier is attached to all off-network coverage calls, that are made over analog facilities or over ISDN facilities, if the call is interworked to non-ISDN facilities on the public network.

When you enable CCRON:

- The system monitors off-network calls and returns the calls to the system if the calls are not answered within the administered time interval. Calls also return to the system if the system detects a call progress tone, such as busy or reorder.
- A simulated bridge appearance (SBA) is put on the called extension, and the green lamp flashes. A user can answer the call at the called extension at any time.

- When the system uses a call classifier port to classify the call, the system plays local ringback tone to the caller while the system is classifying the off-network call. The system uses the local ringback tone so that the user does not hear what is happening on the public network. As a result, the calling party might not hear the first few syllables that the answering party speaks.
- If any party on the call is on hold when the system routes the call off the network, the call classifier is removed from the call. The call behaves as if CCRON is not enabled.
- While an off-network call is undergoing call classification, any party that is not already on the call cannot bridge onto the call. Also, the originating party cannot release the call, conference anyone else onto the call, or transfer the call to a new party. Once the call is answered at an off-network destination, or the call is returned to the system for further call processing, these restrictions are removed.
- If the last point in a coverage path is an off-network destination and no trunks are available to route the call, the system attempts to again terminate the call to the called extension.
- The system has no control over any redirection of the call that might take place at an off-network destination. However, further coverage treatment is provided if the off-network redirection interval expires before the call is answered at an off-network destination.

Call Coverage changeable coverage paths

With the changeable coverage path capability, users can use a Feature Access Code (FAC) to modify coverage paths.

Extended User Administration of Redirected Calls

The Extended User Administration of Redirected Calls capability allows users to change the lead coverage path or the call forwarding destination from any onsite or off-site location. This capability is also known as remote access. For more information, see the Remote Access feature.

Call coverage criteria

Coverage criteria determine the conditions when the system redirects a call from the called extension to the first position in the coverage path. The Call Coverage feature provides the following coverage criteria:

- Active

  Redirects calls to coverage immediately when the called extension is active on at least one call appearance. For a telephone with only one appearance or a single-line extension, assign the Busy criterion instead of the Active criterion.

- Busy

  Redirects calls to coverage when all available call appearances at the called extension are in use.

  The system redirects an incoming call, other than a priority call, to coverage only when all call appearances are in use.

  A TEG is considered busy if any telephone in the group is active on a call.

  Each telephone in a UCD group or a DDC group must be active on at least one call appearance for the system to redirect a call to coverage. If any telephone in the group is idle, the system directs the call to the idle telephone. If no telephone is available, the call can queue, if queuing is provided. If queuing is not provided, the system routes the call to coverage. If the queue is full or all agents are in an AuxWork mode, the system routes the call to coverage. Queued calls remain in the queue for the specified interval.

  A call does not cover to a hunt group if no agents are logged in, or if all agents are in AuxWork mode.

- Don’t Answer

  Redirects calls to coverage if the calls are unanswered during a specified interval. A call rings for the specified number of seconds, and then the system redirects the call to coverage.

- Cover All Calls

  Redirects all incoming calls to coverage. This criterion has precedence over any other previously assigned criterion.

- Send All Calls/Go to Cover

  Allows users to activate Send All Calls or Go to Cover as overriding coverage criteria. You must assign this redirection criteria before a user can activate Send All Calls or Go to Cover.

- No Coverage

  Occurs when no coverage criteria are assigned. The system redirects calls to coverage only when the call extension activates Send All Calls, or the caller activate Go to Cover.

You can combine Active/Don’t Answer and Busy/Don’t Answer coverage criteria. Other combinations are either not possible or not useful.

You assign redirection criteria separately for internal and external calls. You can link coverage paths so that you can assign Busy Don’t Answer for internal calls, and Active for external calls. Similarly, you can assign Busy/Don’t Answer for external calls, and No Coverage for internal calls. When you assign No Coverage for internal calls, internal calls remain directed to the called telephone or the called group.

All calls that are extended by the attendant are treated as external.

Enhanced Redirection Notification

The redirection features available in Communication Manager Release 5.2 include Do Not Disturb, Send All Calls, and Call Forwarding. In Communication Manager Release 5.2, the activation of redirection features at a user's station is indicated through visual display or through a special dial tone (if the station is not equipped with a display). This feature works on DCP and IP (H.323) telephones, but not on IP (SIP) telephones and attendant consoles.

Description

Enhanced Redirection Notification allows display of the status of redirection features, selected posted message, and date and time information.

- Do Not Disturb
- Send All Calls
- Call Forward
- Selected Posted Message
- LNCC
- Enhanced Call Forward
- Station lock

If there are multiple status messages, the active features are displayed on scrolling, in the order of decreasing priority. The date and time information is displayed at the end of the loop and has the lowest priority, but is displayed for twice as long as any of the other status messages. If **Scroll Status messages Timer (sec.)** is set to blank, scrolling is disabled, and only the feature with the highest priority is displayed. When no feature is active, only the date and time information is displayed. To guard against loading the system with status messages, the scrolling is started randomly. For example, when the user releases the handset for the first time.

Note:
After activation or deactivation of the feature, the display might remain unchanged until the first user interaction, such as going on-hook.

Limitations

Enhanced Redirection Notification applies only when a station is idle and in normal display mode (not displaying a crisis alert or directory.) Enhanced Redirection Notification does not work if ringing is prevented at the station through use of **Silent Ringing**, **Ringing Abbreviated/ Delayed**, or **Per Button Ring Control**. If the redirection number to be displayed does not fit into the display because the number is too long(18 digits or more), the standard scroll applies.

VDN in a call coverage path (VICP)

If you assign a vector directory number (VDN) extension as the last point in a call coverage path, you apply call vectoring functionality to the coverage point. The programmable vector that is associated with the VDN provides flexibility in call handling.

You can program a vector that is assigned to the VDN in the coverage path to queue a redirected call to a messaging split for call answer operation, and to allow the caller to leave a message at the called extension. The same VDN can also be used to retrieve messages. You can also vary the vector program by split status or time-of-day to provide different types of coverage.

When a redirected call covers to a VDN, the simulated bridged appearance of the called extension is removed when vector processing starts.

When covered calls or direct calls are connected to CM Messaging or to a messaging split through call vectoring, both the original reason for redirection and the called extension must be passed to the adjunct over the Switch Communication Interface (SCI) link.

Use of a VDN as a coverage point provides integration to Centralized Messaging. That is, the distributed communication system (DCS) message that is sent to the remote switch with CM Messaging includes the original reason for redirection and the called extension.

Coverage answer groups

You can create coverage answer groups that allow two to eight telephones to ring simultaneously when calls are redirected to the group. Anyone in the answer group can answer the incoming call.

Announcement in a coverage path

In general, do not assign an announcement as a point in a coverage path. When the system redirects a call to an announcement, the system plays the announcement and then drops the call. The system drops the call even if there are additional points in the coverage path.

You might want to use an announcement as the last point in a coverage path. The announcement could inform the caller that there is no one to answer the call and advise the caller to call back at another time. Keep in mind that the system drops the call once the system plays the announcement.

Hunt group in a coverage path

You can assign call coverage for a hunt group. If a hunt group queue is full, a call waits for a specified interval,. The system then directs the call to the coverage path. The call coverage point can be another hunt group. A call does not cover to a hunt group if no agents are logged in, or if all agents are in AuxWork mode.

Subsequent redirection interval

The subsequent redirection interval controls the number of times that a call rings at a coverage point before the call moves to the next coverage point. The number of rings that the interval control depends on the type of coverage point. For example, the number of rings is different at a local coverage point and a remote coverage point.

Notifying users when the calls are redirected

You can administer a setting that notifies users when the users have a capability active that might redirect the calls. For example, if send all calls or call forwarding is active for a user, you can administer a setting to play a special dial tone when the user goes off hook.

Caller response interval

The system uses a single, short tone, called a "redirect" tone, to inform an internal calling party (including incoming trunk calls from DCS and QSIG-VALU trunk groups) that the system is redirecting a call to coverage. The redirect tone is followed by an optional period of silence, called the Caller Response Interval. This interval allows the calling party time to decide whether to:

- Hang up
- Activate Priority Calling (this overrides coverage and re-rings the called party with a special ringing tone)
- Activate Leave Word Calling (LWC)
- Activate Automatic Callback
- Activate Go to Cover (this cancels the remaining Caller Response Interval and rings the first available coverage point)

Note that each of the above features except Go To Cover is available both locally on a single server, as well as over DCS and QSIG-VALU. The ability for the calling party to hear the redirect tone does not require the optional feature "DCS Call Coverage"; it is part of basic DCS.

Administer the redirect tone on page 2 of the Tone Generation screen (**change tone-generation**) by selecting **redirect** in the **Tone Name** field.

Note:
If the majority of the calls on your system go directly to voice mail without first covering to another party, and if features such as Leave Word Calling, Automatic Callback, Go To Cover, and Priority Calling are rarely used, it is advisable to reduce the length of this interval from its default value of 4 seconds, since this timer increases the delay before the voice mail system answers the call.

Consult

When a user answers a coverage call, the user can communicate with the called user without the caller hearing the conversation. This is called *private consultation*. To consult privately with the called user, the covering user presses the Transfer button, and then the Consult button. When the covering user presses the Transfer button, and then the Consult button, the system places the caller on hold. The system then establishes a connection between the called user and the covering user.

The covering user can create a conference call between the called user, the covering user, and the caller.

The covering user can transfer the call back to the called user.

The system maintains a Consult call at a Temporary Bridged Appearance, if a Temporary Bridged Appearance is available. If a Temporary Bridged Appearance is unavailable, the system uses any idle call appearance for the Consult call. If an idle call appearance is unavailable, the system denies the Consult call.

Limit number of Concurrent Calls

Beginning with Communication Manager Release 4.0 or later, you can use the Limit Number of Concurrent Calls (LNCC) feature to restrict the number of calls that can terminate on an active multi-appearance terminal to one call.

A typical CM digital/IP station has three call appearances. The first two call appearances are for receiving incoming calls, and, if the first two call appearances are active, the last one can be reserved for call origination or receiving priority, provided the **Restrict Last Appearance** field on the Station screen is set to **y**. With the LNCC feature enabled, and the user on a call, subsequent incoming calls receive a busy signal.

The LNCC feature does not restrict outgoing calls, incoming priority calls, 911 emergency callback and crisis alert button activation. The LNCC feature applies to station directed calls only. That is, if LNCC is activated on a station by a logged in agent, LNCC will still be active on the station after the agent logs off.

The LNCC feature is considered to be part of the station's attributes and is saved as part of the station record by a save translations. Subsequent resets will restore the LNCC state to what it was when the save translations was executed.

The feature is activated and deactivated by a new feature button (**limit-call**), or by using two new Feature Access Codes (Limit Number of Concurrent Calls Activation/Deactivation). The **limit-call** button indicates whether the LNCC feature is active or not.

Enhancements to LNCC

In Communication Manager Release 5.2, a call to a station that is LNCC-busy is treated like a normal busy station. The call follows the call coverage path for the busy status in the following conditions:

- A station that has LNCC activated will follow a coverage path. The user does not hear a busy tone. The coverage path can be administered.
- The call hunts for a station per the administered coverage path if LNCC is activated in ***Hunt to Station*** mode.

To administer or view the coverage path for LNCC-busy, use the **change coverage path** ***n*** command or the **display coverage path** ***n*** command, where *n* indicates the number of the coverage path assigned to the station. For more information, see Creating a coverage path on page 454.

To administer or display the hunt-to station, use the **change station** or **display station** command.

Features that override Call Coverage

Some features override Call Coverage criteria. The system checks the criteria of the overriding features before the system checks the coverage criteria. The following features override Call Coverage:

- Call Forwarding All Calls

  Call Forwarding All Calls temporarily overrides the redirection criteria if Send All Calls is not active. The system attempts to complete the call at the forwarded-to extension before the system redirects the call to coverage. If the redirection criteria of the called extension are met at the forwarded-to extension, the system redirects the call to the coverage path of the called extension.

- Go to Cover

  Users can use Go to Cover to send a call directly to coverage, when the users call an internal extension. The internal calling party activates Go to Cover, and can assign Go to Cover to a telephone.

- Send All Calls

  Users can use Send All Calls to temporarily direct all incoming calls to coverage, regardless of the coverage criteria that are assigned to their extension. The feature also allows users to temporarily remove their telephones from the coverage path of another user.

  A user cannot activate Send All Calls, if Send All Calls is not included in the coverage criteria of the extension.

  Send All Calls does not affect TEG calls.

- Send Term

  Send Term is the TEG equivalent of Send All Calls. Since a TEG cannot be in a coverage path, Send Term applies only to a TEG that is called directly.

Conditions that override Call Coverage

Call Coverage redirects calls from the called extension or the called group to alternate answering positions when certain criteria are met. Sometimes calls are sent back to the called extensions or the alternate destination, even though the redirection or overriding criteria are met.

The following list contains the conditions that cause the system to override Call Coverage.

- If no answering positions are available in the overage path, the call rings at the called telephone, if possible. If the call cannot ring at the called telephone, the calling party receives busy tone. The calling party receives busy tone, even if the Cover All Calls redirection criterion or the Send All Calls overriding criterion is active.
- If the system redirects a call to a coverage point that is unavailable, the call goes to the next coverage point. The call goes to the next coverage point, regardless of the type of coverage that is administered in the coverage point that is unavailable.

- When UCD and DDC group members are unavailable to answer calls to the group, the calls go to a queue, if queuing is available. The call remains in the queue for the call response interval before the system routes the call according to the coverage path. If no points on the path are available, the call remains in the queue. When neither group queuing nor a coverage point is available, the caller receives a tone or ringback, depending on the type of trunk that carries the call.

  If the redirection criterion is Active or Cover All Calls, a called extension can receive a redirection notification signal when the system routes the call to coverage. The redirection notification signal is a short burst of ringing. You can administer the redirection notification signal option for any extensions in your system.

  Redirected calls maintain an appearance on the called telephone, if possible. The call appearance status lamp flashes to indicate an incoming call before the system attempts to redirect the call. When the system redirects the call, the status lamp continues to flash. If the system redirects the call to CM Messaging, the lamp goes out. If the call appearance is flashing, a user presses the call appearance button to answer the call. If a covering user answers the call, the called user can bridge onto the call. If a covering user answers the call, the status lamp on the telephone of the called user lights steadily.

- Telephone users use Directed Call Pickup to answer calls that ring at another telephone or calls that alert at a coverage point. A call alerts when a call causes a call appearance on the telephone to flash. Directed Call Pickup allows a user to answer an alerting call from any telephone on the system.
- The system routes the following types of calls to the telephone of the called user until the user activates Go to Cover:
  - Priority calls
  - Dial Intercom calls
  - Automatic Intercom calls

  The system gives these calls precedence over the redirection criteria, and seizes the call appearance that is usually reserved for outgoing calls, if no other call appearances are available.

Administering Call Coverage

The following steps are part of the administration process for the Call Coverage feature:

- Creating a coverage path
- Assigning a coverage path to a user
- Assigning a Consult button for a user
- Defining coverage redirected off-network calls

- Assigning the telephone numbers for the off-network coverage points
- Administering the coverage path for redirected off-network calls
- Assigning time-of-day coverage
- Creating a coverage answer group
- Assigning Internal Alerting
- Enabling enhanced Redirection Notification

This section describes:

- Any prerequisites for administering the Call Coverage feature
- The screens that are required to administer the Call Coverage feature
- Complete administration procedures the Call Coverage feature

Prerequisites for administering Call Coverage

You must complete the following actions before you can administer the Call Coverage feature:

- Ensure that Feature Access Codes (FACs) for activating and deactivating Send All are available on your system, if you want users to use an FAC for these capabilities.

To ensure that FACs for activating and deactivating Send All are available on your system:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen.

2. Click **Next** until you see the **Send All Calls Activation** field (Figure 96: Feature Access Code (FAC) screen on page 452).

Figure 96: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 3 of 7
                            FEATURE ACCESS CODE (FAC)

                  Priority Calling Access Code:
                           Program Access Code:
       Refresh Terminal Parameters Access Code:
              Remote Send All Calls Activation:       Deactivation:
              Self Station Display Access Code:
                     Send All Calls Activation:       Deactivation:
         Station Firmware Download Access Code:
                       Station Lock Activation:       Deactivation:
      Station Security Code Change Access Code:
              Station User Admin of FBI Assign:                 Remove:
  Station User Button Ring Control Access Code:
                          Telephone Activation: #*
             Terminal Dial-up Test Access Code:
Terminal Translation Initialization Merge Code:       Separation Code:
            Transfer to Voice Mail Access Code:
          Trunk Answer Any Station Access Code:
              User Control Restrict Activation:       Deactivation:
  Voice Coverage Message Retrieval Access Code:
 Voice Principal Message Retrieval Access Code: *80
```

3. Type an FAC in the **Send All Calls Activation** field.
4. Type an FAC in the **Send All Calls Deactivation** field.

   For more information, see the "Feature Access Code" feature.
5. Press **Enter** to save your changes.

Screens for administering Call Coverage

Screen Name	Purpose	Fields
Call Coverage Answer Group	Establish answer groups.	All
Coverage Path	Establish points in the coverage path.	All
Feature Access Code	Assign Feature Access Codes (FACs) to activate or deactivate coverage-related actions.	• **Send All Calls Activation** • **Send All Calls Deactivation**

Screen Name	Purpose	Fields
Hunt Groups	Establish groups of users who answer calls for each other.	All
Remote Call Coverage Table	Assign the telephone numbers of remote coverage points.	All
Station	Define coverage information and button assignments for the called user.	• **Coverage Path 1** • **Coverage Path 2** • **Redirect Notification** • **Button Assignments for goto-cover and send-calls**
	Define button assignments for the user to whom the system redirects the call.	Button assignments for do not disturb (**dn-dst**), go to cover (**goto-cover**), and send all calls (**send-calls**)
	Define the goto-cover coverage point.	Button Assignment for **goto-cover**
System-Parameters Call Coverage/Call Forwarding	Enable the Call Coverage Off-Net capability.	**Coverage of Calls Redirected Off-Net Enabled**
System-Parameters Features	Enable Enhanced Redirection Notification.	REDIRECTION NOTIFICATION fields
Optional Features	Verify that the CCRON capability is allowed in your system.	**Cvg of Calls Redirected Off-Net**
Terminating Extension Group	Define the group of users who can answer a call that simultaneously alerts at the telephones of the group members.	All
Time of Day Coverage Table	Assign coverage throughout the day and week.	All
Trunk Group: • APLT • ISDN-PRI • Tie	Specify the internal ringing and call coverage used for incoming trunk calls.	**Internal Alert?**

Creating a coverage path

Prerequisites

You must complete the following actions before you can create a coverage path:

- Verify that the settings on the System-Parameters Call Coverage/Call Forwarding screen contain the values that you want for your system. For basic Call Coverage, Avaya recommends that you not change the default settings. However, if you decide to change the default settings, read the field definitions and the field descriptions carefully before you make changes.

  To view this screen, type **`display system-parameters call coverage/call forwarding`**. Press **Enter**.

  For a complete description of the System-Parameters Call Coverage/Call Forwarding screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

To create a coverage path:

1. Type **`add coverage path next`**. Press **Enter**.

   The system displays the Coverage Path screen (Figure 97: Coverage path screen on page 455), that shows the next undefined coverage path. The **Coverage Path Number** field is a display-only field. The total number of coverage paths cannot exceed 600.

Figure 97: Coverage path screen

```
                               COVERAGE PATH

                 Coverage Path Number: 14
                                                 Hunt after Coverage? n
                     Next Path Number:           Linkage

COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
              Active?             n               n
                Busy?             y               y
       Don't Answer?              y               y         Number of Rings: 2
                 All?             n               n
 DND/SAC/Goto Cover?              y               y

COVERAGE POINTS

    Terminate to Coverage Pts. with Bridged Appearances? n

  Point1: 4101      Rng: 3  Point2:                   Point3:
  Point4:                   Point5:                   Point6:
```

2. To see the extensions or the groups that use a specific coverage path, type **display coverage sender group *n***, where ***n*** is the coverage path number. For example, you might want to see which extensions use a coverage path before you make changes to the coverage path.
3. In the **Hunt After Coverage?** field, type **y** if you want the system to attempt station hunting from the last coverage point, when the coverage point is a busy station. If you do not want the system to attempt station hunting from the last coverage point when the coverage point is a busy station, leave the default set to **n**.
4. In the **Next Path Number** field, perform one of the following actions:

- Type a coverage path number in the field if you want the system to redirect if the coverage criteria of the current path does not match the call status. If the coverage criteria of the next path matches the call status, the system uses the coverage criteria to redirect the call, and no other path is searched.
- If you do not want the system to redirect the call, leave the field blank.

  Linkage is a display-only field that shows one or two assigned coverage paths that are linked to the number in the **Next Path Number** field.

5. Find the **Coverage Criteria** area. Note that there is a column for inside calls and a column for outside calls. You can accept the defaults for both columns or only one column. Likewise, you can change the defaults for both columns or only one column. Perform any of the following actions:
   - In the **Active?** fields, perform one of the following actions:

- Accept the default **n,** if you *do not* want the call to go to coverage if only one call appearance is busy.
- If you want the call to go to coverage if only one call appearance is busy, type **y**.

- In the **Busy?** fields, perform one of the following actions:
  - Accept the default **y,** if you want the call to go to coverage if the extension is busy.
  - If you *do not* want the call to go to coverage if the extension is busy, type **n.**
- In the **Don't Answer?** fields, perform one of the following actions:
  - Accept the default **y**, if you want the call to go to coverage if the number of rings exceeds the number specified in the **Number of Rings** field.
  - If you *do not* want the call to go to coverage if the number of rings exceeds the number specified in the **Number of Rings** field, type **n**.
- In the **Number of Rings** field, type a number from **1** to **99.** This number indicates the number of times a call rings at a telephone before the system redirects the call to the first coverage point. The default is **2**.
- In the **All?** fields, perform one of the following actions:
  - Accept the default **y**, if you want the users with this path to answer their own calls.
  - If you *do not* want the users with this path to answer their own calls, type **n**.If you type **n**, the users can never answer their own calls. These user calls always immediately go to coverage.
- In the **DND/SAC/Goto Cover?** fields, perform one of the following actions:
  - Accept the default **y**, if you want users to activate Send All Calls, temporarily direct all incoming calls to coverage (regardless of the assigned Call Coverage redirection criteria), and to temporarily remove their telephone from the coverage path.
  - If you *do not* want users to activate Send All Calls, temporarily direct all incoming calls to coverage (regardless of the assigned Call Coverage redirection criteria), and to temporarily remove their telephone from the coverage path, type **n**.
- In the **Terminate to Coverage Pts. with Bridged Appearance?** field, perform one of the following actions:
  - Accept the default **n**, if you want a call to skip the coverage point if the call has already alerted as a bridged call.
  - Type **y** to allow a call to alert as a bridged call and a redirected call.

6. In the **Point** fields, type the extensions, the hunt group number, or the coverage answer group numbers that you want for coverage points. When you type a number and move to the next **Point** field, the system displays the **Rng** field.
   - In the **Ring** field, perform one of the following actions:
     - If you want to use the number of rings entered in the **Number of Rings** field, leave the **Rng** field blank.

– If you *do not* want to use the number of rings entered in the **Number of Rings** field, type the number of rings for this coverage point.

Note:
To enter an extension that is assigned as a vector directory number (**VDN)** as the last point in the coverage path, you must make an administration change. For more information, see *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.

7. Press **Enter** to save your changes.

Assigning a coverage path to a user

Prerequisites

You must complete the following actions before you can assign a coverage path:

- Administer the coverage path. For the procedure, see Creating a coverage path on page 454.

To assign a coverage path to a user:

1. Type **`change station n`**, where ***n*** is the extension to which you want to assign a coverage path. Press **Enter**.

   The system displays the Station screen for the extension that you requested.

2. Click **Next** until you see the **Coverage Path 1** field (Figure 98: Station screen on page 458).

Figure 98: Station screen

```
                                STATION

Extension: 30019                          Lock Messages? n          BCC: 0
     Type: 4612                           Security Code: *           TN: 1
     Port: S04007                       Coverage Path 1:           COR: 1
     Name: station 30019                Coverage Path 2:           COS: 1
                                        Hunt-to Station:

STATION OPTIONS
              Loss Group: 19            Personalized Ringing Pattern: 1
                                                   Message Lamp Ext: 30019
            Speakerphone: 2-way                 Mute Button Enabled? y
       Display Language: english

                                                  Media Complex Ext:
                                                       IP SoftPhone? n
```

3. In the **Coverage Path 1** field, type a coverage path number of a previously administered Call Coverage path screen.
4. Perform one of the following actions:
   - In the **Coverage Path 2** field, type a coverage path number of a previously administered Call Coverage path screen, if you want the extension to have an alternative coverage path.
   - If you *do not* want a second coverage path, leave the **Coverage Path 2** field blank.
5. Press **Enter** to save your changes.
6. Click **Next** until you find the **Redirect Notification?** field (Figure 99: Station screen on page 459).

Figure 99: Station screen

```
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe           Auto Select Any Idle Appearance? n
          LWC Activation? y                     Coverage Msg Retrieval? y
  LWC Log External Calls? n                                 Auto Answer: none
            CDR Privacy? n                            Data Restriction? n
   Redirect Notification? y                  Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                    Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n      Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: enhanced             Audible Message Waiting? n
    MWI Served User Type:                    Display Client Redirection? n
             AUDIX Name:                   Select Last Used Appearance? n
                                             Coverage After Forwarding? y
                                               Multimedia Early Answer? n
                                        Direct IP-IP Audio Connections? y
 Emergency Location Ext: 30019                    IP Audio Hairpinning? y
```

7. In the **Redirect Notification?** field, perform one of the following actions:
   - Accept the default **y** if you want a half ring at the telephone when the system redirects a call to coverage.
   - If you do not want the half ring, type **n**.
8. Press **Enter** to save your changes.
9. Click **Next** until you find the **Button Assignments** area (Figure 100: Station screen on page 460).

   If you want the user to have buttons on the telephone for do not disturb, go to cover, or send all calls, use the **Button Assignments** area to assign the buttons. Note that you can use assign any, all, or none of the buttons, but you can make only one assignment per button.

Figure 100: Station screen

```
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                             7:
 2: call-appr                             8:
 3: call-appr                             9:
 4:                                      10:dn-dst
 5:                                      11:goto-cover
 6:                                      12:send-calls Ext:
```

10. Move to the button that you want to use, and perform any of the following actions:
    - If you want to assign a do-not-disturb button, type **dn-dst** after a button number.
    - If you want to assign a go-to-over button, type **goto-cover** after a button number.
    - If you want to assign a send-all-calls button, type **send-calls** after a button number. When you click **Next** or press **Tab** or **Enter**, the system displays the **Ext** field. If you want to send calls to the extension you specified when you typed the **change station** command, leave the **Ext** field blank. If you want to send calls to another extension, type the extension number to which the system redirects calls when the user presses the send-calls button.
11. Press **Enter** to save your changes.

Assigning a Consult button for a user

To assign a Consult button for a user:

1. Type **change station** ***n***, where ***n*** is the extension of the user to whom you want to assign the Consult capability. Press **Enter**.

   The system displays the Station screen for the extension that you requested.
2. Click **Next** until you see the **Button Assignments** area (Figure 100: Station screen on page 460).

3. In the **Button Assignments** area, type **consult** next to the button that you want the user to use for Consult.
4. Press **Enter** to save your changes.

Defining coverage redirected off-network calls

To define coverage for calls that the system redirects to external, off- network calls, you must complete the following procedures.

- Assigning the telephone number for the external coverage point
- Administering the coverage path for calls redirected to external numbers

Prerequisites

You must complete the following actions before you define coverage for calls that the system redirect off the network:

- On the Optional Features screen, verify that the **Cvg of Calls Redirected Off-Net** field is set to **y**. To view this screen, type **`display system-parameters customer-options`**. Press **Enter**.

  If the **Cvg of Calls Redirected Off-Net** field is set to **n**, your system is not enabled for the Call Coverage Off Network capability. Contact your Avaya representative for assistance before continuing with this procedure.

Assigning the telephone numbers for the off-network coverage points

To assign the telephone numbers for the off-network coverage points:

1. Type **`change coverage remote n`**, where ***n*** is the number of the Remote Call Coverage table that you want to change. Valid numbers are between 1 and 10. Press **Enter**.

   The system displays the Remote Call Coverage Table (Figure 101: Remote Call Coverage Table screen on page 462).

Figure 101: Remote Call Coverage Table screen

```
                        REMOTE CALL COVERAGE TABLE

01: 93035381000_____      16: _________________      31: _________________
02: _________________     17: _________________      32: _________________
03: _________________     18: _________________      33: _________________
04: _________________     19: _________________      34: _________________
05: _________________     20: _________________      35: _________________
06: _________________     21: _________________      36: _________________
07: _________________     22: _________________      37: _________________
08: _________________     23: _________________      38: _________________
09: _________________     24: _________________      39: _________________
10: _________________     25: _________________      40: _________________
11: _________________     26: _________________      41: _________________
12: _________________     27: _________________      42: _________________
13: _________________     28: _________________      43: _________________
14: _________________     29: _________________      44: _________________
15:_________________      30: _________________      45: _________________
```

2. Type the telephone number (maximum of 16 digits) of the remote coverage point in one of the remote call coverage table fields.

   Note:
   If you need a digit to get outside your network, add the digit before the external number. In this example, the system requires a **9** to place outside calls.

   The sequentially numbered fields in which you assign telephone numbers are called *remote code numbers*. You need this number to complete the procedure for defining coverage for calls redirected to external numbers. In this example the remote code number is **r1**. The letter **r** indicates remote, and **1** refers to the number 01 where you typed the telephone number on the screen. If you type a telephone number at number 15 on the screen, the remote code number for that entry is **r15**.

3. Press **Enter** to save your changes.

Administering the coverage path for redirected off-network calls

To administer the coverage path for redirected off-network calls:

1. Type **change coverage path *n***, where ***n*** is the number that is assigned to the coverage path that you want to administer for off-network coverage. Press **Enter**.

   The system displays the Coverage Path screen (Figure 102: Coverage Path screen on page 463).

Figure 102: Coverage Path screen

```
                                COVERAGE PATH

                  Coverage Path Number: 1
                                                Hunt after Coverage? n
                      Next Path Number:         Linkage

COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
              Active?             n              n
                Busy?             y              y
       Don't Answer?              y              y         Number of Rings: 2
                 All?             n              n
 DND/SAC/Goto Cover?              y              y

COVERAGE POINTS

    Terminate to Coverage Pts. with Bridged Appearances? n

  Point1: 4101      Rng: 3  Point2: r1        Rng:    Point3: h77       Rng:
  Point4:                   Point5:                   Point6:
```

Note:

To enter an extension that is assigned as a vector directory number (VDN) as the last point in the coverage path, you must make an administration change. For more information, see the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.

2. In the **Coverage Points** area, type the remote code number. The **Point** field that you select determines where the number is used in the coverage path. In this example:
   - **r1** is coverage point 2.
   - A call first covers to extension 4101.
   - If extension 4101 is unavailable or busy, the system redirects the call to the off-network number that is assigned to remote code number **r1** in the Remote Call Coverage table.

   When you move to the next **Point** field**,** the system displays the **Rng** field. If you want to use the number of rings displayed in the **Number of Rings** field on this screen, leave the **Rng** field blank.

   If you *do not* want to use the number of rings displayed in the **Number of Rings** field on this screen, type the number of rings for this coverage point.
3. Press **Enter** to save your changes.

Assigning time-of-day coverage

To assign time-of-day coverage for a user, you must complete the following procedures:

- Setting up a time-of-day coverage plan
- Assigning a time-of-day coverage plan to a the extension of the user

Prerequisites

You must complete the following actions before you can define a time-of-day coverage path:

- Administering the coverage path
- Setting up a time-of-day coverage plan

To administer the coverage path, see Creating a coverage path on page 454.

To set up a time-of-day coverage plan:

1. Type **`add coverage time-of-day next`**. Press **Enter**.

   The system displays the next Time of Day Coverage Table screen (Figure 103: Time of Day Coverage Table on page 464). If this is the first Time of Day Coverage plan in your system, the table number is 1. This is the table number that you assign to a user extension.

Figure 103: Time of Day Coverage Table

```
                        TIME OF DAY COVERAGE TABLE: 1

          Act   Cvg     Act   Cvg     Act   Cvg     Act   Cvg     Act   Cvg
          Time  Path    Time  Path    Time  Path    Time  Path    Time  Path

Sun        0:00 3         :             :             :             :
Mon        0:00 3       08:00 1       17:30 2       20:00 3         :
Tue        0:00 3       08:00 1       17:30 2       20:00 3         :
Wed        0:00 3       08:00 1       17:30 2       20:00 3         :
Thu        0:00 3       08:00 1       17:30 2       20:00 3         :
Fri        0:00 3       08:00 1       17:30 2       20:00 3         :
Sat        0:00 3       08:00 1       17:30 2       20:00 3         :
```

2. To define your coverage plan, type the time period and the path number for each day of the week that you want to cover.

   Enter the time in a 24-hour format, from the earliest to the latest. For example, assume that coverage path 1 goes to the co-worker, coverage path 2 goes to the home, and coverage path 3 goes to voice mail. In this example, the user has the following coverage:

- During the work day from 08:00 to 05:29, the system uses coverage path 1 to route calls to a co-worker.
- In the evening from 05:30 to 19:59, the system uses coverage path 2 to route calls to home.
- At night from 20:00 to 7:59 the following morning, the system uses coverage path 3 to route calls to voice mail.

  Define the path for the time period from 00:01 to 23:59 that you want coverage to operate. If you do not assign a coverage path to a specific time interval, no coverage exists from that time until the next coverage path activation time.

3. Press **Enter** to save your changes.

To assign the time-of-day coverage to a user.

1. Type **change station** ***n***, where ***n*** is the user telephone extension number. Press **Enter**.

   The system displays the Station screen (Figure 104: Station screen on page 465).

Figure 104: Station screen

```
                              STATION

Extension: 2054                              Lock Messages? n       BCC: 0
     Type: 7406D                             Security Code: 4196__   TN: 1
     Port: _____                           Coverage Path 1: t1       COR: 1
     Name: ______________________________  Coverage Path 2: ___      COS: 1
                                                  Hunt-to-Station: _______

STATION OPTIONS
             Data Module? n                Personalized Ringing Pattern: 1
          Display Module? n                     Message Lamp Ext: ________


                                             MM Complex Data Ext: ________
```

2. In the **Coverage Path 1** field, type **t** plus the number of the Time of Day Coverage Table. In this example, the coverage path is **t1.** The system redirects calls to this extension as defined in the Time of Day Coverage Table number 1.
3. Press **Enter** to save your changes.

Creating a coverage answer group

To add a coverage answer group:

1. Type **add coverage answer-group next**. Press **Enter**.

   The system displays the next Coverage Answer Group screen (Figure 105: Coverage Answer Group on page 466).

Figure 105: Coverage Answer Group

```
                        COVERAGE ANSWER GROUP

                     Group Number: ___
                     Group Name: COVERAGE_GROUP_

GROUP MEMBER ASSIGNMENTS
   Ext      Name (first 26 characters)     Ext      Name (first 26 characters)
1: ________ ___________________________ 5: ________ ___________________________
2: ________ ___________________________ 6: ________ ___________________________
3: ________ ___________________________ 7: ________ ___________________________
4: ________ ___________________________ 8: ________ ___________________________
```

2. In the **Group Name** field, type a name to identify the coverage group. The default name is **Coverage Group**.
3. In the **Ext** column, type the extension of each group member that you want to include in this group. You can type only one extension in each **Ext** field.
4. Press **Enter** to save your new group list.

Note:
The system automatically completes the **Name** field when you press **Enter**.

Assigning Internal Alerting

To assign internal alerting for APLT, ISDN-PRI, or Tie trunks:

1. Type **change trunk-group *n***, where ***n*** is the number of the trunk-group for which you want to administer Remote Access.

   The system displays the Trunk Group screen.
2. Click **Next** until you see the **Internal Alert?** field.
3. In the **Internal Alert?** field, perform one of the following actions:
   - If you want internal ringing and coverage for your system, type **y**.

- If you do not want internal ringing and coverage for your system, type **n**.

4. Type **Enter** to save your changes.

Enabling enhanced Redirection Notification

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the **Feature-Related System Parameters** screen. See Figure 106.

2. Click **Next** till you see the **Redirection Notification** field.

Figure 106: Feature Related System Parameters- Redirection Notification

```
change system-parameters features                              Page  15 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

SPECIAL TONE
                                  Special Dial Tone? n
          Special Dial Tone for Digital/IP Stations: none

REDIRECTION NOTIFICATION
                           Display Notification for Do Not Disturb? n
                           Display Notification for Send All Calls? n
                             Display Notification for Call Forward? n
                     Display Notification for Enhanced Call Forward? y
                          Display Notification for a locked Station? n
         Display Notification for Limit Number of Concurrent Calls? n
                           Display Notification for Posted Messages? n
                                 Scroll Status messages Timer(sec.): ___




Chained Call Forwarding? n
```

3. Enable notification for the features that you want by setting the respective **Display Notification for?** fields to **y**.
4. In the **Scroll Status messages Timer (sec.)** field, enter a value for the time delay between messages of different notification types. Leave the field blank to disable scrolling.

   For more information about the **Display Notification for** and **Scroll Status messages Timer** fields, see Avaya Aura™ Communication Manager *Screen Reference*, 03-602878.

5. Press **Enter** to save your changes.

Reports for Call Coverage

The following reports provide information about the Call Coverage feature:

- The Coverage Path Measurement report shows coverage activity about the coverage paths.
- The Principal Coverage Measurement report shows coverage activity about the called extensions.
- The Call Detail Recording (CDR) report shows the outgoing trunk calls.

For detailed information on these reports and the associated commands, see *Avaya Aura™ Communication Manager Reports*, 555-233-505.

Considerations for Call Coverage

This section provides information about how the Call Coverage feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Coverage under all circumstances.

- Tie-trunk calls

  Incoming tie-trunk calls can be administered as either internal calls or external calls, and are redirected to Call Coverage accordingly.

Interactions for Call Coverage

This section provides information about how the Call Coverage feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call Coverage in any feature configuration.

- Agent Call Handling

  Do not assign Cover All Calls to agents who have the Automatic Answer option enabled. Any Automatic Call Distribution (ACD) or any non-ACD call to an extension on which Automatic Answer is enabled, and for which the coverage redirection criteria is administered as Cover All Calls, does not go to coverage. Instead, the call goes to the called extension. Cover All Calls redirection criteria do not affect incoming calls when a user is in the Auto-Answer mode.

- Answer Detection

  Coverage of Calls Redirected Off-Net (CCRON) competes with Answer Detection for call classifier ports.

- Automatic Callback and Ringback Queuing

  The system does not redirect callback calls to coverage. The caller can activate Automatic Callback when the user hears a ringing, redirection notification signal or a busy signal.

- Automatic Intercom, Dial Intercom, and Priority Calling

  The system does not redirect calls that use these features to coverage, unless the caller presses the Go to Cover button.

- Bridged Call Appearance

  Coverage criteria for bridged call appearances are based entirely on the criteria of the primary extension that is associated with the bridged call appearance.

  If a telephone user activates Send All Calls on the primary extension, incoming calls still ring bridged call appearances of that extension, as long as a simulated bridged appearance of the call is maintained at the primary extension.

  While an off-network call is undergoing call classification, the system blocks a user from bridging onto the call.

- Call Detail Recording (CDR)

  When the **Coverage of Calls Redirected Off-Net** field (CCRON) is enabled, the system generates a CDR record only after the call is answered off the network. The dialed number in the record is the off-network number to which the call covers. The calling number is the station that is covered to the off-network destination.

- Call Forwarding

  Call Forwarding temporarily overrides the redirection criteria. When the redirection criteria are met at the forwarded-to extension, the system redirects the call to the coverage path of the forwarding extension.

  The system allows calls that are forwarded off the network to be tracked for busy or no-answer conditions, and to return for further call-coverage processing under those conditions. However, if the called extension does not have a coverage path, the system does not track the call and the call is left at the off-network destination, regardless of whether the call is answered or busy.

  For calls redirected to QSIG networks, if coverage after forwarding is not enabled, the QSIG redirection takes precedence over the CCRON capability. However, if coverage after forwarding is enabled, CCRON takes precedence, enabling the call to be tracked back to the network to follow the coverage path.

  If both Send All Calls and Call Forwarding are active, the system immediately redirects most calls to that extension to coverage. However, the system forwards priority calls to the designated forwarding destination.

  If Cover All Calls is part of the coverage redirection criteria, and if Call Forwarding is active at an extension, the system immediately directs most calls to that extension to coverage. However, the system forwards priority calls to the designated forwarding destination.

  Activation of Send All Calls at the forwarded-to extension does not affect calls that are forwarded to that extension.

- Call Pickup

  Any call that the system directs to a covering user who is a member of a call pickup group can be answered by other members of the group.

- Call Prompting

  Coverage of Calls Redirected Off-Net (CCRON) competes with the Call Prompting feature for call classifier ports.

- CallVisor ASAI

  Coverage of Calls Redirected Off-Net (CCRON) competes with CallVisor for call classifier ports.

- Centralized Attendant Service (CAS)

  If an incoming CAS call is directed to a hunt group, the call is not redirected to the coverage path of the hunt group.

- Class of Restriction (COR) and Controlled Restrictions

  Users who might usually be restricted from receiving calls can receive calls that the system directs to them from the Call Coverage feature.

- Conference

  The system blocks users from conferencing another party onto a call that was routed off the network while the call is undergoing call classification. If any party on the call is on hold, the system routes the call off the network, but the system does not attempt to classify the call. The system routes the call off the network, even when the **Coverage of Calls Redirected Off-Net** field (CCRON) is enabled.

  A call that covers to a vector directory number (VDN) cannot be added to a conference while the call is in vector processing.

- Direct Department Calling (DDC), Uniform Call Distribution (UCD), and Automatic Call Distribution (ACD)

  If a user with an Auxiliary Work button activates or deactivates Send All Calls, the Auxiliary Work function that is associated with the DDC feature or the UCD feature is activated or deactivated simultaneously.

  If a user has no Auxiliary Work button, activating or deactivating Send All Calls makes the user unavailable or available, respectively, for **DDC and UCD** calls, but Auxiliary Work is not activated or deactivated. The user can use a Feature Access Code (FAC) to activate or deactivate Auxiliary Work mode.

  Activating or deactivating the Auxiliary Work function does not activate or deactivate Send All Calls.

- Direct Outward Dialing (DOD)

  Coverage of Calls Redirected Off-Net (CCRON) competes with DOD for call classifier ports when DOD uses MFC signaling. The Call Classifier - Detector port provides the MFC tones. Non-MFC DOD calls do not need the Call Classifier - Detector port for this purpose, because Non-MFC DOD calls do not need MFC tones.

- Global Call Classification

  To classify tones in countries that do not use the USA tone plan, time cadences and frequencies must be administered so that time cadences and frequencies can be downloaded to the call classification circuit packs. You need a Call Classifier-Detector or Tone Clock with Call Classifier-Tone Detector circuit pack.

- Hold

  If a covering user puts a call on hold, and the called user picks up on the call, the coverage appearance might be dropped, depending on administration.

  If any party is on hold when the system routes a coverage call off the network, that call does not undergo call classification. In this case, the call does not undergo call classification, even when the **Coverage of Calls Redirected Off-Net** (CCRON) field is enabled on your system.

- Internal Automatic Answer (IAA)

  If call coverage redirection criteria redirects an internal call to another telephone, that call is eligible for IAA at that telephone.

  IAA does not apply to calls to the original called extension when the:

  — User at the called extension has Do Not Disturb, Send All Calls, or Cover All Calls active

  — Calling user selects Go To Cover before the user places the call

  Calls that are directed to a Coverage Answering Group cannot use IAA.

- ISDN End-to-End Calls

  When ISDN facilities carry an off-network coverage call end-to-end, call classification is accomplished through the ISDN protocol, rather than by a call classifier port.

- Leave Word Calling (LWC)

  Call Coverage can be used with or without LWC. However, the two features complement each other. When a covering user activates LWC during a coverage call, a message is left for the called user to call the covering user. When a covering user activates Coverage Callback during a coverage call, a message is left for the called user to call the internal caller.

- Tenant Partitioning

  The Tenant Partitioning feature might not block coverage calls across tenant partitions.

Interactions for Limit Number of Concurrent Calls

The following are the interactions for the Limit Number of concurrent calls (LNCC) feature.

- Logged in agent call with LNCC active

  LNCC activation from a login agent is allowed. If activated, LNCC operation applies to station directed call, which the agent logged on, only and not agent directed calls. That is, call to a busy LNCC active station will get busy treatment. Upon agent logoff, the LNCC state will remain in effect for the station and not the agent extension.

- Auto Callback - Any call to an LNCC active station that activates the auto callback feature will receive a call back when the LNCC active station becomes available.

- Bridged Call Appearance (BCA) - A busy LNCC active station will receive bridged calls. This includes the case for a station where no primary call appearances are assigned. Any station that has a BCA of a busy LNCC active station will not receive bridged calls.

- Call Coverage

  - Call to a busy LNCC active station without call coverage

    When an incoming call terminates at a busy LNCC active station, the calling party will receive busy signal for incoming ISDN call.

- Call to a busy LNCC active station with call coverage

  When an incoming call terminates at a busy LNCC active station, the calling party will receive busy signal, regardless if the coverage criteria is met.

- LNCC station covering point

  A busy LNCC active station, LNCC station covering point is as busy.

- Group Termination

  When a member of a group has LNCC active, LNCC applies to the individual station even if the station receives calls for various groups as a member. Thus, a busy LNCC active will not be able to receive a group call as a member. Moreover, if an LNCC active station is busy on a group call, then a subsequent individual call will get busy treatment. Other members in the group that are not LNCC active can still receive the call.

- Hold

  Calls can be put on hold on a busy LNCC active station.

  A call to a LNCC active station with a call on hold will receive busy.

- Conference

  A conference call can be initiated from a LNCC active station as long as there is at least one available call appearance.

- Crisis Alert

  A busy LNCC active station with crisis alert button assigned will be alerted if an emergency call is initiated.

- E911 Callback

  Emergency callback to a LNCC active station with multiple call appearance is allowed regardless if the station has an idle call appearance or not.

- Enhanced Mobility User (EMU)

  The LNCC button will not be part of the support button set.

- Multiple Level Precedence Preemption (MLPP)

  A call with a higher precedence level than the LNCC active station call will be preempted. If the incoming MLPP call is at equal or lower precedence level and precedence call waiting is enabled then call waiting will occur on the active call other wise the call will be busy.

- No Hold Conference

  A LNCC active station can initiate a no hold conference.

- OPTIM

  There will be no LNCC feature support added for OPTIM terminals. If an OPTIM terminal calls a LNCC active station, the call will be handled the same as detailed in the requirements of this document.

- Personal Station Access (PSA)/Terminal Translation Initialization (TTI)

  Since the LNCC status is saved in the station translation, thus the LNCC status is retained along with PSA association.

- Primary and Bridged Call Appearance

  A station busy on a bridged call appearance with LNCC active will not receive call for primary call appearance.

- Priority Call Termination

  A priority call to a LNCC active station with multiple call appearances is allowed if the called station has an idle call appearance available.

- Remote Access

  LNCC FAC dialing from a remote access trunk will result in intercept tone.

- Send All Calls (SAC)

  On a station with both SAC and LNCC active, the call terminates at an idle station with both SAC and LNCC activated; the incoming call will be routed to the station's coverage.

- Transfer

  A call can be transferred from a LNCC active station as long as there is at least one available call appearance.

Interaction for Enhanced Redirection Notification

The following are the interactions for the enhanced Redirection Notification:

- Bridged Call Appearance

  Does not work on stations that have no call appearance of their own.

- Call Forwarding

  Applies to Call Forwarding All, Call Forwarding Busy/Don't Answer, and Enhanced Call Forwarding.

- Do Not Disturb

  Applies to Do Not Disturb whether activated from the station or from an attendant console.

- Enterprise Mobility User

  Applies only to the home user of the telephone. If the user is a visitor at another station, no notification is displayed.

Troubleshooting Call Coverage

This section lists the known or common problems that users might experience with the Call Coverage feature:

Problem	Possible cause	Action
The system redirects some unanswered calls to the Attendant console, instead of the coverage path.	A call that is transferred internally, and not answered within the interval that is specified in the **Return Call Timeout** of the Console Parameters screen, redirects to the attendant console.	Verify that the called extension has a coverage path by typing the **`status station`** command. If the **active coverage option** field on the Station screen has a coverage path, increase the number of seconds in the **Return Call Timeout** interval on the Console Parameters screen. Increase the interval so that it exceeds the total time that a call rings on the called extension and all points in the coverage path of the called extension.
The system does not redirect to the correct destination in the coverage path of the called extension.	The called extension is forwarded to another destination.	Type the **`status station`** command to determine if either Call Forwarding or Send All Calls is active at the called extension. If the **CF Destination Ext** field contains a forwarded-to extension, cancel Call Forwarding for the called extension. If the **SAC Activated?** field is set to **yes**, cancel Send All Calls for the called extension.
	The coverage path that you assigned to the called extension is incorrect.	Type the **`display station`** command to verify that you assigned the correct coverage path to the called extension. Change the coverage path if the coverage path is not the coverage path that you want for the called extension.

Problem	Possible cause	Action
The system does not redirect to the coverage path of the called extension.	The points in the coverage path are unavailable.	Run the **status station** command to determine if either Call Forwarding or Send All Calls is active at the called extension. If the **CF Destination Ext** field contains a forwarded-to extension, cancel Call Forwarding for the called extension. If the **SAC Activated?** field is set to **yes**, cancel Send All Calls for the called extension. If the coverage path of the called extension contains a hunt group, ensure that the length of the queue is sufficient to contain all the calls that the system redirects to the hunt group.

Call Detail Recording

Use the Call Detail Recording (CDR) feature to record information on incoming, outgoing, and tandem calls for each trunk group that you administer for CDR, including auxiliary trunks. The system records information on each trunk-group call and each station-to-station call.

Detailed description of Call Detail Recording

Use the Call Detail Recording (CDR) feature to record information on incoming, outgoing, and tandem calls for each trunk group that you administer for CDR, including auxiliary trunks. The system records information on each trunk-group call and each station-to-station call.

You can also request that CDR record information on:

- Temporary signaling connections (TSCs) that involve trunks
- Calls that use loudspeaker paging
- Calls to which account code dialing or a Feature Access Code (FAC) apply
- Ineffective call attempts

  If you request that the system record information in ineffective call attempts, you greatly increase the number of calls that the system records. However, the request to record ineffective call attempts can also help you to increase security, because the system records call attempts that are blocked because of insufficient calling privileges.

  Information on ineffective call attempts can also show you that your users cannot make calls because all the trunks on your system are busy.
- The audio service link calls that the switch uses for IP softphones that are set up as telecommuter IP softphones.

  An IP softphone can use one audio service link to make many short calls. The system shows these many short calls as one long call on the CDR reports.

Some call accounting systems do not support all the information that CDR offers. See your Avaya representative for information on how CDR operates on your system.

CAUTION:
When migrating a platform from a legacy system to a Linux-based system of Communication Manager 3.0 or newer, where both the old and new systems utilize CDR, ensure that the older CDR parsing scripts correctly utilize all of the characters identified in each of the fields contained in the applicable format table (see Table 25 through Table 42).

Monitoring call detail records

You can monitor call detail records daily for unusual calling patterns, long calls, international calls, calls that are outside the normal business hours, and other indications of toll fraud. Call accounting systems are available that automatically monitor CDR output for fraudulent calling patterns.

Legacy CDR and Survivable CDR

Beginning with Communication Manager Release 5.0, you can have Legacy or Conventional CDR or Survivable CDR for your system. Both methods provide the identical call accounting information and support the same CDR formats.

In a Legacy CDR environment, Communication Manager generates all CDR records to the active server and then exports the records to a CDR adjunct (using IP links) for further processing. In these systems, the CDR adjunct functions in a "listen only" mode receiving the records sent by Communication Manager. This type of CDR processing was used exclusively in Communication Manager up through Release 3.X. In a Legacy CDR environment, the system cannot collect CDR records when link between main, LSP and/or ESS and CDR adjunct is down (this is generally the case when a LSP or ESS is active). It also requires the IP link between Communication Manager and the CDR adjunct to be up at all times.

Communication Manager 4.x or later introduced a new method of data collection called Survivable CDR. Survivable CDR allows CDR data records to be stored on the Communication Manager server's local hard drive, if desired. The CDR adjunct then periodically polls each the Communication Manager server and collects the CDR data files from the servers. Survivable CDR was introduced in Communication Manager Release 4.0 and it was only supported on LSP platforms. Beginning with Communication Manager Release 5.0, Survivable CDR is supported on all Communication Manager platforms, that is, on the "mains", LSPs and ESS. Survivable CDR allows CDR data to be transferred in an encrypted manner from the Communication Manager server to the CDR adjunct using the Secure File Transfer Protocol (SFTP). Note that Survivable CDR requires updated CDR adjuncts. CDR records are stored and transferred in batches, rather than one record at a time as with Legacy CDR.

Setting up Survivable CDR

The Survivable CDR feature is used to store CDR records to a server's hard disk. For ESS servers and LSPs, the Survivable CDR feature is used to store the CDR records generated from calls that occur when an LSP or ESS server is controlling one or more gateways or port networks. For a main server, the Survivable CDR feature provides the ability to store CDR records on the server's hard disk.

When the Survivable CDR feature is enabled, the CDR records are saved in a special directory named **/var/home/ftp/CDR** on the server's hard disk. The CDR adjunct retrieves the Survivable CDR data files by logging into the server and copying the files to its own storage device. The CDR adjunct uses a special login that is restricted to only accessing the directory where the CDR records are stored. After all the files are successfully copied, the CDR adjunct deletes the files from the server's hard disk and processes the CDR records in the same manner that it does today.

Note:
This feature is available on main servers and ESS servers that are Communication Manager Release 5.0 and later releases only. It is available on LSP platforms running Communication Manager 4.0 and later.

The CDR adjunct must poll each main, LSP, and ESS server regularly to see if there are any new data files to be collected. This is required even when an LSP or ESS server is not controlling a gateway or a port network because the CDR adjunct has no way of knowing if a LSP or ESS server is active.

The Survivable CDR feature utilizes the same CDR data file formats that are available with legacy CDR.

Note:
For procedural information on administering Survivable CDR, see Administering Survivable CDR on page 596.

Files for Survivable CDR

When Survivable CDR is enabled, the server writes the CDR data to files on the hard disk instead of sending the CDR data over an IP link. The Survivable CDR feature creates two types of CDR data files: a Current CDR data file that the server uses to actively write CDR data and a set of archive files containing CDR data that the server collected earlier but has not yet been collected and processed by the CDR adjunct. The naming convention for both file types are similar. However the name of the Current CDR file is always prefixed by a 'C-' (for more information see File naming conventions for Survivable CDR on page 480).
The CDR Current file remains active until one of the following events happen:

- The server's system clock reaches 12:00 midnight.
- The Current CDR file reaches or exceeds 20 megabytes. A 20 megabyte file may contain up to 140K CDR records depending on the CDR format used.

- A filesync, a reset system 2 (cold restart), or a reset system 4 (reboot) occurs.

After one of the above events occur the following actions take place:

- The Current CDR file is closed and it becomes an archive CDR file
- The file permissions change from read/write (rw) for root and read only for members of the CDR_User group to:
  - Owner (root): Read/Write/Execute (rwx)
  - Group (CDR_User): Read/Write (rw-)
  - World: none (---)
- The 'C-' prefix is removed from the front of the file name
- For a main server, a new Current CDR file is created
- For an LSP or an ESS server, a new Current CDR file is created only if the LSP or the ESS server is controlling one or more gateways or port networks.

File naming conventions for Survivable CDR

The Survivable CDR data files have the following naming conventions:

tssssss-cccc-YYMMDD-hh_mm

where:

- t is populated with an L for an LSP, an E for an ESS server, or an S for a main server
- ssssss is populated with the least significant six digits of the System ID or SID. The SID is a unique number in the RFA license file used to identify the system. The SID for a server can be viewed by using one of the following methods:
  - Use the **`statuslicense -v`** BASH command.
  - Use the command **`display system-parameters customer-options`** on the SAT.
- cccc is populated with the least significant four digits of the Cluster ID (CL ID) or Module ID (MID). To display the MID for the server:
  - Use the **`statuslicense -v`** BASH command.
- YY is populated with the two digit number of the year the file was created.
- MM is populated with the two digit number of the month the file was created.
- DD is populated with the two digit day of the month the file was created.
- hh is populated with the hour of the day the file was created based on a 24 hour clock.
- mm is populated with the number of minutes after the hour when the file was created.

The Current CDR file uses the same naming convention except the name is prefixed with a 'C-'.

Removing Survivable CDR files

You can remove CDR files by:

- The Survivable CDR feature: The Survivable CDR feature on the main, LSP, or ESS server automatically removes the oldest CDR data achieve file anytime the number of archived files exceed 20. The Current CDR file is not an archived file and therefore not counted in the 20 files allowed on the hard disk.
- CDR adjunct: In a normal operating environment, the CDR adjunct has the responsibility to delete the CDR data files after they are copied and verified that they are correct.

Accessing Survivable CDR files

A special user group called CDR_User exists that allows the administrator to identify all users authorized to access the CDR storage directory. The archived CDR files are stored in /var/home/ftp/CDR.

QSIG Supplementary Service - Advice of Charge

Beginning with Communication Manager Release 4.0 or later, use the QSIG Supplementary Service - Advice of Charge feature to extend charging information from the public network into the private network. The charging information that many service providers supply is extended from a gateway enterprise system to the end user's enterprise system. The charging information can then be displayed on the user's desktop.

Information can be extended and displayed either:

- At intervals during the call and at the end of the call, or
- Only at the end of the call

QSIG stands for Q-Signaling, which is a common channel signal protocol based on ISDN Q.931 standards and used by many digital telecommunications systems. Only charge information received from the public network with ETSI Advice of Charge, and Japan Charge Advice is extended into the QSIG private network.

The following describes a call flow with the QSIG Supplementary Service - Advice of Charge feature:

1. A user places a call through the private telecommunication network (PTN) and into the public switching telecommunication network (PSTN).
2. Charging information from the PSTN is conveyed to the gateway switch either:
   - At intervals during the call and at the end of the call, or
   - Only at the end of the call

   This is determined by Communication Manager administration, and by subscription, at the gateway switch, of Charge Advice with the PSTN Service Provider.

3. If Communication Manager is the gateway, CDR information may be recorded at the gateway and routed to the user's switch for recording there as well. This enables accounting the call to an end user in addition to recording the trunk used.
4. If there is a tandem node in the call path, the tandem node may also send call record data to a CDR port.
   - If the tandem node is a Tenovis I55, the record can contain charge information.
   - If the tandem node is Communication Manager, the record is passed without CM doing anything with it.

Customer options that are required for the feature are ISDN, QSIG Basic Call and QSIG Basic Supplementary Services. These options are typically activated by enabling the Communication Manager - Enterprise Edition RFA file.

To use this feature, you must have adjunct devices that are capable of logging or interpreting CDR output formats that record ISDN Call Charge.

Existing PRI, BRI, and H.323 hardware interfaces providing QSIG and bearer transport are used for this feature.

Administering Charge Advice for QSIG trunks

To administer charge advice for a trunk group with Supplementary Services Protocol "b":

1. On the Trunk Group screen, for Group Type <tab> to the **Charge Advice** field.
2. Select from the following options:
   - during-on-request - to request that charging information be provided at intervals during a call, and also at the end of the call
   - end-on request - to request that charging information be provided only at the end of a call
   - none - no charging information will be requested for the trunk group

Note:
Receipt of charge advice on the QSIG trunk group is also dependent on Charge Advice administration at the PSTN trunk group involved on the call, and whether charges are received from the public network.

- On the Trunk Group screen, administer the **Decimal Point** field.
  - period (.) -This is the default. If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a period as the decimal point.
  - comma (,) - If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a comma as the decimal point.

Note:
If the received charge contains no decimals, no decimal point is displayed (that is, the administered decimal point is ignored for charge information received with no decimals). On an upgrade from a QSIG trunk group with the **Decimal Point** field administered as **none**, the field defaults to **period**.

Answer Detection

Communication Manager provides three methods to determine whether the called party answers a call:

- Call classification
- Network answer supervision
- Answer supervision by timeout

Call classification

A call-classifier circuit pack detects tones and voice-frequency signals on the line to determine whether a call is answered. This method is fairly accurate. The calls that are answered are usually classified correctly. But the following exceptions exist:

- Miscellaneous tones, such as confirmation tones, might be classified as answers.
- Loud background noise might activate answer detection, and cause the a call to be classified as answered, even if the call is not connected.
- Some calls that are answered might be incorrectly classified as fast busy signals.
- Call classifier circuit packs do not recognize Special Information Tones (SIT) as answers.

The system generates a call record for any call that is classified as answered, whether the classification is correct or not. If Call Classification incorrectly classifies a call as answered, and the call is subsequently answered, the call duration that CDR reports includes both the time between the incorrect classification and the actual answer, and the remaining duration of the call.

Network answer supervision

The central office (CO) sends a signal to the originating switch when the far end answers a call. If a call travels over a private network before the call reaches the CO, the signal is transmitted back over the private network to the originating switch. This method is extremely accurate, but network answer supervision is unavailable over most loop-start trunks. For example, network answer supervision in not available over CO, foreign exchange (FX), and Wide Area Telecommunications Service (WATS) trunks in the US.

Answer supervision by timeout

If the caller is off-hook when the answer timer expires, the system assumes that the outgoing call is answered. Answer supervision by timeout is the least accurate method to detect that a call is answered. Calls that are shorter than the timer duration do not generate call records. Calls that ring for a long time produce call records, even if the calls are unanswered.

Network answer supervision overrides answer supervision by timeout.

Call Detail Recording (CDR) supports the following capabilities:

- Account Code Dialing
- Forced Entry of Account Codes
- Call Splitting
- Intraswitch CDR
- CDR Privacy

Account Code Dialing

Use the Account Code Dialing capability to associate a call with an account number. A user enters a FAC for Account Code Dialing before a user dials a telephone number. You can specify that the use of the FAC is mandatory or optional for the user. When a user dials a telephone number and the FAC, the system records the:

- Telephone number
- Account code
- Trunk Access Code (TAC), or the Automatic Route Selection (ARS) access code

The system does not record the FAC for Account Code Dialing.

Forced Entry of Account Codes

If you require that users enter an account code FAC, you have several options. You can require that:

- All users enter an account code for all calls
- All users enter an account code for calls that are made on a specific trunk.
- All users enter an account code for calls that are made to a specific telephone number
- A specific user enters an account for all calls that are made by that user

If you use the Forced Entry of Account Codes (FEAC) capability, the system rejects any call that a user makes without an account code FAC, if the call requires an account code. When the system rejects the call, the user hears intercept tone.

Avaya recommends that you use the FEAC capability to make your system more secure.

Note:

The system does not verify account codes. The system only verifies that the user enters the number of digits that you specify. If you want the system to verify account codes, you need to use the Authorization Codes feature. For more information, see the "Authorization Codes" feature.

The following types of calls never require an account code:

- Calls that an attendant makes
- Calls that an attendant makes to determine if a trunk is busy
- Calls that a user makes to determine if a trunk is busy
- Distributed Communications System (DCS) calls, unless the Class of Restriction (COR) of the trunk requires an account code
- Personal Central Office Line (PCOL) calls
- Remote access calls that do not have barrier codes
- Trunk-to-trunk calls

Call Splitting

You use the Call Splitting capability to record information about the following calls that:

- Are part of a conference
- Transferred
- Involve an attendant

The system records a separate CDR record for each participant on any of these types of calls.

You can request call splitting information for both incoming and outgoing trunks. You can also request call splitting information for an attendant call on an incoming trunk, and for an attendant call on an outgoing trunk

Incoming trunk call splitting

If you request incoming trunk call splitting (ITCS) information for a call, the system creates a CDR record when a user uses the Conference feature or the Transfer feature. The CDR record includes the:

- Duration of the user participation

- Incoming TAC
- Number that the caller dialed
- Condition code

When a user drops a call, or successfully transfers a call, the system records the action of the user. The duration of a transferred call starts when the transferring party presses the transfer button for the second time.

When a user uses the Conference feature for an incoming trunk call, the system creates a CDR record when the user adds a participant to the conference call. The CDR record of these calls shows the duration of the call for each user who participated. The CDR records of a conference call contain duration information that overlaps.

The system creates an incoming trunk call record when:

- You requested ITCS for your system.
- A user adds another user to a conference call. or a user transfers another user
- The user who is added to the conference call, or who is transferred, is on a local extension that has the Intraswitch CDR option activated.

The system does not create an Intraswitch CDR record.

Examples

ITCS and a conference call: The following example shows the interaction between the participants of a conference call and the system, when ITCS is active, and all participants are on the same server:

- Caller A, at extension 123, makes an incoming trunk call to participant B, at extension 565-7890.
- Caller A and participant B talk for 2 minutes.
- Participant B adds participant C, at extension 5-4321, to the conference call.
- Participant B adds participant D, at extension 5-9876, to the conference call.
- Caller A, participant B, participant C, and participant D talk for an additional 8 minutes.
- Participant B drops the call.
- The system creates a CDR record for call segment A-B.
- Caller A, participant C, and participant D talk for an additional 5 minutes.
- Caller A, participant C, and participant D drop the call.
- The system creates two additional CDR records, one for call segment A-C and one for call segment A to D. Note that each CDR record shows the incoming trunk ID as the calling number, 123.

Table 15: ITCS conference call on the same server on page 487 shows the CDR information that changes when ITCS is active during a conference call. The call durations are approximate.

Table 15: ITCS conference call on the same server

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:10:0	C	-	123	5657890
A-C	0:13:0	C	-	123	54321
A-D	0:13:0	C	-	123	59876

ITCS and a call transfer on the same server : The following example shows the interaction between the participants of a transfer call and the system when ITCS is active, and all participants are on the same server:

- Caller A, at extension 123, calls participant B, at extension 565-7890.
- Caller A and participant B talk for 1 minute.
- Participant B transfers the call to participant C, at extension 5-4321.
- The system creates a CDR record for call segment A-B.
- Caller A and participant B talk for an additional 5 minutes.
- Caller A and participant B drop the call.
- The system creates a CDR record for call segment A-C.

Table 16: ITCS transfer on the same server on page 487 shows the CDR information this scenario. The call durations are approximate.

Table 16: ITCS transfer on the same server

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:01:0	9	-	123	5657890
A-C	0:05:0	9	-	123	54321

ITCS and a call transfer to the public network: The following example shows the interaction between the participants of a transfer call and the system when ITCS is active, and all the participants are *not* on the same server:

- Caller A, at extension 123 on server, calls participant B, at extension 565-7890.

  Both caller A and participant B are on the same server.
- Caller A and participant B talk for 1 minute.
- Participant B transfers the call to participant C, at telephone number 566-5555.

  Participant C is on the public network.

- Participant B and participant C talk for an additional 4 minutes.
- Participant B and participant C drop the call.
- The system creates two CDR records, one for call segment A-B, and one for call segment A-C.

Table 17: ITCS transfer to an outgoing trunk on page 488 shows the CDR information that changes when ITCS is active during a call transfer. The call durations are approximate. Note that the duration of the original incoming trunk call, call segment A to B, includes the duration of the conversation between caller A and participant B, and the duration of the conversation between participant B and participant C.

Table 17: ITCS transfer to an outgoing trunk

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:05:0	9	-	123	5657890
A-C	0:04:0	9	345	123	5665555

Outgoing trunk call splitting

If you request outgoing trunk call splitting (OTCS), the system creates CDR records of transferred outgoing calls in the same manner as for ITCS. See Table 16: ITCS transfer on the same server on page 487 and Table 17: ITCS transfer to an outgoing trunk on page 488 for a description of the CDR information on transfer calls when ITCS is active.

If a user requests OTCS and originates a conference call, the call duration for that user starts when the user originates the call. The call duration for that user ends when the user drops the call. When that user drops the call, the system creates a second CDR record for the users who remain on the conference call.

Examples

OTCS and a conference call on the public network: The following example shows the interaction between the participants of a transfer call and the system, when OTCS is active, and all the participants are *not* on the same server:

- Caller A, at extension 123 on server, calls participant B, at telephone number 777-7890.

  Participant B is on the public network.
- Caller A and participant B talk for 5 minutes
- Caller A adds participant C to the conference call.
- Participant B transfers the call to participant C, at telephone number 777-5678.

  Participant C is on the public network.

- Caller A, participant B, and participant C talk for an additional 5 minutes.
- Caller A, participant B, and participant C drop the call.
- The system creates two CDR records, one for call segment A-B, and one for call segment A-C.

Table 18: OTCS conference call on page 489 shows the CDR information that changes when OTCS is active during a conference call. The call durations are approximate.

Table 18: OTCS conference call

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:10:0	C	345	57890	7771234
A-C	0:05:0	C	345	57890	7775678

OTCS and a call transfer to a public network: The following example shows the interaction between the participants of a transfer call and the system, when OTCS is active, and all the participants are *not* on the same server:

- Caller A, at extension 51234 on server, calls participant B, at telephone number 777-7890.

  Participant B is on the public network.
- Caller A and participant B talk for 5 minutes.
- Caller A transfers the call participant C, at extension 54444.

  Caller A and participant C are on the same server.
- The system creates two CDR records, one for call segment A-B, and one for call segment C-B.

Table 19: OTCS call transfer on page 489 shows the CDR information that changes when OTCS is active during a call transfer. The call durations are approximate.

Table 19: OTCS call transfer

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
A-B	0:01:0	A	345	51234	5659999
C-B	0:05:0	A	345	54444	5659999

ITCS, OTCS, and attendant call recording

If you request either ITCS or OTCS, you have the option for the system to generate a CDR record of the attendant portion for calls that are transferred.

If you request either ITCS or OTCS, the system always creates a separate CDR record of the attendant portion of a conference call.

Examples

An example of an attendant incoming trunk call transfer: The following example shows the interaction between the participants of a transfer call and the system, when either ITCS or OTCS is active:

- Caller A, at TAC 123, calls the attendant, and asks the attendant to transfer the call to participant B, at extension 5-888

  Caller A is on the public network.

  The attendant and participant B are on the same server.
- Caller A and the attendant talk for 1 minute.
- Caller A and participant B, talk for 5 minutes.
- The system creates two CDR records, one for call segment A-Attd, and one for call segment A-B.

Table 20: Attendant transfer of an incoming trunk call on page 490 shows the CDR information that changes when ITCS or OTCS is active when an attendant transfers an incoming public network call.

Table 20: Attendant transfer of an incoming trunk call

Call Segment	Call Duration	Condition code	Access code used	Calling number	Dialed number
A-Attd	0:01:0	9	-	123	Attd
A-B	0:05:0	9	-	123	58888

An example of an attendant call transfer on a public network trunk: The following example shows the interaction between the participants of a transfer call and the system, when either ITCS or OTCS is active, and an attendant transfers a call to the public network:

- The attendant dials participant A at extension 5-9999.
- The attendant and participant A talk for 1 minute.
- The attendant transfers the call to participant B at telephone number 444-5678.
- The participant B and participant B, talk for 5 minutes.
- The system creates two CDR records, one for call segment A-Attd, and one for call segment A-B.

Table 21: Attendant call transfer on a public network trunk on page 491 shows the CDR information that changes when ITCS or OTCS is active when an attendant transfers a call to an outgoing public network trunk.

Table 21: Attendant call transfer on a public network trunk

Call segment	Call duration	Condition code	Access code used	Calling number	Dialed number
Attd-B	0:01:0	A	345	Attd	4445678
A-B	0:05:0	A	345	59999	4445678

Intraswitch CDR

The system uses the Intraswitch CDR capability to create CDR records for calls to and from users on the same local server. Before the system can create an intraswitch CDR record, you must assign the Intraswitch CDR capability for one of the extensions.

If you enable ITCS for your system, and you assign the Intraswitch CDR capability for an extension, the system-wide ITCS overrides the Intraswitch CDR for the extension. When the system-wide ITCS overrides the Intraswitch CDR for the extension, the system generates trunk call records for an incoming trunk call to the extension. The system does not generate Intraswitch CDR records for an incoming trunk call to the extension.

The records that the system creates for the Intraswitch CDR capability are similar to the records that the system creates for other CDR records. However, some of the information differs. For example, the system does not provide TACs or circuit IDs for intraswitch calls, because that information is unnecessary.

Some calls might appear to be intraswitch CDR calls, but are actually trunk calls. For example, the system creates a trunk CDR record for an internal call to an extension that is forwarded to an outgoing trunk, even if you assigned the Intraswitch CDR capability for either station.

You can assign the Intraswitch CDR capability to:

- A Terminating Extension Group (TEG)
- A station
- A data module
- A Vector Directory Number (VDN)
- A Primary Rate Interface (PRI)
- An endpoint
- An access endpoint
- A hunt group

The number that appears in the **Dialed Number** field depends on whether you administered the CDR System Parameters to record hunt group/member or VDN information. You *cannot* assign the Intraswitch CDR capability to an attendant console or a CallVisor Adjunct-Switch Application Interface (ASAI) station.

Note that the system generates a CDR record for a call only if the user is the caller or the recipient of the call, and has the Intraswitch CDR capability active for the extension of the user. For example, if the user participates in the call as the result of Call Pickup or Call Forwarding, the system does not create a CDR record.

CDR Privacy

Use the CDR Privacy capability to maintain the privacy of the caller. The system replaces some of the digits that the user dials with blanks. The system records the call information, including the account number that the user enters. But the CDR information does not show the telephone number that the user dials.

You can assign the CDR Privacy capability individually to each of your users.You decide the number of digits that the system replaces with blanks. The system then uses this information for all calls of the users to whom you assign the CDR Privacy capability.

The CDR Privacy capability does not apply under the following conditions:

- Some countries require that the system replace a specific number of the digits that the user dials with blanks. If a country requires that the system replace a specific number of the digits that the user dials with blanks, the requirement applies to all calls.
- When an adjunct-originated call is made on behalf of a hunt group, and the **Calls to Hunt Group - Record** field on the CDR System Parameter screen is set to **group-ext**, CDR Privacy does not apply. However, CDR Privacy does apply if the **Hunt Group - Record** field is set to member extension.
- When an adjunct-originated call is made on behalf of a hunt group and the **Calls to Hunt Group - Record** field on the CDR System Parameter screen is set to **member-ext**, then CDR Privacy applies.
- Some report processors do not support the CDR Privacy capability.

CDR output

When operating in Legacy CDR mode, you can administer two CDR output ports: the Primary and the Secondary. You can administer different CDR formats for each of these two output ports. The Secondary port is generally used to troubleshoot network issues, or view CDR records locally.

CDR record formats

Beginning with Communication Manager 4.0, a new field **Use Legacy CDR Formats?** on the CDR System Parameters screen allows the system administrator to choose either the Communication Manager 3.x (legacy) CDR formats, or the new Communication Manager 4.0 formats to create CDR records for the system.

The default value for this field is **y** which utilizes the legacy formats.

When the **Use Legacy CDR Formats** field is set to **n,** the system uses the Communication Manager 4.0 formats. The **INS** field in the CDR records increases from three to five characters and the **Attendant Console** field increases from two characters to four characters.

Note:
For information on CDR formats for Communication Manager 4. 0, see Table 25 through Table 42 of this document. For more information on legacy CDR formats, see Table 43 through Table 60.

Note:
The CDR record tables that changed for Communication Manager 4.0 are Table 26, Table 31, Table 34, Table 35, Table 36, Table 37, Table 38, Table 39, and Table 42. All other CDR record tables remain unchanged between Communication Manager 4.0 and prior releases.

For more information, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

The system sends two types of records to the CDR output device, a date record and a call detail record.

Date record format

CDR sends date information to the CDR device once a day at midnight, or when someone connects the device to the system. The record that the system generates at this time is a noncall record, and contains only the information that is shown in one of the date record formats.

Three date record formats exist:

- CDRU
- Printer
- TELESEER

The records that the system sends to the TELESEER and the printer contain the date only. The records to the CDRU contain time. These tables are the same for "legacy" and Communication Manager 4.0.

See the following tables for date record formats:

- Table 22: Date record format to LSU, LSU-expand, unformatted, and customized on page 494

- Table 23: Date record format for printer and expanded on page 494
- Table 24: Date record format for TELESEER 59 character, int-proc, int-direct, and int-ISDN on page 495

Table 22: Date record format to LSU, LSU-expand, unformatted, and customized

Position	Description
1-2	Hour (leading 0 added if needed)
3	Colon (:)
4-5	Minute (leading 0 added if needed)
6	Blank
7-8	Month (leading 0 added if needed)
9	Slash (/)
10-11	Day (leading 0 added if needed)
12	Carriage return
13	Line feed
14-16	Null

Table 23: Date record format for printer and expanded

Position	Data field description
1-2	Month (leading 0 added if needed)
3	Space
4-5	Day (leading 0 added if needed)
6	Carriage return
7	Line feed
8-10	Null

Table 24: Date record format for TELESEER 59 character, int-proc, int-direct, and int-ISDN

Position	Data field description
1-2	Month (leading 0 added if needed)
3-4	Day
5	Carriage return
6	Line feed
7-9	Null

Customized CDR call record formats

You can use the customized record formats to define the call records for your system. You can determine the data elements that you want, and the position of the data elements in the record.

However, the device that you use to interpret the CDR data must be programmed to accept the data formats that you choose. Consult your Avaya representative before you use a customized record format.

Standard CDR call record formats for Communication Manager 4.0

See the following tables for a description of the standard call record formats for Communication Manager 4.0:

Table 25: CDR data format - TELESEER for Communication Manager 4.0 or later

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	Access code dialed
	1 of 2

Table 25: CDR data format - TELESEER for Communication Manager 4.0 or later

Position	Description
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code
54	facilities restriction level (FRL)
55	inter-exchange carrier (IXC)
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-76	Space
77	Carriage return
78	Line feed
79-81	Null
	2 of 2

Table 26: CDR data format - ISDN TELESEER for Communication Manager 4.0 or later

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	IXC

Table 26: CDR data format - ISDN TELESEER for Communication Manager 4.0 or later

Position	Description
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code
54	INS (units)
55	FRL
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-73	INS (ten-thousands, thousands, hundreds, tens)
74-78	Space
79	Line feed
80-82	Null

Table 27: CDR data format - enhanced TELESEER for Communication Manager 4.0 or later

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-16	IXC code
17-19	Access code used

Table 27: CDR data format - enhanced TELESEER for Communication Manager 4.0 or later

Position	Description
20-34	Dialed number
35-39	Calling number
40-54	Account code
55	ISDN NSV (units)
56	FRL
57-59	Incoming circuit ID
60-62	Outgoing circuit ID
63	Feature flag
64-70	Authorization code
71-74	ISDN NSV (ten-thousands, thousands, hundreds, tens)
75-78	Space
79	Carriage return
80	Line feed
81-83	Null

Table 28: CDR data format - 59 character for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-12	Access code dialed
13-15	Access code used
16-30	Dialed number

Table 28: CDR data format - 59 character for Communication Manager 4.0 or later

Position	Description
31-35	Calling number
36-50	Account code
51	FRL
52	IXC
53-55	Incoming circuit ID
56-58	Outgoing circuit ID
59	Carriage return
60	Line feed
61-63	Null

Table 29: CDR data format - printer for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	Access code dialed
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
	1 of 2

Table 29: CDR data format - printer for Communication Manager 4.0 (continued)or

Position	Description
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66-69	Space
70	FRL
71	Space
72	IXC
73	Space
74-76	Incoming circuit ID
77	Space
78-80	Outgoing Circuit ID
81	Space
82	Feature flag
83	Carriage return
84	Line feed
	2 of 2

Table 30: CDR data format - ISDN printer for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
	1 of 3

Table 30: CDR data format - ISDN printer for Communication Manager 4.0 or later

Position	Description
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	IXC
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66	Space
67-70	INS (ten thousands thousands, hundreds, tens)
71	Space
72	INS (units)
73	Space
74	FRL
75	Space
76-78	Incoming circuit ID
79	Space
80-82	Outgoing circuit ID
	2 of 3

Table 30: CDR data format - ISDN printer for Communication Manager 4.0 or later

Position	Description
83	Space
84	Feature flag
85	Carriage return
86	Line feed
	3 of 3

Table 31: CDR data format - enhanced printer for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	IXC code
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-43	Calling number
44	Space
45-59	Account code
	1 of 2

Table 31: CDR data format - enhanced printer for Communication Manager 4.0 or later

Position	Description
60	Space
61-67	Authorization code
68	Space
69-73	ISDN NSV
74	Space
75	FRL
76	Space
77-79	Incoming circuit ID
80	Space
81-83	Outgoing Circuit ID
84	Space
85	Feature flag
86	Carriage return
87	Line feed
	2 of 2

Table 32: CDR data format - LSU-expand for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
	1 of 3

Table 32: CDR data format - LSU-expand for Communication Manager 4.0 or later

Position	Description
12	Space
13-15	Access code dialed
16-18	Access code used
19	Space
20-34	Dialed number
35	Space
36-39	Calling number
40	Space
41-45	Account code
46	Space
47-53	Authorization code
54-57	Space
58	FRL
59	Space
60	Calling number (1st digit)
61	Space
62-63	Incoming circuit ID (tens, units)
64	Space
65	Feature flag
66	Space
67-68	Outgoing circuit ID (tens, units)
69	Space
70	Outgoing circuit ID (hundreds)
71	Space
72	Incoming circuit ID (hundreds)
73	IXC
74	Carriage return
	2 of 3

Table 32: CDR data format - LSU-expand for Communication Manager 4.0 or later

Position	Description
75	Line feed
76-78	Null
	3 of 3

Table 33: CDR data format - LSU for Communication Manager 4.0 or later

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-8	Access code dialed
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (first 5 digits)
36-42	Authorization code or digits 6-12 of the account code
43-44	Space or digits 13-14 of account code
45	FRL or digit 15 of the account code
46	Calling number (1st digit)
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	IXC
55	Carriage return
56	Line feed
57-59	Null

Table 34: CDR data format - ISDN LSU for Communication Manager 4.0 or later

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-8	IXC
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (digits 1-5)
36-42	Authorization code or digits 6-12 of the account code
43-45	INS (ten thousands, thousands, hundreds, or digits 13-14 of account code
46-47	INS (tens, units), FRL, or digit 15 of the account code
48	Calling number (1st digit of a 5-digit calling number)
49-50	Incoming circuit ID (tens, units)
51	Feature flag
52-54	Outgoing circuit ID (tens, units, hundreds)
55	Incoming circuit ID (hundreds)
56	FRL
57	Carriage return
58	Line feed
57-61	Null

Table 35: CDR data format - enhanced LSU for Communication Manager 4.0 or later

Position	Description
1	Duration-hours
2-3	Duration-minutes

Table 35: CDR data format - enhanced LSU for Communication Manager 4.0 or later

Position	Description
4	Duration-tenths of minutes
5	Condition code
6-9	IXC code
10-12	Access code used
13-27	Dialed number
28-31	Calling number
32-35	Account code (digits 1-4)
36-42	Authorization code or digits 6-12 of the account code
43-47	ISDN NSV
48	1st digit of a 5-digit calling number
49-50	Incoming circuit ID (tens, units)
51	Feature flag
52-54	Outgoing circuit ID (tens, units, hundreds)
55	Incoming circuit ID (hundreds)
56	FRL
57	Carriage return
58	Line feed
59-61	Null

Table 36: CDR data format - expanded for Communication Manager 4.0 or later

Position	Description
1-2, 3-4	Time of day-hours, -minutes
5	Space
6, 7-8, 9	Duration-hours, minutes, tenths of minute
10	Space
11	Condition code
	1 of 3

Table 36: CDR data format - expanded for Communication Manager 4.0

Position	Description
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73-76	Space
77	FRL
78	Space
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
89-92	Attendant console
93	Space
94-97	Incoming trunk access code
98	Space
99-100	Node number
	2 of 3

Table 36: CDR data format - expanded for Communication Manager 4.0

Position	Description
101	Space
102-106	INS
107	Space
108-110	IXC
111	Space
112	Bearer capability class (BCC)
113	Space
114	Message-Associated User-to-User Signaling (MA-UUI)
115	Space
116	Resource flag
117	Space
118-121	Packet count
122	Space
123	temporary-signaling connection (TSC) flag
124	Space
125-133	Reserved
134	Space
135	Carriage return
136	Line feed
137-139	Null
	3 of 3

Table 37: CDR data format - enhanced expanded for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73	Space
74-75	Time in queue
76	Space
77	FRL
78	Space
	1 of 3

Table 37: CDR data format - enhanced expanded for Communication Manager 4.0 or later

Position	Description
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
89-92	Attendant console
93	Space
94-97	Incoming TAC
98	Space
99-100	Node number
101	Space
102-106	ISDN NSV
107	Space
108-111	IXC
112	Space
113	BCC
114	Space
115	MA-UUI
116	Space
117	Resource flag
118	Space
119-122	Packet count
123	Space
124	TSC flag
	2 of 3

Table 37: CDR data format - enhanced expanded for Communication Manager 4.0 or later

Position	Description
125	Space
126-127	Bandwidth
128	Space
129-134	ISDN CC (digits 1-6)
135-139	ISDN CC (digits 7-11) / periodic pulse metering (PPM) count (1-5)
140-150	Reserved for future use
151	Carriage return
152	Line feed
153-155	Null
	3 of 3

Table 38: CDR data format - unformatted for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
43-57	Account code
58-64	Authorization code
	1 of 2

Table 38: CDR data format - unformatted for Communication Manager 4.0

Position	Description
65-66	Space
67	FRL
68-70	Incoming circuit ID (hundreds, tens, units)
71-73	Outgoing circuit ID (hundreds, tens, units)
74	Feature flag
75-78	Attendant console
79-82	Incoming TAC
83-84	Node number
85-89	INS
90-92	IXC
93	BCC
94	MA-UUI
95	Resource flag
96-99	Packet count
100	TSC flag
101-104	Reserved
105	Carriage return
106	Line feed
107-109	Null
	2 of 2

Table 39: CDR data format - enhanced unformatted for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
	1 of 3

Table 39: CDR data format - enhanced unformatted for Communication Manager 4.0 or later

Position	Description
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
43-57	Account code
58-64	Authorization code
65-66	Space
67	FRL
68-70	Incoming circuit ID
71-73	Outgoing circuit ID
74	Feature flag
75-78	Attendant console number
79-82	Incoming TAC
83-84	Node number
85-89	ISDN NSV
90-93	IXC code
94	BCC
95	MA-UUI
96	Resource flag
97-100	Packet count
101	TSC flag
	2 of 3

Table 39: CDR data format - enhanced unformatted for Communication Manager 4.0 or later

Position	Description
102-103	Bandwidth
104-109	ISDN CC (digits 1-6)
110-114	ISDN CC (digits 7-11)/PPM count (1-5)
115-118	Reserved for future use
119	Carriage return
120	Line feed
121-123	Null
	3 of 3

Table 40: CDR data format - int process for Communication Manager 4.0 or later

Position	Description
1-2	Format code
3-4	Time of day-hours
5-6	Time of day-minutes
7	Duration-hours
8-9	Duration-minutes
10	Duration-tenths of minutes
11	Space
12	Condition code
13	Space
14-16	Access code dialed
17-19	Access code used
20	Space
21-38	Dialed number (digits 1-18)
39-43	Calling number (digits 1-5)
	1 of 2

Table 40: CDR data format - int process for Communication Manager 4.0 or later

Position	Description
44	Space
45-59	Account code (digits 1-15)
60	Space
61	IXC
62	FRL
63-65	Space
66-67	Incoming circuit ID (digits 1-2)
68-70	Space
71-72	Outgoing circuit ID (digits 1-2)
73	Space
74-78	PPM count (digits 1-5)
79	Carriage return
80	Line feed
81-83	Null
	2 of 2

Table 41: CDR data format - int-direct for Communication Manager 4.0 or later

Position	Description
1-2	Day of month
3-4	Month
5-6	Year
7	Space
8-9	Time of day-hours
10-11	Time of day-minutes
12	Space
	1 of 2

Table 41: CDR data format - int-direct for Communication Manager 4.0 or later

Position	Description
13	Duration-hours
14-15	Duration-minutes
16	Duration-tenths of minutes
17	Space
18	Condition code
19	Space
20-22	Access code dialed
23-25	Access code used
26	Space
27-44	Dialed number used
45	Space
46-50	Calling number
51	Space
52-66	Account code
67	Space
68-72	PPM count
73	Space
74-75	Incoming circuit ID
76	Space
77-78	Outgoing circuit ID
79	Carriage return
80	Line feed
	2 of 2

Table 42: CDR data format - int-ISDN for Communication Manager 4.0 or later

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73	Space
74	Line feed
75	Space
76	FRL
77	Space
	1 of 3

Table 42: CDR data format - int-ISDN for Communication Manager 4.0 or later

Position	Description
78	Incoming circuit ID (hundreds)
79	Incoming circuit ID (tens)
80	Incoming circuit ID (units)
81	Space
82-84	Outgoing circuit ID
85	Space
86	Feature flag
87	Space
88-91	Attendant console (1st digit)
92	Space
93-96	Incoming trunk access code
97	Space
98-99	Node number
100	Space
101-105	INS
106	Space
107-110	IXC
111	Space
112	BCC
113	Space
114	MA-UUI
115	Space
116	Resource flag
117	Space
118-123	Reserved
	2 of 3

Table 42: CDR data format - int-ISDN for Communication Manager 4.0 or later

Position	Description
124-128	PPM or reserved
129-135	Space
136	Carriage return
137	Line feed
138-140	Null
	3 of 3

Standard CDR call record formats for "legacy" CDR

See the following tables for a description of the standard call record formats for legacy CDR:

Note:
"Legacy" CDR refers to CDR formats for releases before Communication Manager Release 4.0.

Table 43: CDR data format - TELESEER for Communication Manager 3.x

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	Access code dialed
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code

Table 43: CDR data format - TELESEER for Communication Manager 3.x

Position	Description
54	facilities restriction level (FRL)
55	inter-exchange carrier (IXC)
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-76	Space
77	Carriage return
78	Line feed
79-81	Null

Table 44: CDR data format - ISDN TELESEER for Communication Manager 3.x

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-15	IXC
16-18	Access code used
19-33	Dialed number
34-38	Calling number
39-53	Account code
54	INS (units)
55	FRL

Table 44: CDR data format - ISDN TELESEER for Communication Manager 3.x

Position	Description
56-58	Incoming circuit ID
59-61	Outgoing circuit ID
62	Feature flag
63-69	Authorization code
70-71	INS (hundreds, tens)
72-76	Space
77	Line feed
78-80	Null

Table 45: CDR data format - enhanced TELESEER for Communication Manager 3.x

Position	Description
1-3	Space
4-5	Time of day-hours
6-7	Time of day-minutes
8	Duration-hours
9-10	Duration-minutes
11	Duration-tenths of minutes
12	Condition code
13-16	IXC code
17-19	Access code used
20-34	Dialed number
35-39	Calling number
40-54	Account code
55	ISDN NSV (units)
56	FRL
57-59	Incoming circuit ID
60-62	Outgoing circuit ID

Table 45: CDR data format - enhanced TELESEER for Communication Manager 3.x

Position	Description
63	Feature flag
64-70	Authorization code
71-72	ISDN NSV (hundreds, tens)
73-76	Space
77	Carriage return
78	Line feed
79-81	Null

Table 46: CDR data format - 59 character for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-12	Access code dialed
13-15	Access code used
16-30	Dialed number
31-35	Calling number
36-50	Account code
51	FRL
52	IXC
53-55	Incoming circuit ID
56-58	Outgoing circuit ID
59	Carriage return

Table 46: CDR data format - 59 character for Communication Manager 3.x

Position	Description
60	Line feed
61-63	Null

Table 47: CDR data format - printer for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	Access code dialed
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66-69	Space
	1 of 2

Table 47: CDR data format - printer for Communication Manager 3.x (continued)

Position	Description
70	FRL
71	Space
72	IXC
73	Space
74-76	Incoming circuit ID
77	Space
78-80	Outgoing circuit ID
81	Space
82	Feature flag
83	Carriage return
84	Line feed
	2 of 2

Table 48: CDR data format - ISDN printer for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	IXC
	1 of 2

Table 48: CDR data format - ISDN printer for Communication Manager 3.x (continued)

Position	Description
16	Space
17-19	Access code used
20	Space
21-35	Dialed number
36	Space
37-41	Calling number
42	Space
43-57	Account code
58	Space
59-65	Authorization code
66	Space
67-68	INS (hundreds, tens)
69	Space
70	INS (units)
71	Space
72	FRL
73	Space
74-76	Incoming circuit ID
77	Space
78-80	Outgoing circuit ID
81	Space
82	Feature flag
83	Carriage return
84	Line feed
	2 of 2

Table 49: CDR data format - enhanced printer for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	IXC code
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-43	Calling number
44	Space
45-59	Account code
60	Space
61-67	Authorization code
68	Space
69-71	ISDN NSV
72	Space
73	FRL
74	Space
	1 of 2

Table 49: CDR data format - enhanced printer for Communication Manager 3.x

Position	Description
75-77	Incoming circuit ID
78	Space
79-81	Outgoing circuit ID
82	Space
83	Feature flag
84	Carriage return
85	Line feed
	2 of 2

Table 50: CDR data format - LSU-expand for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-15	Access code dialed
16-18	Access code used
19	Space
20-34	Dialed number
35	Space
36-39	Calling number
	1 of 2

Table 50: CDR data format - LSU-expand for Communication Manager 3.x

Position	Description
40	Space
41-45	Account code
46	Space
47-53	Authorization code
54-57	Space
58	FRL
59	Space
60	Calling number (1st digit)
61	Space
62-63	Incoming circuit ID (tens, units)
64	Space
65	Feature flag
66	Space
67-68	Outgoing circuit ID (tens, units)
69	Space
70	Outgoing circuit ID (hundreds)
71	Space
72	Incoming circuit ID (hundreds)
73	IXC
74	Carriage return
75	Line feed
76-78	Null
	2 of 2

Table 51: CDR data format - LSU for Communication Manager 3.x

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-8	Access code dialed
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (first 5 digits)
36-42	Authorization code or digits 6-12 of the account code
43-44	Space or digits 13-14 of account code
45	FRL or digit 15 of the account code
46	Calling number (1st digit)
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	IXC
55	Carriage return
56	Line feed
57-59	Null

Table 52: CDR data format - ISDN LSU for Communication Manager 3.x

Position	Description
1	Duration-hours
2-3	Duration-minutes

Table 52: CDR data format - ISDN LSU for Communication Manager 3.x (continued)

Position	Description
4	Duration-tenths of minutes
5	Condition code
6-8	IXC
9-11	Access code used
12-26	Dialed number
27-30	Calling number (digits 2-5 for a 5-digit dial plan)
31-35	Account code (digits 1-5)
36-42	Authorization code or digits 6-12 of the account code
43-44	INS or digits 13-14 of account code
45	INS (3rd digit), FRL, or digit 15 of the account code
46	Calling number (1st digit of a 5-digit calling number)
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	FRL
55	Carriage return
56	Line feed
57-59	Null

Table 53: CDR data format - enhanced LSU for Communication Manager 3.x

Position	Description
1	Duration-hours
2-3	Duration-minutes
4	Duration-tenths of minutes
5	Condition code
6-9	IXC code

Table 53: CDR data format - enhanced LSU for Communication Manager 3.x

Position	Description
10-12	Access code used
13-27	Dialed number
28-31	Calling number
32-35	Account code (digits 1-4)
36-42	Authorization code or digits 6-12 of the account code
43-45	ISDN NSV
46	1st digit of a 5-digit calling number
47-48	Incoming circuit ID (tens, units)
49	Feature flag
50-52	Outgoing circuit ID (tens, units, hundreds)
53	Incoming circuit ID (hundreds)
54	FRL
55	Carriage return
56	Line feed
57-59	Null

Table 54: CDR data format - expanded for Communication Manager 3.x

Position	Description
1-2, 3-4	Time of day-hours, -minutes
5	Space
6, 7-8, 9	Duration-hours, minutes, tenths of minute
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
	1 of 3

Table 54: CDR data format - expanded for Communication Manager 3.x (continued)

Position	Description
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73-76	Space
77	FRL
78	Space
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
89-90	Attendant console
91	Space
92-95	Incoming trunk access code
96	Space
97-98	Node number
99	Space
100-102	INS
103	Space
	2 of 3

Table 54: CDR data format - expanded for Communication Manager 3.x (continued)

Position	Description
104-106	IXC
107	Space
108	Bearer capability class (BCC)
109	Space
110	Message-Associated User-to-User Signaling (MA-UUI)
111	Space
112	Resource flag
113	Space
114-117	Packet count
118	Space
119	temporary-signaling connection (TSC) flag
120	Space
121-129	Reserved
130	Space
131	Carriage return
132	Line feed
133-135	Null
	3 of 3

Table 55: CDR data format - enhanced expanded for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
	1 of 4

Table 55: CDR data format - enhanced expanded for Communication Manager 3.x

Position	Description
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73	Space
74-75	Time in queue
76	Space
77	FRL
78	Space
79-81	Incoming circuit ID
82	Space
83-85	Outgoing circuit ID
86	Space
87	Feature flag
88	Space
	2 of 4

Table 55: CDR data format - enhanced expanded for Communication Manager 3.x

Position	Description
89-90	Attendant console
91	Space
92-95	Incoming TAC
96	Space
97-98	Node number
99	Space
100-102	ISDN NSV
103	Space
104-107	IXC code
108	Space
109	BCC
110	Space
111	MA-UUI
112	Space
113	Resource flag
114	Space
115-118	Packet count
119	Space
120	TSC flag
121	Space
122-123	Bandwidth
124	Space
125-130	ISDN CC (digits 1-6)
131-135	ISDN CC (digits 7-11) / periodic pulse metering (PPM) count (1-5)
136-146	Reserved for future use
	3 of 4

Table 55: CDR data format - enhanced expanded for Communication Manager 3.x

Position	Description
147	Carriage return
148	Line feed
149-151	Null
	4 of 4

Table 56: CDR data format - unformatted for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
43-57	Account code
58-64	Authorization code
65-66	Space
67	FRL
68-70	Incoming circuit ID (hundreds, tens, units)
71-73	Outgoing circuit ID (hundreds, tens, units)
74	Feature flag
75-76	Attendant console
77-80	Incoming TAC
	1 of 2

Table 56: CDR data format - unformatted for Communication Manager 3.x

Position	Description
81-82	Node number
83-85	INS
86-88	IXC
89	BCC
90	MA-UUI
91	Resource flag
92-95	Packet count
96	TSC flag
97-100	Reserved
101	Carriage return
102	Line feed
103-105	Null
	2 of 2

Table 57: CDR data format - enhanced unformatted for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-13	Access code dialed
14-17	Access code used
18-32	Dialed number
33-42	Calling number
	1 of 2

Table 57: CDR data format - enhanced unformatted for Communication Manager 3.x

Position	Description
43-57	Account code
58-64	Authorization code
65-66	Time in queue
67	FRL
68-70	Incoming circuit ID
71-73	Outgoing circuit ID
74	Feature flag
75-76	Attendant console number
77-80	Incoming TAC
81-82	Node number
83-87	ISDN NSV
88-89	IXC code
90	BCC
91	MA-UUI
92	Resource flag
93-96	Packet count
97	TSC flag
98-99	Bandwidth
100-105	ISDN CC (digits 1-6)
106-110	ISDN CC (digits 7-11)/PPM count (1-5)
111-114	Reserved for future use
115	Carriage return
116	Line feed
117-119	Null
	2 of 2

Table 58: CDR data format - int process for Communication Manager 3.x

Position	Description
1-2	Format code
3-4	Time of day-hours
5-6	Time of day-minutes
7	Duration-hours
8-9	Duration-minutes
10	Duration-tenths of minutes
11	Space
12	Condition code
13	Space
14-16	Access code dialed
17-19	Access code used
20	Space
21-38	Dialed number (digits 1-18)
39-43	Calling number (digits 1-5)
44	Space
45-59	Account code (digits 1-15)
60	Space
61	IXC
62	FRL
63-65	Space
66-67	Incoming circuit ID (digits 1-2)
68-70	Space
71-72	Outgoing circuit ID (digits 1-2)
73	Space
74-78	PPM count (digits 1-5)
	1 of 2

Table 58: CDR data format - int process for Communication Manager 3.x (continued)

Position	Description
79	Carriage return
80	Line feed
81-83	Null
	2 of 2

Table 59: CDR data format - int-direct for Communication Manager 3.x

Position	Description
1-2	Day of month
3-4	Month
5-6	Year
7	Space
8-9	Time of day-hours
10-11	Time of day-minutes
12	Space
13	Duration-hours
14-15	Duration-minutes
16	Duration-tenths of minutes
17	Space
18	Condition code
19	Space
20-22	Access code dialed
23-25	Access code used
26	Space
27-44	Dialed number used
45	Space
	1 of 2

Table 59: CDR data format - int-direct for Communication Manager 3.x (continued)

Position	Description
46-50	Calling number
51	Space
52-66	Account code
67	Space
68-72	PPM count
73	Space
74-75	Incoming circuit ID
76	Space
77-78	Outgoing circuit ID
79	Carriage return
80	Line feed
	2 of 2

Table 60: CDR data format - int-ISDN for Communication Manager 3.x

Position	Description
1-2	Time of day-hours
3-4	Time of day-minutes
5	Space
6	Duration-hours
7-8	Duration-minutes
9	Duration-tenths of minutes
10	Space
11	Condition code
12	Space
13-16	Access code dialed
	1 of 3

Table 60: CDR data format - int-ISDN for Communication Manager 3.x (continued)

Position	Description
17	Space
18-21	Access code used
22	Space
23-37	Dialed number
38	Space
39-48	Calling number
49	Space
50-64	Account code
65	Space
66-72	Authorization code
73	Space
74	Line feed
75	Space
76	FRL
77	Space
78	Incoming circuit ID (hundreds)
79	Incoming circuit ID (tens)
80	Incoming circuit ID (units)
81	Space
82-84	Outgoing circuit ID
85	Space
86	Feature flag
87	Space
88-89	Attendant console (1st digit)
90	Space
	2 of 3

Table 60: CDR data format - int-ISDN for Communication Manager 3.x (continued)

Position	Description
91-94	Incoming trunk access code
95	Space
96-97	Node number
98	Space
99-101	INS
102	Space
103-106	IXC
107	Space
108	BCC
109	Space
110	MA-UUI
111	Space
112	Resource flag
113	Space
114-119	Reserved
120-124	PPM or reserved
125-131	Space
132	Carriage return
133	Line feed
134-136	Null
	3 of 3

Call detail record field descriptions

The following information describes the CDR data that the system collects for each call, and the length of each field. The information is right adjusted in the **CDR record** field, unless otherwise indicated. The customized field name appears, if the field names for customized records differ from the names of standardized records.

- Access Code Dialed

  Customized field name: **code-dial**

  Length: 3 or 4 digit

  This field contains the access code that the user dials to place an outgoing call. The access can be the automatic route selection (ARS) access code, an Automatic Alternate Routing (AAR) access code, or the access code of a specific trunk group. This field is also used to record the X.25 Feature Access Code of an outgoing X.25-addressed call.

- Access Code Used

  Custom field name: **code-used**

  Length: 3 or 4 digits

  This field is used only for outgoing calls when the system uses a trunk group that differs from the access code that the user dials. This field is not used when a user dials a TAC. For example, your system might use an FAC for ARS. This field contains the access code of the trunk group that the system uses to route the call. When the access code that the user dials, and the access code that the systems uses are the same, this field is blank.

  If you use ISDN or enhanced formats with TELESEER, LSU, or printer record types, this field contains the access code of the trunk group, even if the user dials the same access code.

  Length: 2 digits

  If an attendant participates in a call, this field contains the number of the attendant console.

- Account Code

  Custom field name: **acct-code**

  Length: 1 to 15 digits

  This field is either blank, or contains a number to associate call information with projects or account numbers. For some formats, a long account code overwrites spaces on the record that are assigned to other fields.

- Attendant Console

  Custom field name: **attd-console**

  Length: 2 digits

  If an attendant participates in a call, this field contains the number of the attendant console.

- Authorization Code

  Custom field name: **auth-code**

  Length: 4 to 13 digits

  This field contains the authorization code that the user used to make the call. The system truncates an authorization code to 7 digits for formats other than customized formats.

  Note that the authorization code for the non-ISDN format and the ISDN local storage init (LSU) format has fewer than 6 digits. The authorization code for the Enhanced LSU format has 5 digits. The system does not record the authorization on the 59-character record.

- Bandwidth

  Length: 2 digits

  This field contains the bandwidth of the wide band calls to support H0, H11, H12, and N x 64 kbps data rates. For Enhanced Expanded, Enhanced Unformatted, and customized record formats, this value in this field is the number of DSOs of 64-kbps channels that comprise a call.

- Bearer Capability Class

  Custom field name: **bcc**

  Length: 1 digit

  This field contains the bearer capability class (BCC) for ISDN calls. The BCC identifies various capabilities that are available for a ISDN call. Any one of the following BCCs can appear in this field.

  0 - Voice grade data and voice

  1 - Mode 1, 56 kbps synchronous data

  2 - Mode 2, less than 19.2 kbps synchronous or asynchronous data

  3 - Mode 3, 64 kbps data for Link Access Procedure data (LAPD) protocol

  4 - Mode 0, 64 kbps data clear

  M - Multimedia

  W - Wideband

Note:

The Bearer Capability Class field in the CDR records shows the capabilities that are available for a given call. It is *not* a report of the capabilities that were used for the call.

For intraswitch CDR records, the BCC field system provides information for wideband calls only.

- Calling Number

  Custom field name: **calling-num**

  Number of digits, standard: 1 to 10

  Number of digits, custom: 1 to 15

  For outgoing or intraswitch calls, this field contains the extension of the originating telephone user. For incoming and tandem calls, this field contains the TAC in standard formats. The fifth digit is the first digit of a 5-digit dialing plan.

  For formats in which the Calling Number field has 7 digits, the field contains the TAC of the incoming call.

  For Unformatted records or Expanded records, this field contains the number of the calling party. If the number of the calling party is unavailable, this field is blank for both the Unformatted and the Expanded record formats.

  For an outgoing, or an originating, NCA-TSC CDR record, this field contains the local extension of the noncall-associated/temporary-signaling connection (NCA-TSC) endpoint. This field is blank for terminating, tandem, or unsuccessful NCA-TSC CDR records.

- Calling Number/Incoming TAC

  Custom field name: **clg-num/in-tac**

  You can use this field on a customized record to display the calling number, if the calling number is available.

  If the calling party number is unavailable, this field contains the incoming TAC.

  For outgoing calls, this field contains the calling extension.

- Calling Party Category

  Custom field name: **clg-pty-cat**

  Length: 2 digits

  This field is used only on the customized format.This parameter is associated with R2MFC trunks.

- Carriage Return

  Custom field name: **return**

  The **ASCII** carriage return character, followed by a line feed, indicates the end of a call record.

- Condition Code

  Length: 1 character

  The condition code indicates the type of call that this record describes. For example, condition code C identifies a conference call, and condition code 7 identifies an ARS call.

  Table 61: Condition codes on page 548 shows the condition codes for most record formats. The condition codes for the 59-character format differ from the condition codes of the other record types. The codes that apply to 59-character records appear in parentheses in the table.

Table 61: Condition codes

Condition codes	Description
0	Identifies an intraswitch call, which is a call that originates and terminates on the switch
1 (A)	Identifies an attendant-handled call or an attendant-assisted call, except conference calls
4 (D)	Identifies an extremely long call or a call with an extremely high message count TSC. An extremely long call is a call that lasts for 10 or more hours. An extremely high message count TSC is 9999 or more messages. When a call exceeds10 hours, the system creates a call record with this condition code and a duration of 9 hours, 59 minutes, and 1-9 tenths of a minute. The system creates a similar call record with this condition code after each succeeding 10-hour period. When the call terminates, the system creates a final call record with a different condition code that identifies the type of call.
6 (E)	Identifies calls where no CDR records are generated because the CDR (SMDR) processes do not have enough resources available to generate a record. For example, a CDR resource shortage could be the CDR buffer space available. The CDR record that includes this condition code also includes the time and the duration of the CDR resource outage.
7 (G)	Identifies calls that use the AAR or ARS feature.
8 (H)	Identifies calls that are served on a delayed basis by the Ringback Queuing feature.
	1 of 3

Table 61: Condition codes (continued)

Condition codes	Description
9 (I)	Identifies: • An incoming call • A tandem call • An incoming NCA-TSC call • A tandem NCA-TSC call
A	Identifies an outgoing call.
B	Identifies an adjunct-placed outgoing call.
C (L)	Identifies a conference call. For trunk CDR, the system creates a separate call record, with this condition code, for each incoming or outgoing trunk that is used during the conference call. If you disable ITCS and OTCS, the system records the extension of the originator of the conference call. The system does not record any other extension. If you disable ITCS, and you administer the originator of the conference call to use Intraswitch CDR, the system generates a call with this condition code whenever the originator of the conference dials a nontrunk conference participant. If ITCS is active, and you do *not* administer the originator of the conference call to use Intraswitch CDR, the system generates a call with this condition code whenever the originator of the conference dials an intraswitch conference participant.
E (N)	Identifies a call that the system does not complete because the following facilities to complete the call are unavailable: • Outgoing calls – The trunks are busy, and no queue exists. – The trunks are busy, and the queue is full. • Incoming calls – The extension is busy. – The extension is unassigned. This condition code also identifies an ISDN Call By Call Service Selection call that is unsuccessful because of an administered trunk usage allocation plan. Incoming trunk calls to a busy telephone do not generate a CDR record.
	2 of 3

Table 61: Condition codes (continued)

Condition codes	Description
F	Identifies a call that the system does not complete because of one of the following conditions: ● The originator of the calls has insufficient calling privileges. ● An NSF mismatch occurs for an ISDN call. ● An authorization mismatch occurs for a data call.
G	Identifies a call that the system terminates to a ringing station.
H	Notes that the system abandoned a ring call.
I	Identifies a call that the system terminates to a busy station.
J	Identifies an incoming trunk call that is a new connection that uses Additional Network Feature-Path Replacement (ANF-PR) or DCS with Rerouting. For more information on QSIG and ANF-PR, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
K	Identifies an outgoing trunk call that is a new connection that uses ANF-PR or DCS with Rerouting. For more information on QSIG and ANF-PR, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
M	Identifies an outgoing trunk calls that the system disconnects because the call exceeds the time allowed.
T	Identifies CDR records for calls that meet the following conditions: ● The **Condition Code 'T' for Redirected Calls?** field on the CDR System Parameters screen is set to **y**. ● The incoming trunk group is direct inward dialing (DID). ● The system automatically redirects an incoming call off of the server.
	3 of 3

If the **Trunk-group CDR Reports** field is set to **ring**, CDR records the ring time to answer or abandon for incoming calls that the trunk group originates. CDR also indicates if the incoming destination is busy. This record is separate from the normal call duration record that is printed for an answered call. This information is indicated by the condition code.

When a trunk group originates an incoming call with this option set that is terminated to an internal destination, the call is tracked from the time that ringing feedback is given to the originator. If the call is answered, a CDR record is printed with condition code G, and the duration reflects the time between the start of ringing and when the call is answered. If the call is abandoned before being answered, the system prints a record with condition code H, and the duration reflects the time between the start of ringing and the time that the call was abandoned. If the destination is busy, a CDR record is printed with condition code I and a duration of 0.

- Condition code overrides

  If two condition codes apply to the same call, one code overrides the other. The following matrix, Table 62: Condition code override matrix on page 551, defines the overrides.

  To use this table, locate one of the condition codes that you want to compare in the row of condition codes at the top of the table. Then locate the other condition code that you want to compare in the column of condition code at the far left of the table. Then locate the intersection of these two condition codes. The condition code at the intersection of the two condition codes, is the condition code that the system uses. For example, assume that the system can assign condition 7 and condition code A to the same call. The system uses condition code 7 for the call.

  If the intersection of the two condition codes contains a dash, the two conditions never occur for the same call.

Table 62: Condition code override matrix

Condition codes																
	0	**1**	**4**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**E**	**F**	**J**	**K**	**M**	**T**
0	-	0	4	6	0	-	-	-	B	C	-	-	-	-	-	-
1	0	-	4	6	1	-	9	1	B	C	E	-	J	K	-	-
4	4	4	-	6	4	4	4	4	4	4	-	-	J	K	-	-
6	6	6	6	-	6	6	6	6	6	6	6	6	6	6	-	-
7	0	1	4	6	-	7	9	7	B	C	E	F	J	K	-	-
8	-	-	4	6	7	-	-	8	B	C	E	-	-	K	-	-
9	-	9	4	6	9	-	-	-	-	C	E	F	-	-	-	-
A	-	1	4	6	7	8	-	-	B	C	E	F	-	-	-	-

1 of 2

Table 62: Condition code override matrix (continued)

Condition codes																
	0	**1**	**4**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**E**	**F**	**J**	**K**	**M**	**T**
B	B	B	4	6	B	B	-	B	-	B	E	F	-	K	-	-
C	C	C	4	6	C	C	C	C	B	-	-	-	J	K	M	-
E	-	E	-	6	E	E	E	E	E	-	-	-	E	E	-	-
F	-	-	-	6	F	-	F	F	F	-	-	-	F	F	-	-
J	-	J	J	6	J	-	-	-	-	J	E	F	-	-	-	-
K	-	K	K	6	K	K	-	-	-	K	E	F	-	-	-	-
M	-	-	-	-	-	-	-	-	-	M	-	-	-	-	-	-
T	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

2 of 2

- Country From

  Custom field name: **country-from**

  Number of digits: 3

  The **country-from** field is a country number, used with the Multinational Locations feature, for currency conversion. The field length is 3, the same as the length of the **Country code for CDR** field on the Location Parameters screen. The **country-from** field indicates the administered CDR country code of the PBX interface of the calling party.

- Country To

  Custom field name: **country-to**

  Number of digits: 3

  The **country-to** field is a country number, used with the Multinational Locations feature, for currency conversion. The field length is 3, the same as the length of the **Country code for CDR** field on the Location Parameters screen. The **country-to** field indicates the administered CDR country code of the PBX interface of the called party.

Note:
If the Multinational Locations feature is turned off in the license file, the key words **country-from** and **country-to** are invalid.

- **Date**

  You can include the date in customized CDR records only. The format of the date is based on the value of the **CDR Date Format** field on the CDR System Parameters screen.

- **Dialed Number**

  Custom field name: **dialed-num**

  Length: 23 digits

  For an outgoing call, this field contains the number that the system user dials. For an incoming call, this field contains the extension of the system user that is called. If a Dialed Number Identification System (DNIS) exists, the field contains the implied extension for an incoming call. If the originator of the call dials more than eighteen digits, the system truncates the number or the extension to 18 digits. The system truncates the least significant digits, starting at the right. For example, if the originator of the call dials the number 11111111111111111852, the system truncates the digits 852.

  – CDR Privacy

    If CDR Privacy is active for the calling number, and this CDR record is for an outgoing call, the system modifies and records the number that the user dials according to the following procedure:

    - The system truncates the numbers that the user dials to 18 digits
    - The system replaces some of digits with blanks to ensure the privacy of the call.

  – NCA-TSC or tandem NCA-TSC outgoing calls

    For outgoing NCA-TSC or tandem NCA-TSC calls, this field contains the digits that the user dials, and that the system uses to establish a route to the server.

    The field contains the local extension that is used as the NCA-TSC endpoint when the extension is for a terminating NCA-TSC. For an unsuccessful NCA-TSC outgoing call, this field is blank.

  The field can contain a pound sign (#) or the letter E for either ARS calls or TAC calls when:

  – A user dials a pound sign (#) at the end of a string of digits

  – An outgoing call exceeds the interdigit-timeout interval that is in the ARS Analysis table

  – A user dials a TAC for a Look Ahead Interflow (LAI). For example, a successful LAI to <TAC> 1001, where 1001 is the remote VDN extension, yields 1001E or 1001# in the Dialed Number field. The vector processing software uses the pound sign (#) or E to indicate the end of the string of digits that the user dials.

    You administer the CDR System Parameter screen so the pound sign (#) or the letter E need not be the last digit of the CDR record.

- Duration

  Custom field name: **duration** or **sec-dur**

  Length: 4 digits

  This field contains the duration of the call, which the system records in hours (0 to 9), minutes (00 to 59), and tenths of minutes (0 to 9). The system rounds the duration of the call down in 6-second increments. For example, the system records the duration of a 5-second call as a duration of zero. If this field contains the value 9999, the call was in progress when a time change was made in the switch.

  You can use the customized record format to report the duration of the call in hours, minutes, and seconds.

- Feature Flag

  Custom field name: **feat-flag**

  Length: 1 digit

  The feature flag indicates whether a call received network answer supervision, and whether the call was interworked in the network. The duration of the call starts when the system receives the network answer.

  You can administer the **Feature flag** field on the CDR System Parameters screen to reflect whether the network reported an outgoing ISDN call as interworked.

  - The number 0 in this field indicates either a voice call without network answer supervision or a call for which NCA-TSC is not established.
  - The number 1 in this field indicates a data call without network answer supervision.
  - The number 2 in this field indicates a voice call with network answer supervision, but interworked.
  - The number 3 in this field indicates a data call with network answer supervision, but interworked.
  - The number 4 in this field indicates a voice call with network answer supervision.
  - The number 5 in this field indicates a data call with network answer supervision.

  The time of the answer and the duration of the call are accurate if the feature flag indicates that the call received network answer supervision.

  The time of the answer and the duration of the call might not be accurate, if the call does not receive network answer supervision, or the call receives answer supervision but is interworked with non-ISDN trunks.

  Calls are considered data calls if the calls use a conversion resource, such as a modem, and the calls either originate or terminate on a data module.

- Format Code

  Length: 2 digits

  This field contains two values:

- 00 indicates no PPM.
- 03 indicates a PPM count in the digits record.

- FRL

  Length: 1 digit

  Facilities restriction levels (FRLs) are numbered 0 through 7, are associated with the AAR and the ARS features, and define calling privileges. If the call is an:

  - Outgoing call, and an authorization code is not used to make the call, this field contains the FRL of the originating user FRL.
  - Outgoing call, and an authorization code is used to make the call, this field contains the FRL that is associated with the authorization code that the user dials.
  - Incoming or a tandem call, this field contains the FRL that is assigned to the incoming trunk group.
  - Incoming tandem tie trunk call, this field contains either the FRL that is assigned to the tandem tie trunk or the TCM sent with the tandem tie trunk call. If an FRL was used to complete the call, the field contains the FRL. If a TCM was used to complete the call, the field contains the TCM. With ISDN calls, this field always contains the TCM, if the TCM was received.

  You can administer CDR so that this field contains disconnect information instead of the FRL. If you administer CDR so this field contains disconnect information for trunk CDR, the system records the information shown in Table 63: Disconnect information for trunk CDR on page 555.

Table 63: Disconnect information for trunk CDR

Data	Meaning
0	The system cannot determine which participant on the call dropped the call first.
1	The switch participant dropped the call first.
2	CO participant dropped the call first.
3	Maintenance seized the trunk

For intraswitch CDR, the field contains the information that is shown in Table 64: Intra-switch CDR call disconnect information on page 556 instead of the FRL.

Table 64: Intra-switch CDR call disconnect information

Data	Meaning
0	The system cannot determine which participant on the call dropped the call first.
1	The calling participant dropped the call first.
2	The dialed participant dropped the call first.

- Incoming Circuit Identification

  Custom field name: **in-crt-id**

  Length: 3 digits

  This field contains the member number of a trunk within a trunk group that is used for an incoming call. For outgoing calls, this field is blank. Tandem calls contain both incoming and outgoing circuit ID numbers.

  The format of this field varies from record to record. For printer, TELESEER, and 59-character formats, the numbers are inverted on the record. For example, the circuit ID 123 appears as 231 (tens, units, hundreds). If you want to change the order to hundreds, tens, units format, for example, 123, use the **Modified Circuit ID Display** field on the CDR System Parameters screen.

- Incoming TAC

  Custom field name: **in-trk-code**

  Length: 4 digits

  This field contains the access code of the incoming trunk group.

- INS

  Length: 3 digits

  This field specifies the ISDN Network Service (INS) that is requested for a call. This field applies only to ISDN calls. Each network specific facility has a corresponding INS value, shown in Table 65: Network-specific facility to INS mapping on page 557.

  This field also appears as ISDN NSV (network service value).

Table 65: Network-specific facility to INS mapping

Network specific facility	INS value
OUTWATS Band 0 OUTWATS Band 1-255	33 34-288
Network Operator	324
Pre subscribed Common Carrier Operator	325
Software Defined Network (SDN)	352
MEGACOM 800	353
MEGACOM	354
INWATS	355
Maximum Banded WATS	356
ACCUNET Digital Service	357
AT&T Long Distance Service	358
International 800	359
Multiquest	367

- ISDN CC

  The call charge that the ISDN advice of charge function supplies.
- ISDN NSV

  See INS.

- IXC Code

  The length for non-ISDN formats: 1 digit hexadecimal

  Interexchange Carrier (IXC) codes,1-F hexadecimal, indicate the carrier used on the call. This information is sent to the CDR output device in ASCII code as a hexadecimal representation, for example, ASCII F equals 15 that is.

  Users must dial an IXC access number to access a specific common carrier for a call. In the US, this number is in the form 10XXX, 950 - 1XXX, or any 8 to 11 digit number. The IXC access numbers that are applicable at a given location are associated with an IXC code on the Inter-Exchange Carrier Codes screen.

  When ARS is used, and a route pattern inserts one of the administered IXC codes, the report contains the associated IXC code. If no IXC access number is used, or the carrier is selected at the central office (CO), the report contains a zero.

  Length for ISDN formats: 3 or 4 digits

  With an ISDN record format, this 3-digit or 4-digit field identifies the actual IXC used on an ISDN call. This information is determined from the route pattern administration. For AAR and ARS calls, the 3-digit IXC value is administered in the route pattern for all ISDN calls. If a user dials an IXC code with a 10XXX format as administered on the Inter-Exchange Carrier Codes screen, the CDR record contains only the last 3 digits (4 digits or Enhanced). If a user dials a 7-digit IXC code, this field contains a zero.

- Line Feed

  Length: 1 character

  The ASCII line feed character comes after a carriage return to terminate CDR records.

- Location From

  Custom field name: **location-from**

  Number of digits: 3

  The **location-from** field is a location number, used with the Multinational Locations feature, for record sorting. The field length is 3, the same as the length of the **location** field on the cabinet, media gateway, remote office, and ip-network region screens. The **location-from** field indicates the location code of the PBX interface of the calling party.

- Location To

  Custom field name: **location-to**

  Number of digits: 3

  The **location-to** field is a location number, used with the Multinational Locations feature, for record sorting. The field length is 3, the same as the length of the **location** field on the cabinet, media gateway, remote office, and ip-network region screens. The **location-to** field indicates the location code of the PBX interface of the called party.

Note:
If the Multinational Locations feature is turned off in the license file, the key words **location-from** and **location-to** are invalid.

- MA-UUI

  Length: 1 digit

  Message Associated User-to-User Signaling shows the number of ISDN messages that contain user data that are sent on an outgoing call. This field contains a number from 0 to 9.

- Node Number

  Custom field name: **node-num**

  Length: 2 digits

  This field identifies the DCS node number of a switch within a DCS arrangement. This number is the local ID, which is the same as the node number on the Dial Plan screen.

- Null

  Length: 1 character

  The Null character, usually in triplets, is used to terminate and divide CDR Records, when a receiving adjunct needs a record divider or terminator.

- Outgoing Circuit Identification

  Custom field name: **out-crt-id**

  Length: 3 digits

  For outgoing calls, this field contains the member number of the trunk within a trunk group that is used on the call. This field is blank for incoming calls. Tandem calls include both incoming and outgoing circuit ID numbers. For outgoing and tandem NCA-TSCs, this field contains the signaling group that is used to carry the NCA-TSC.

  The format of this field varies from record to record. For printer, TELESEER and 59-character formats, and the ISDN and Enhanced forms of those records, the numbers are inverted on the record. For example, the circuit ID 123 appears as 231 (tens, units, hundreds). If you want to change the order to hundreds, tens, units format, for example, 123, use the **Modified Circuit ID Display** field on the CDR System Parameters screen.

- Packet Count

  Custom field name: **tsc_ct**

  Length: 4 digits

  For ISDN TSCs, this field contains the number of ISDN-PRI USER INFO messages that are sent, received, or, for tandem TSCs, passed through the switch.

- PPM

  Periodic Pulse Metering (PPM) contains the pulse counts that are transmitted over the trunk line from the serving CO. The pulse counts are used to determine call charges.

- Resource Flag

  Custom field name: **res-flag**

  Length: 1 digit

  This field indicates whether a conversion resource was used, or if the call involved a Multimedia Application Server Interface (MASI) terminal or MASI trunk, or if a video or wideband codec was used.

  - 0 indicates no conversion device used, no video or wideband codec and no MASI devices
  - 1 indicates wideband audio codec used
  - 2 indicates conversion device used
  - 4 indicates video codec used
  - 5 indicates video codec and wideband audio codec used
  - 8 indicates a MASI call
  - **A** indicates a MASI call with a conversion device used

  Note:
  Video or wideband takes precedence over MASI/conversion. If video or wideband is used, the field does not indicate if MASI or a conversion device was used.

- Sec-dur

  For customized records only, you can uses this field to set the duration field to record seconds instead of tenths of minutes.

- Space

  Length: 0 to 40 characters

  The ASCII space character separates other CDR fields or fills unused record locations.

- TSC-Count

  Custom field name: **tsc_ct**

  This field is the customized name for Packet Count. See Packet Count for more information.

- TSC Flag

  Custom field name: **tsc_flag**

  Length: 1 digit

  This field describes call records that pertain to temporary signaling connections. When the value of this field is not equal to zero, this field indicates the status of the TSC. Table 66: Encoding for the TSC flag on page 561 shows the TSC flag encoding.

Table 66: Encoding for the TSC flag

Code	Description
0	Circuit-switched call without TSC requests
1-3	Reserved
4	Call Associated TSC requested and accepted in response to SETUP, no congestion control (applicable to originating node). Call Associated TSC received and accepted by SETUP, no congestion control (applicable to terminating node).
5	Call Associated TSC received and accepted by SETUP, congestion control (applicable to terminating node).
6	Call Associated TSC requested, accepted after SETUP, no congestion control (applicable to originating node). Call Associated TSC received and accepted after SETUP, no congestion control (applicable to terminating node).
7	Call Associated TSC received and accepted after SETUP, congestion control (applicable to terminating node).
8	Call Associated TSC requested, rejected (rejection came from outside the local switch).
9	Call Associated TSC requested, rejected (rejection came from the local switch, that is, lack of resource).
A	Non-call-associated (NCA) TSC received, accepted, no congestion control (applicable to terminating node). NCA TSC received, accepted, no congestion control (applicable to terminating node).
B	NCA TSC requested, accepted, congestion control (applicable to originating node). NCA TSC received, accepted, congestion control (applicable to terminating node).
C	NCA TSC requested, rejected (rejection came from outside the local switch).
D	Non Call Associated TSC requested, rejected (rejection came from the local switch, that is, lack of resource).
	1 of 2

Table 66: Encoding for the TSC flag (continued)

Code	Description
E	Reserved for future use.
F	Reserved for future use.
	2 of 2

- Time

  This fields contains the time that the call ended, or if Call Splitting is active, the time that a user dropped from a multiparty call.

- Timezone From

  Custom field name: **timezone-from**

  Number of digits: 5

  The **timezone-from** field is a time zone offset number, used with the Multinational Locations feature, for call time. The field length is 5, the same as the length of the **timezone offset** field on the cabinet, media gateway, remote office, and ip-network region screens. The **timezone-from** field indicates the timezone offset of the PBX interface of the calling party.

- Timezone To

  Custom field name: **timezone-to**

  Number of digits: 5

  The **timezone-to** field is a time zone offset number, used with the Multinational Locations feature, for call time. The field length is 5, the same as the length of the **location** field on the Locations screen. The **timezone-to** field indicates the timezone offset of the PBX interface of the called party.

Note:
If the Multinational Locations feature is turned off in the license file, the key words **timezone-from** and **timezone-to** are invalid.

- VDN

  Custom field name: **vdn**

  Length: 13 digits

  This field is available on customized records only. The call record contains the VDN extension number. If VDN Return Destination is active, this field contains the first VDN that the caller accessed.

Administering Call Detail Recording

The following steps are part of the administration process for the Call Detail Recording feature:

- Assigning Forced Entry of Account Codes
- Assigning privacy digits for a user
- Administering the CDR system parameters
- Administering CDR for a trunk group
- Administering CDR for a data module
- Identifying the Inter Exchange Carrier
- Administering CDR for the paging ports
- Administering the Intra-Switch CDR
- Administering Survivable CDR

This section describes:

- Any prerequisites for administering the Call Detail Recording feature
- Complete administration procedures for the Call Detail Recording feature

Prerequisites for administering Call Detail Recording

You must complete the following actions before you can administer the Call Detail Recording (CDR) feature:

To ensure that the CDR account code is available on you system:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen (Figure 107: Feature Access Code (FAC) screen on page 564).

Figure 107: Feature Access Code (FAC) screen

```
                      FEATURE ACCESS CODE (FAC)

         Abbreviated Dialing List1 Access Code: *00
         Abbreviated Dialing List2 Access Code: *01
         Abbreviated Dialing List3 Access Code: *02
Abbreviated Dial - Prgm Group List Access Code: *03
                      Announcement Access Code: *04
                       Answer Back Access Code: *05

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: *9    Access Code 2: 9
                Automatic Callback Activation: *06    Deactivation: #06
Call Forwarding Activation Busy/DA: *07    All: *08    Deactivation: #09
                         Call Park Access Code: *10
                       Call Pickup Access Code: *11
CAS Remote Hold/Answer Hold-Unhold Access Code: *50
                  CDR Account Code Access Code: *12
                        Change COR Access Code:
                   Change Coverage Access Code: *13
                   Contact Closure   Open Code:          Close Code:
                   Contact Closure  Pulse Code:
```

2. In the **CDR Account Code Access Code** field, type the code that you want a user to enter before the user enters a CDR account code number.

   For more information, see the "Feature Access Code" feature.

3. Press **Enter** to save your changes.

To ensure that call classification is enabled for your system:

1. View the Optional Features screen, and ensure that the **Answer Supervision by Call Classifier** field is set to **y**. If the **Answer Supervision by Call Classifier** field is set to **n**, your system is not enabled for call classification. Contact your Avaya representative if you want to use call classification.

   To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Assigning Forced Entry of Account Codes

Prerequisites

You must complete the following actions before you can assign FEAC for all calls:

1. View the Optional Features screen, and ensure that the **Forced Entry of Account Codes** field is set to **y**. If the **Forced Entry of Account Codes** field is set to **n**, your system is not enabled for FEAC for all calls. Contact your Avaya representative if you want to use FEAC for all calls.

   To view the Optional Features screen, type **`display System-Parameters Customer-Options`**. Press **Enter**.

Assigning FEAC for all calls

To assign FEAC for all calls:

1. Type **`change system-parameters cdr`**. Press **Enter**.

   The system displays the CDR System Parameters screen (Figure 108: CDR System Parameters on page 565).

Figure 108: CDR System Parameters

```
change system-parameters cdr                                    Page   1 of 2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 18                    CDR Date Format: month/day
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
Modified Circuit ID Display? n                  Remove # From Called Number? y
                 Record Outgoing Calls Only? n            Intra-switch CDR? y
  Suppress CDR for Ineffective Call Attempts? y     Outg Trk Call Splitting? y
      Disconnect Information in Place of FRL? n       Outg Attd Call Record? y
                                                   Interworking Feat-flag? y
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                   Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y              Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
      Record Call-Assoc TSC? n  Digits to Record for Outgoing Calls: outpulsed
   Privacy - Digits to Hide: 0              CDR Account Code Length: 4
```

2. In the **Force Entry of Acct Code for Calls Marked on Toll Analysis Form?** field, perform one of the following actions:
   - If you want the system to require that a user enter an account code for all calls, type **y**.
   - If you do not want the system to require that a user enter an account code for all calls, type **n**.

Note:
The information in the **Force Entry of Acct Code for Calls Marked on Toll Analysis Form?** field does not override other call restrictions that the user might have.

Assigning FEAC to a COR

To assign FEAC to a COR:

1. Type **change cor *n***, where ***n*** is the number of the COR to which you want to assign FEAC. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 109: Class of Restriction screen on page 566).

Figure 109: Class of Restriction screen

```
change cor 1                                                Page   1 of 4
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 7                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? y
         Priority Queuing? n                Direct Agent Calling? y
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? y
         Send ANI for MFE? n             Add/Remove Agent Skills? y
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? y
                        Can Be Picked Up By Directed Call Pickup? n
                                     Can Use Directed Call Pickup? n
                                     Group Controlled Restriction: inactive
```

2. In the **Forced Entry of Account Codes** field, perform one of the following actions:

- If you want all users to enter an account code for calls that require an account code, type **y**.
- If you do not want all users to enter an account code for calls that require an account code, type **n**.

3. Press **Enter** to save your changes.

Assigning FEAC to a user

To assign FEAC to a user:

1. Type **change station *n***, where ***n*** is the number of the user extension to which you want to assign FEAC. Press **Enter**.

   The system displays the Station screen (Figure 110: Station screen on page 567).

Figure 110: Station screen

```
change station 1014                                          Page 1 of X
                              STATION

Extension: 1014               Lock Messages? n                    BCC: 0
     Type:                    Security Code:                       TN: 1
     Port:                  Coverage Path 1:                      COR: 1
     Name:                  Coverage Path 2:                      COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                          Message Lamp Ext: 1014
          Speakerphone: 2-way                   Mute button enabled? y
       Display Language? English                   Expansion Module?
                   Model:

 Survivable GK Node Name:                          Media Complex Ext:
                                                        IP Softphone? y
                                                 Remote Office Phone? y
```

2. In the **COR** field, type the number of the COR that requires the user to enter an account code.
3. Press **Enter** to save your changes.
4. Type **change trunk-group *n***, where ***n*** is the number of the trunk group to which you want to assign FEAC. Press **Enter**.

   The system displays the Trunk Group screen.

5. In the **COR** field, type the number of the COR that requires a user to enter an account code for calls that use this trunk group.

6. Press **Enter** to save your changes.

Assigning privacy digits for a user

Prerequisites

You must complete the following actions before you can assign privacy digits for a user:

Assign the system-wide privacy digits

1. Type **`change system-parameters cdr`**. Press **Enter**.

   The system displays the CDR System Parameters screen (Figure 111: CDR System Parameters screen on page 568).

Figure 111: CDR System Parameters screen

```
change system-parameters cdr                                    Page   1 of 2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 18                     CDR Date Format: month/day
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
Modified Circuit ID Display? n                  Remove # From Called Number? y
                  Record Outgoing Calls Only? n            Intra-switch CDR? y
  Suppress CDR for Ineffective Call Attempts? y     Outg Trk Call Splitting? y
     Disconnect Information in Place of FRL? n       Outg Attd Call Record? y
                                                    Interworking Feat-flag? y
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                  Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
      Record Call-Assoc TSC? n  Digits to Record for Outgoing Calls: outpulsed
   Privacy - Digits to Hide: 0             CDR Account Code Length: 4
```

2. In the **Privacy - Digits to Hide** field, type the number of user-dialed digits that the system replaces with blanks when the system generates a CDR record of the call.
3. Press **Enter** to save your changes.

Assigning CDR privacy to a user:

1. Type **change station *n***, where ***n*** is the number of the user extension to which you want to assign CDR privacy. Press **Enter**.

   The system displays the Station screen (Figure 112: Station screen on page 569).

Figure 112: Station screen

```
change station 75001                                          Page 2 of X
                                    STATION

FEATURE OPTIONS
           LWC Reception? spe                Auto Select Any Idle Appearance? n
          LWC Activation? y                          Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
            CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n            Per Station CPN - Send Calling Number? _
       Service Link Mode: as-needed
         Multimedia Mode: basic
    MWI Served User Type: ______                 Display Client Redirection? n
         Automatic Moves:
               AUDIX Name:                     Select Last Used Appearance? n
                                                 Coverage After Forwarding? _
     Recall Rotary Digit? n                        Multimedia Early Answer? n

Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001                          IP Audio Hairpinning? n
```

2. Click **Next** until you see the **CDR Privacy?** field.
3. In the **CDR Privacy?** field, perform one of the following actions:
   - If you want the system to replace some of the digits that the user dials, when the system generates a CDR record of the call, type **y**.
   - If you do not want the system to replace some of the digits that the user dials, when the system generates a CDR record of the call, type **n**.
4. Press **Enter** to save your changes.

Administering the CDR system parameters

To administer the CDR system parameters for your system:

1. Type **change system-parameters cdr**. Press **Enter**.

   The system displays the CDR System Parameters screen (Figure 113: CDR System Parameters screen on page 570).

Figure 113: CDR System Parameters screen

```
change system-parameters cdr                                    Page   1 of 2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 18                      CDR Date Format: month/day
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
Modified Circuit ID Display? n                  Remove # From Called Number? y
                  Record Outgoing Calls Only? n            Intra-switch CDR? y
  Suppress CDR for Ineffective Call Attempts? y     Outg Trk Call Splitting? y
      Disconnect Information in Place of FRL? n       Outg Attd Call Record? y
                                                   Interworking Feat-flag? y
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? y
                                   Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                 Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n  Digits to Record for Outgoing Calls: outpulsed
   Privacy - Digits to Hide: 0              CDR Account Code Length: 4
```

2. In the **Inc Trk Call Splitting?** field, perform one of the following actions:
   - If you want an incoming trunk call, that is conferenced or transferred to a local extension that is optioned for Intraswitch CDR, to produce an incoming trunk call record, type **y**.

     If you set the **Inc Trk Call Splitting?** field to **y**, you must set the **Record Outgoing Calls Only** field to **n**.
   - If you do not want an incoming trunk call, that is conferenced or transferred to a local extension that is optioned for Intraswitch CDR, to produce an incoming trunk call record, type **n**.
3. In the **Record Outgoing Calls Only** field, perform one of the following actions:
   - If you only want the system to record outgoing calls, type **y**.
   - If you want the system to record both incoming and outgoing calls, type **n**.

4. In the **Call Record Handling Option** field, perform one of the following actions:
   - Type **reorder** if you want the system block calls generate reorder tone when the buffer is full. If you choose this option, no one can make or receive calls if the system cannot generate CDR records for the calls.
   - Type **warning** if you want the system stop recording call when the buffer is full. If the buffer is full, and you choose this option, the system generates a minor alarm.

     Warning is the system default for this field. Note that if you change the default, the system might redirect the ACD calls and the vector calls the system records for CDR.
   - Type **attendant** if you want the system to route all the calls to the attendant as non-CDR calls.

     Note that if you change the system default of **warning,** ACD calls and vector calls that are measured by CDR might be redirected. Also note that the system displays the **Call Record Handling Option** field only for DEFINITY R. The system uses the information in this field to control call routing when:
     - New calls come in.
     - The CDR link is not operating.
     - The buffer is full.
5. In the **Calls to Hunt Group-Record** field, perform one of the following actions:
   - If you want the system to record the extension of the telephone or data terminal where the call terminates, type **member-ext**.
   - If you want the system to record the extension that the user dials, type **group-ext**.
6. In the **CDR Account Code Length** field, type the number of digits that you want the system to record when a user enters an account code. For some record formats, the system overwrites the information in other fields if the account code is too long.
7. In the **CDR Date Format** field, perform one of the following actions:
   - If you want to use the month and day date format for the date stamp that starts each new day of call records, type **month/day**.
   - If you want to use the day and month date format for the date stamp that starts each new day of call records, type **day/month**.
8. In the **Condition Code 'T' for Redirected Calls** field, perform one of the following actions:
   - If you want the system to record condition code *T* for both CDR records of the call that the system automatically redirects off the server that runs Communication Manager, type **y**.
   - If you want the system to record the condition codes that are usually associated with the **Record Outdoing Call Only** field for calls that the system automatically redirects off the server that runs Communication Manager, type **n**.
9. In the **Digits to Record for Outgoing Calls** field, perform one of the following actions:
   - To record the digits that a user dials, type **dialed**.

- To record the digits that the software actually sends out over the trunk, type **outpulsed**. This information includes any additions or deletions that take place during routing.

10. In the **Disconnect Information in Place of FRL** field, perform one of the following actions:
    - If you want the system to replace the **Facility Restriction Level (FRL)** field with the call disconnect information, type **y**. You can use the call disconnect information to isolate problems between the DEFINITY R and the telephone network.
    - If you want the system to record the facilities restriction level (FRL) of the call, type **n**.
11. In the **EIA Device Bit Rate** field, type the baud of the CDR device that is connected to the Electronic Industries Association (EIA) port. The valid bauds for this field are:
    - 300
    - 1200
    - 2400
    - 4800
    - 9600

    Note that the system displays this field only if either the **Primary Output Format** field or the **Secondary Output Format** field is set to **eia,** and then only for a DEFINITY SI.
12. In the **Inc Attd Call Record** field, perform one of the following actions:
    - If you want the system to generate separate records of the attendant portions of incoming calls that the attendant transfers or conferences, type **y**.
    - If you do not want the system to generate separate records of the attendant portions of incoming calls that the attendant transfers or conferences, type **n**.

      Note that the system displays this field only when the **Inc Trk Call Splitting** field is set to **y**.
13. In the **Inc Trk Call Splitting** field, perform one of the following actions:
    - If you want the system to create separate records for each portion of an incoming call that is transferred or conferenced, type **y**.
    - If you do not want the system to create separate records for each portion of an incoming call that is transferred or conferenced, type **n**.

      Note that the system only displays this field when the **Record Outgoing Calls Only** field on the System Parameters CDR screen is set to **n**.
14. In the **Interworking Feat-flag** field, perform one of the following actions:
    - If you want the system to record, in the **Feature Flag** field of a CDR record, that a call is an interworked outgoing ISDN call, type **y**.

      An interworked call is a call that passes through more than one ISDN node.

- If you want the system to record, in the **Feature Flag** field of a CDR record, that there is no answer supervision for interworked calls, type **n**.

15. In the **Intra-Switch CDR** field, perform one of the following actions:
    - If you want the system to record calls within the server. If you type **y**, you must administer the Intraswitch CDR screen to specify the extensions that you want the system to monitor, type **y**.
    - If you do not want the system to record calls within the server, type **n**.
16. In the **Modified Circuit ID Display** field, perform one of the following actions:
    - If you want the system to display the circuit ID in the actual format of 100's, 10's units, for example, if you want the system to display circuit ID 123 as 123, type **y**. Verify that the output device of your system can accept this format.
    - To display the circuit ID in its default format (10's, units, 100's). For example, the system displays circuit ID 123 appears as 231, type **n**.

      The information in the **Modified Circuit ID Display** field pertains to the following CDR output formats:

      — Printer

      — TELESEER

      — 59-character

The **Node Number (Local PBX ID)** field is a display-only field that is set to the distributed communications system (DCS) switch node number in a network of switches.

17. In the **Outg Attd Call Record** field, perform one of the following actions:
    - If you want the system to generate separate records of the attendant portions of outgoing calls that the attendant transfers or conferences, type **y**.
    - If you do not want the system to generate separate records of the attendant portions of outgoing calls that the attendant transfers or conferences, type **n**.

      Note that the system displays this field only when the **Outg Trk Call Splitting** field is set to **y**.
18. In the **Outg Trk Call Splitting** field, perform one of the following actions:
    - If you want the system to create separate records for each portion of an outgoing call that is transferred or conferenced, type **y**.
    - If you do not want the system to create separate records for each portion of an outgoing call that is transferred or conferenced, type **n**.
19. In the **Primary Output Endpoint** field, perform one of the following actions:
    - If the system uses the EIA port to connect the CDR device, type **eia**. This option is not valid for DEFINITY R systems.
    - Type the extension of the data module that links the primary output device to the server.

- If the CDR device connects over a TCP/IP link, and the TCP/IP link is defined as CDR1 on the IP Services screen, type **CDR1**.
- If the CDR device connects over a TCP/IP link, and the TCP/IP link is defined as CDR2 on the IP Services screen, type **CDR2**.

20. In the **Primary Output Format** field, perform one of the following actions:
    - Type **customized** if you do not want to use the standard CDR record formats. If you use a customized record format, your system must have call accounting software that is also customized to receive the customized records. Talk with your call accounting vendor before you select this option.
    - Type **printer** if you want the system to send the CDR record formats to a printer instead of to a record collection system or to a call accounting system.
    - Type the standard record format that you want to use on your system. The valid standard record formats are:
      - 59-char
      - expanded
      - lsu
      - lsu-expand
      - int-direct
      - int-isdn
      - int-process
      - TELESEER
      - unformatted

      The standard record format that you choose must be compatible with the call accounting software on your system. To ensure that the standard record format that you choose is compatible with your call accounting system, talk with your vendor or see the call accounting system documentation.
21. In the **Privacy - Digits to Hide** field, type the number of dialed number digits that you want the system to hide for an extension with the **CDR Privacy** field on the Station record that is set to **y**. The valid entries for the **Privacy - Digits to Hide** field are **0** through **7**.

    The system hides the dialed digits from right to left. If you type **4** in the **Privacy - Digits to Hide** field, and the user dials 5551234, the system records the dialed number as 555.
22. In the **Record Agent ID on Incoming** field, perform one of the following actions:
    - If you want the system to record the login ID of the EAS agent in the **Dialed Number** field of the CDR record, type **y**.

- if you want the system to record the physical extension in the **Dialed Number** field of the CDR record, type **n**.

  The system displays the **Record Agent ID on Incoming field o**nly if the **Expert Agent Selection (EAS)** field on the Optional Features screen is set to **y**.

  You cannot use both the **Called VDN** field and the **Agent Login ID Instead of Group or Member** field. Only one of these fields can be set to **y**.

23. In the **Record Agent ID on Outgoing** field, perform one of the following actions:

    - If you want the system to record the login ID of the EAS agent in the **Dialed Number** field of the CDR record, type **y**.
    - If you want the system to record the physical extension in the **Dialed Number** field of the CDR record, type **n**.

    The system displays the **Record Agent ID on Outgoing** field only if the **Expert Agent Selection (EAS)** field on the Optional Features screen is set to **y**.

24. In the **Record Call-Assoc TSC** field, perform one of the following actions:

    - If you want the system to generate records for call-associated temporary signaling connections, type **y**.

      Consider the capacity of your call collection device before you decide to generate records for call-associated noncall-associated/temporary-signaling connection (TSCs).

    - If you do not want the system to generate records for call-associated TSCs, type **n**.

25. In the **Record Called Vector Directory Number Instead of Group or Member** field, perform one of the following actions:

    - If you want the system to record the Vector Directory Number (VDN) in the **Dialed Number** field of the CDR record for calls that the system routes to a hunt group because of a vector, type **y**. If the system routes a call through more that one VDN, the system records the first VDN in the **Dialed Number** field of the CDR record
    - If you want the system to record the group number or the member number in the **Dialed Number** field of the CDR record for calls that the system routes to a hunt group because of a vector, type **n**.

      You cannot use both the **Called VDN** field and the **Agent Login ID Instead of Group or Member** field. Only one of these fields can be set to **y.**

26. In the **Record Non-Call-Assoc TSC** field, perform one of the following actions:

    - If you want the system to create records for noncall-associated temporary signaling connections, type **y**.

      Consider the capacity of your call collection device before you decide to generate records for call-associated TSCs.

- If you do not want the system to generate records for noncall-associated TSCs, type **n**.

  A TSC is a virtual connection that is established within an ISDN D-channel. For more information, see the DEFINITY® Communications System Generic 2.2 and Generic 3 V2 DS1/CEPT1/ISDN PRI Reference.

27. In the **Record Outgoing Calls Only** field, perform one of the following actions:
    - If you want the system to record only outgoing calls type **y**.
    - If you want the system to record incoming and outgoing calls, type **n**.
28. In the **Remove # From Called Number** field, perform one of the following actions:
    - If you want the system remove the pound sign (#) or the letter E from the **Dialed Number** field of the call detail record, type **y**.

      Verify that your output device can accept this format.
    - If you want the system to record the trailing pound sign (#) or the letter E in the **Dialed Number** field whenever interdigit time out occurs or users dial the pound sign # to indicate the end of a dialed string, type **n**.
29. In the **Secondary Output Endpoint** field, perform one of the following actions:
    - If the system uses the EIA port to connect the CDR device, type **eia**. This option is not valid for DEFINITY R systems.
    - Type the extension of the data module that links the primary output device to the server.
    - If the CDR device connects over a TCP/IP link, and the TCP/IP link is defined as CDR1 on the IP Services screen, type **CDR1**.

    The system displays the **Secondary Output Endpoint** field when the you administer the **Secondary Output Format** field.
30. In the **Secondary Output Format** field, type the formats that you want your system to use for a secondary output device. The valid formats for a secondary out device are:
    - customized
    - int-direct
    - int-process
    - lsu
    - unformatted

    CAUTION:
    Ensure that only qualified service personnel administer a secondary output device. This option can cause loss of data when the buffer contains large amounts of data.
31. In the **Suppress CDR for Ineffective Call Attempts** field, perform one of the following actions:

- if you want the system to ignore ineffective call attempts, type **y**. Perform this action if you have limited storage space for CDR records and the CDR records often overrun the buffer.
- If you want the system to record ineffective call attempts, type **n**.

  Ineffective call attempt information shows you how often your users cannot place outgoing calls, or if numerous incoming calls are not completed. You can also use the information to document attempts to contact a client when you use ISDN trunks.

Your system requires more space for records if the system records ineffective call attempts than if the system does not record ineffective call attempts. Ineffective call attempts are calls that the system blocks because:

- The user does not have sufficient calling privileges.
- All the outgoing trunks are busy.
- Incoming or outgoing trunks are unavailable because of trunk usage allocation for ISDN Call-by-Call Service Selection trunks.
- Incoming calls have an network-specific facility (NSF) mismatch.
- A cause value is provided for ISDN calls that are not complete at the far end.

The system record the ineffective call attempt as condition code E.

Note:
Even when the **Suppress CDR for Ineffective Call Attempts** field is set to **y**, it is possible to generate a CDR record for an outgoing trunk call if the **Answer Supervision Timeout** field on the Trunk Group screen for the outgoing trunk is administered to a small number (something generally less than 5 or 6). This is because when the Answer Supervision by Timeout feature is active and the timer expires, the server treats that call as an effective call, and therefore creates a CDR record regardless of the state of the **Suppress CDR for Ineffective Call Attempts** field.

32. In the **Use Enhanced Formats** field, perform one of the following actions:
    - If you want to use the enhanced version of the specified primary output format in you system, type **y**. You cannot use enhanced formats and ISDN formats at the same time.
    - If you do not want to use the enhanced version of the specified primary output format, type **n**.

    The enhanced formats provide additional information about the time a call is in a queue and about ISDN call charges. The **Use Enhanced Formats** field pertains to following output formats:
    - Expanded
    - TELESEER
    - Lsu
    - Printer

- Unformatted

33. In the Use **ISDN Layouts** field, perform one of the following actions:
    - To use the ISDN version of the specified primary output format, type **y**. You cannot use ISDN formats and enhanced formats at the same time.
    - If you do not want to use the ISDN version of the specified primary output format, type **y**.

    The ISDN formats provide more accurate information about the IXC and the ISDN network services that are used for a call. The **Use ISDN Layouts** field pertains to the following output formats:
    - Lsu
    - Printer
    - Any format with an ISDN layout, such as TELESEER
34. Click **Next** to see the second page of the CDR System Parameters screen (Figure 114: CDR System Parameters screen on page 578).

Note:
The system displays this second CDR System Parameters screen only if the **Primary Record Format** field is set to **customized**.

Figure 114: CDR System Parameters screen

```
change system-parameters cdr                                    Page   2 of 2
                          CDR SYSTEM PARAMETERS

     Data Item - Length          Data Item - Length          Data Item - Length
 1: date             - 6   17: clg-num/in-tac   - 10  33:                   -
 2: space            - 1   18: space            - 1   34:                   -
 3: time             - 4   19: bandwidth        - 2   35:                   -
 4: space            - 1   20: space            - 1   36:                   -
 5: sec-dur          - 5   21: in-crt-id        - 3   37:                   -
 6: space            - 1   22: space            - 1   38:                   -
 7: cond-code        - 1   23: out-crt-id       - 3   39:                   -
 8: space            - 1   24: space            - 1   40:                   -
 9: feat-flag        - 1   25: return           - 1   41:                   -
10: space            - 1   26: line-feed        - 1   42:                   -
11: code-dial        - 4   27:                  -     43:                   -
12: space            - 1   28:                  -     44:                   -
13: code-used        - 4   29:                  -     45:                   -
14: space            - 1   30:                  -     46:                   -
15: dialed-num       - 10  31:                  -     47:                   -
16: space            - 1   32:                  -     48:                   -

                             Record length = 67
```

35. In the **Data Item** field, type the data items in the order that you want the items to appear in the customized CDR record.

    You must include at least three fields on this CDR System Parameters screen if you want to have a customized CDR record. The first field can be any field that you choose from Table 67: Valid data item entries on page 579. The last two fields items in a record must be **line-feed** and **return**, in that order.

Table 67: Valid data item entries

Data item	Length	Data item	Length
acct-code	15	**ins**	3
attd-console	2	**isdn-cc**	11
auth-code	7	**ixc-code**	4
bandwidth	2	**ma-uui**	1
bcc	1	**node-num**	2
calling-num	15	**null**	1
clg-pty-cat	2	**out-crt-id**	3
clg-num/ in-tac	10	**ppm**	5
code-dial	4	**res-flag**	1
code-used	4	**return**	1
cond-code	1	**sec-dur**	5
date	6	**space**	1
dialed-num	23	**time**	4
duration	4	**tsc_ct**	4
feat-flag	1	**tsc_flag**	1
frl	1	**vdn**	1
in-crt-id	3		
in-trk-code	4		
line-feed	1		

36. In the **Length** field, type the maximum length of each data item, if the length of the data item differs from the default length.

    You must type **6** for the length of any date field to ensure proper output.

    In some cases, the system enforces a default field length.

    The **Record Length** field is a display-only field that contains the sum of all the numbers that you type in all the of the Length fields. If you change a Length field, the system automatically changes the number in the **Record Length** field.

37. Press **Enter** to save your changes.

Administering CDR for a trunk group

To administer CDR for a trunk group:

1. Type **`change trunk-group n`**, where ***n*** is the number of the trunk group for which you want to administer CDR. Press **Enter**.

   The system displays the Trunk Group screen.

2. Click **Next** until you see the **Answer Supervision Timeout** field.
3. In the **Answer Supervision Timeout** field, perform one of the following actions:

   - If the **Receive Answer Supervision** field is set to **n**, type the number of seconds that you want the system to wait, before the system acts as if answer supervision was received from the far end.

     The system uses the timing information for outgoing and two-way trunks. For a cut-through operation, the system starts tracking the time after the system sends each outgoing digit. The system stops tracking the time after the far end sends answer supervision. If the timer expires, the system acts as if answer supervision was received. With a senderized operation, the system starts tracking the time after the system sends the last collected digit.

   - If the **Receive Answer Supervision** field is set to **y**, type **0**.

   Note that the **Answer Supervision Timeout** field does not override answer supervision sent from the network or from **DS1** port circuit timers. To control answer supervision that is sent by **DS1** firmware, you must set the **Outgoing End of Dial (sec)** field on the Administrable Timers page of the Trunk Group screen.

4. In the **CDR Reports** field, perform one of the following actions:

   - If you want the system to generate records for all the outgoing calls on this trunk group, type **y**.

     If the **Record Outgoing Calls Only** field on the CDR System Parameters screen is **n**, incoming calls on this trunk group also generate call detail records.

   - If you do not want calls that use this trunk group to generate CDR records, type **n**.

- If you want the system to generate both incoming and outgoing CDR records, type **r** for a ring interval,. The system also generates the ring interval CDR records that Table 68: CDR ring interval records on page 581 shows.

Table 68: CDR ring interval records

Type	Description
Abandoned calls	The system creates a record with condition code H. Condition code H indicates the interval from the start of ringing until the call is abandoned.
Answered calls	The system creates a record with condition code G. Condition code G indicates the interval from the start of ringing until the call is answered.
Calls to busy stations	The system creates a record with condition code I. condition code I indicates a recorded interval of 0.

For ISDN trunk groups, the **Charge Advice** field affects the CDR information. For central office (CO), direct inward and outward dialing (DIOD), foreign exchange (FX), and wide are telecommunications service (WATS) trunk groups, the **Analog PPM** field affects the CDR information.

5. In the **Disconnect Supervision-In** field, perform one of the following actions:
   - Type **y** if you want:
     - Trunk-to-trunk transfers that involve this trunk group

       If you want trunk-to-trunk transfer in your system, you must also set the **Transfer** field on the Feature-Related System Parameters screen to **y**.
     - To make the far end server or switch responsible for releasing the trunk, when the far end server sends a release signal as the calling party releases an incoming call.
     - To enhance Network Call Redirection
   - Type **n** if:
     - You do not want trunk-to-trunk transfers that involve this trunk group.
     - The far end server does not provide a release signa.l
     - The hardware in your system cannot recognize a release signal.

– You prefer to use timers for disconnect supervision on incoming calls.

The system displays the **Disconnect Supervision-In** field if the **Direction** field is set to **incoming** or **two-way**.

If the **Direction** field is set to **outgoing**, the system sets the **Disconnect Supervision-In** field to **n**.

The value in the **Disconnect Supervision-In** field determines whether the system receives disconnect supervision for incoming calls over this trunk group.

CAUTION:
The system does not allow trunk-to-trunk transfers unless at least one party on the call can provide disconnect supervision. If you administer the **Disconnect Supervision-In** field incorrectly, you can cause trunks to become unusable until the problem is detected and the trunks are reset.

For example, if a user connects two trunks through the use of the Conference feature or the Transfer feature, and a far end Avaya S8*XXX* server on the resulting connection does not provide disconnect supervision, the trunks are not released. The trunks are not released because the system cannot detect the end of the call.

Usually, the COs in the United States provide disconnect supervision for incoming calls, but do not provide disconnect supervision for outgoing calls. Public networks in most other countries do not provide disconnect supervision for incoming calls or outgoing calls. Talk with your network services provider to determine if the public networks in your area provide disconnect supervision.

6. Press **Enter** to save your changes.

Administering CDR for a data module

To administer CDR for a data module:

1. Type **`change data-module n`**, where ***n*** is the number of the data module for which you want to administer CDR. Press **Enter**.

   The system displays the Data Module screen (Figure 115: Data Module screen on page 583 and Figure 116: Data Module screen on page 583).

Figure 115: Data Module screen

```
change data-module 30                                          Page 1 of 2
                                DATA MODULE

  Data Extension: 30            Name: 27                          BCC:
            Type: data-line___   COS: 1
            Port: _______        COR: 1
             ITC: restricted__    TN: 1                 Connected to: dte


ABBREVIATED DIALING
  List1:

SPECIAL DIALING OPTION:



ASSIGNED MEMBER (Station with a data extension button for this data module)

          Ext     Name
      1: 1002    27 character   station name
```

Figure 116: Data Module screen

```
change data-module 30                DATA MODULE                Page 2 of 2
        CAPABILITIES
                       KYBD Dialing? y                    Configuration? n
                           Busy Out? n
        SPEEDS
              Low? y           1200? y           4800? y          19200? y
              300? y           2400? y           9600? y     Autoadjust? n
        OPTIONS
                    Permit Mismatch? n                     Dial Echoing? y
                Disconnect Sequence: two-breaks             Answer Text? y
                             Parity: even          Connected Indication? y
```

The system displays the **Ext** and **Name** display-only fields in the **Abbreviated Dialing** area. The fields contain the extension number and the name of the users who have associated data extension buttons, and who share this data module.

2. In the **BCC** field, perform one of the following actions:
   - Type a **1** if the speed is 56 kbps.

- Type a **2**, **3,** or **4** if the speed is 64 kbps.

The system compares the speed setting that you assign here with the speed setting in an associated routing pattern. The system compares the two speed settings when calls that attempt to use the data module are not completed.

The system displays the **BCC** field appears if the **ISDN-PRI** field or the **ISDN-PRI Trunk**s field on the Optional Features screen is set to **y**.

3. The **Capabilities** area contains three fields.
   - In the **Configuration** field, perform one of the following actions:
     - If you want to view and change options from originating or receiving DTEs, such as non intelligent terminals, type **y**.
     - If you do not want view and change options from intelligent devices such as computers, type **n**.

     The system displays the **Configuration** field only when the **KYBD Dialing** field on the Data Module screen is set to **y**.
   - In the **KYBD Dialing** field, perform one of the following actions:
     - If you want the users to dial calls from a keyboard, and to allow the data module endpoint to transmit and receive text during call origination or call termination, type **y**.

       If you type **y**, you must also type **n** in the **Low** field in the **Speeds** area of the Data Module screen.
     - If you do not want the users to dial calls from a keyboard, type **n**.

       If you type **n**, the data module endpoint cannot transmit and receive text during call origination and call termination.

       If you type **n**, data calls can be answered, but text feedback is not provided.
   - In the **Busy Out** field, perform one of the following actions:
     - If you want the system to place the data line circuit (DLC) port in a busyout state so calls do not terminate at the data terminal equipment (DTE) when the DTE control lead to the DLC drops, type **y**. Use this option for DTEs that are members of a hunt group.
     - If you want the system to keep the DLC port out of a busyout state when the DTE control lead to the DLC drops, type **n**.

4. The **Circuit Switched Data Attributes** area contains information that is used with 7500 data modules and World Class BRI data modules.

   Note that the fields in the **Circuit Switched Data Attributes** area contain default information. The default information is for modem pooling conversion resource insertion when the endpoint does not support the data query capability or the administered connections. The information in the fields has no significance for data modules that provide data query, such as Avaya-supported ISDN-BRI data modules. Use the system default settings for Avaya ISDN-BRI data modules or World Class ISDN-BRI data modules.

   - In the **Default Duplex** field, perform one of the following actions:
     - Type **full** to allow simultaneous, two-way transmission.,which is duplex mode.
     - Type **half** to allow only one transmission direction at a time, which is half-duplex mode.
   - In the **Default Mode** field, perform one of the following actions:
     - Type **sync** for synchronous data mode.
     - Type **async** for asynchronous data mode.
   - In the **Default Speed** field, type the data rate. The valid entries are:
     - 1200
     - 2400
     - 4800
     - 9600
     - 19200
     - 56000 when the **Default Mode** field is set to **sync**
     - 64000 when the **Default Mode** field is set to **sync**
5. The system displays the **Connected To** field, when the **Type** field contains either **dpm** or **data-line**.

   In the **Connected To** field, perform one of the following actions:

   - If the Asynchronous Data Unit (ADU) is connected to a data terminal equipment (DTE), type **dte**.
   - If the ADU is connected to an information systems network, type **isn**.
6. In the **COR** field, type the number of the Class of Restriction (COR) for this data module. Valid entries are **0** through **95**.
7. In the **COS** field, type the number of the Class of Service (COS) for this data module. Valid entries are **1** through **15**.
8. The **Data Module Capabilities** area contains three fields with information for the 7500 data modules and the World Class BRI (WCBRI) data modules.

- The **Default Data Applications** field identifies the mode that the system uses to originate calls when the calling parameters do not specify the mode. The system also uses the mode to terminate trunk calls that do not have administered connections, or for which the bearer capability is unspecified. For more information, see the "Uniform Dial Plan" feature.

  In the **Default Data Applications** field, perform one of the following actions:

  — Type M0 to specify mode 0. Use this option for a WCBRI endpoint that the system uses as an administered connection.

  — Type **M1** to specify mode 1.

  — Type **M2_A** to specify mode 2 asynchronous.

  — Type **M2_S** to specify mode 2 synchronous.

  — Type **M3/2** to specify mode 3/2 adaptable.

- In the **Default ITC** field, perform one of the following actions:

  — Type **restricted** for a WCBRI endpoint that is an administered connection.

  — Type **unrestricted** for a WCBRI endpoint that is not an administered connection.

- The display-only **MM Complex Voice Ext** field contains the number of the associated telephone in the multimedia complex. The system displays the **MM Complex Voice Ext** field only when the **Multimedia** field is set to **y**.

  The field is blank until you type the data module extension in the **MM Complex Data Ext** field on the Station screen. When you type the data module extension in the **MM Complex Data Ext** field on the Station screen, the system associates the numbers in the **MM Complex Data Ext** and the **MM Complex Voice Ext** fields as two parts of a one-number complex. The one-number complex is the extension of the telephone.

The system displays the data module extension in the display-only **Data Extension** field.

9. In the **ITC** field, perform one of the following actions:

   - If the data module can send bits at speeds less than or equal to 56 kbps, type **restricted**. If you type **restricted** in the **ITC** field, the system uses a trunk group for which the **COMM Type** field on the Trunk Group screen is set to **rbavd** or **avd** to complete a call from this data module endpoint.

     A restricted transmission facility enforces ones density digital transmission. Ones density digital transmission is a sequence of eight digital zeroes that the firmware on the DS1 port board converts to a sequence of seven zeroes and a digital 1.

   - If the data module can send bits at a speed up to, and including, 64 kbps, type **unrestricted**. If you type **unrestricted** in the **ITC** field, the system uses a trunk group for which the **COMM Type** field on the Trunk Group screen is set to **avd** to complete a

call from this data module endpoint. The value **avd** in the **Comm Type** field indicates that the trunk group provides both restricted and unrestricted transmission facilities.

An unrestricted transmission facility does not enforce ones density digital transmission. The DS1 port board firmware does not convert the digital information.

The system does not display the **ITC** field for voice-only stations or BRI stations. The **ITC** field applies only when the **Comm Type** field on the Trunk Group screen, that the system uses for an outbound call, is set to **avd** or **rbavd**. The **ITC** field specifies the type of transmission facilities that an ISDN call uses when a call originates from this data module endpoint.

10. In the **List1** field in the **Abbreviated Dialing** area, perform one of the following actions:
    - Leave the field blank if you do not want the data module to have an abbreviated dialing list.
    - If you want the data module to have an enhanced abbreviated dialing list, type **e**.
    - if you want the data module to have a group list, type **g**.

      If you type **g**, the system displays a field to the right of the **List1** field. You must type a group list number in this field.
    - If you want the data module to have a personal list, type **p**.

      If you type a **p**, the system displays a field to the right of the **List1** field. You must type a personal list number in this field.
    - If you want the data module to have a system abbreviated dialing list, type **s**.
11. In the **Name** field, perform one of the following actions:
    - Type the name of the user who is associated with the data module.
    - Leave the field blank.
12. The **Options** area contains six fields.
    - In the **Answer Text** field, perform one of the following actions:
      - If you want the system to allow text feedback to the DTE when a user answers a call or the system disconnects a call, type **y**. The text feedback includes both DLC-generated text and system-generated text.
      - If you want the system to disable text feedback to the DTE when a user answers a call or the system disconnects a call, and when the DTE that answers a call is a computer or an intelligent device, type **n**. The system still generates the text, but the DLC does not allow the text to be delivered to the DTE.

      The **Answer Text** field applies to the following call messages:
      - Incoming
      - Answered
      - Disconnected

- Disconnected other end

The system displays the **Answer Text** field only if the **KBDY Dialing** field on the Data Module screen is set to **y**.

- In the **Connected Indication** field, perform one of the following actions:
  - If you want the system to generate a "connected" message to the DTE when the system establishes a connection, type **y**.
  - If you do not want the system to generate a "connected" message to the DTE when the system establishes a connection, type **n**.

  The system displays the **Connected Indication** field only if the **KBDY Dialing** field on the Data Module screen is set to **y**. If the **Connected Indication** field is set to **n**, DLC provides the connection indication when the DLC activates the EIA 232C control lead.
- In the **Dial Echoing** field, perform one of the following actions:
  - If you want the system to echo characters back to the DTE, type **y**.
  - If you do not want the system to echo characters back to the DTE and when an intelligent device provides keyboard dialing, type **n**.

  The system displays the **Dial Echoing** field only if the **KBDY Dialing** field on the Data Module screen is set to **y**.
- In the **Disconnect Sequence** field, perform one of the following actions:
  - Type **long-break** if you want a break that is greater than 2 seconds.
  - Type **two-breaks** if you want a break that is less than 1 second.

  The system displays the **Disconnect Sequence** field only if the **KBDY Dialing** field on the Data Module screen is set to **y**.
- In the **Parity** field, type one of the following types of parity:
  - even
  - odd
  - mark
  - space

  The system displays the **Parity** field only if the **KBDY Dialing** field on the Data Module screen is set to **y**. The DLC generates the parities when the DLC sends call setup text to the DTE. The DLC does not check the parity when the DLC receives dial characters. Select the parity that matches the DTE that connects to the data module.
- In the **Permit Mismatch** field, perform one of the following actions:
  - If you want the DLC to operate at the highest selected speed, which is a higher rate than that of the far end data module, type **y**.

— If you do not want DLC to operate at the highest selected speed, type **n**.

The **Permit Mismatch** field contains information that allows an EIA interface to operate at a rate that differs from the rate that is agreed upon during the data module handshake. The rate that is agreed upon during the data module handshake is always the highest compatible rate among the speeds that each data module reports.

The information in the **Permit Mismatch** field eliminates the need to change the DTE or DLC speed whenever someone, or something, places a call to or from endpoints that operate at a different speed.

When the **Permit Mismatch** field is set to **y**, the DLC reports the highest optional speed and all the lower speeds, or the previously selected autoadjust speed, during the handshake process.

13. In the **Port** field, type the appropriate values from Table 69: Port field values on page 589.

Table 69: Port field values

Characters	Description	Value
1-2	cabinet number	**01** through **44** (For DEFINITY R configurations) **01** through **03** (For DEFINITY SI configurations) **01** through **64** (For IP-PNC)
3	carrier	**A** through **E**
4-5	slot number	**0** through **20**
6-7	circuit number	**01** through **04** (x.25 circuit pack) **01** through **31** (DEFINITY SI, IP-PNC (tdm, pdm) configurations) **01** through **16** (ppp for IP-PNC **01** through **08** (system-port for IP-PNC) **17/33** (Ethernet on IP-PNC)
x	Administration without Hardware	If the **Secondary data module?** field, contains an **n**, you can type **x** in the **Port** field. A **Port** field set to **x** indicates that no hardware is associated with the port assignment.

14. The **Speeds** area contains information about the operating speeds of the data module.
    - In the **Low** field, perform one of the following actions:
      — If you want the data line circuit to operate at a speed of 0 to 1800 bps, type **y**.
      — If the **KYBD Dialing** field on the Data Module screen is set to **y**, type **n.**
    - In the **300, 1200, 2400, 4800, 9600,** and **19200** fields, perform one of the following actions:

- If you want the DLC to operate at the speed, type **y**.

  You can choose any of the speeds for the DLC. The DLC matches the speed for the duration of the call.

  If you select multiple speeds, you must also set the **Autoadjust** field to **n** and select at least three speeds. The speed of the DTE must be the highest speed that you select. The DTE must have the highest speed because the system delivers feedback to the DTE at the highest selected speed.

- If you do not want the DLC to operate at the speed, type **n**.

In the **Autoadjust** field, perform one of the following actions:

- If you want the DLC port to automatically adjust to the operating speed and the parity of the DTE to which the DLC port connects, type **y**.
- If you do not want the DLC port to automatically adjust to the operating speed and the parity of the DTE to which the DLC port connects, type **n**.

The system displays the **Autoadjust** field when the **KYBD Dialing** field on the Data Module screen is set to **y**. The **Autoadjust** field applies only to calls that a user originates from a keyboard.

15. In the **Special Dialing Option** field, perform one of the following actions:
    - Leave the field blank if you do not want the data module to have special dialing
    - If you want the data module to have hot-line dialing, type **hot-line**.

      If you type **hot-line**, the system displays the **Abbreviated Dialing Dial Code (from above list):** field. Type the abbreviated dial code in the **Abbreviated Dialing Dial Code (from above list):** field. Valid entries are **0** through **999**.
    - If you want the data module to have default dialing, type **default**.

      If you type **default**, the system displays the **Abbreviated Dialing Dial Code (from above list):** field. Type the abbreviated dial code in the **Abbreviated Dialing Dial Code (from above list):** field. Valid entries are **0** through **999**.
16. In the **TN** field, type the tenant partition number of the data module. Valid entries are **1** through **100**.
17. In the **Type** field, perform one of the following actions:
    - Type **7500** to assign a 7500 data module.

      The 7500 data module supports:

      - Automatic TEI
      - B-channel, maintenance and management messaging

— **Service Profile Identifier (SPID)** initialization capabilities.

BRI voice endpoints, BRI data endpoints, or both BRI voice and BRI data endpoints are assigned to either the **ISDN**-**BRI** - 4-wire S/T-NT Interface circuit pack **or the ISDN**-**BRI** - 2-wire U circuit pack. Each circuit pack supports up to 12 ports.

BRI provides a multipoint capability. Therefore, you can administer more than one ISDN endpoint, either a voice endpoint or a data endpoint, on one port.

For **BRI**, multipoint administration allows for telephones that have **SPID** initialization capabilities. Multipoint administration is allowed only if no endpoint that is administered on the same port is a fixed tie endpoint, and no station on the same port has B-channel data capability. The system restricts multipoint administration to two endpoints per port.

- Type **data-line** to assign a data line data module.

  Use the Data Line Data Module (DLDM) screen to assign ports on the Data Line (**DLC**) circuit pack that allow **EIA** 232C devices to connect to the system. The **DLC**, with a companion **ADU**, provides a less expensive data interface to the system than other asynchronous DCP data modules.

  The **DLC** supports asynchronous transmissions at speeds of low, and of 300, 1200, 2400, 4800, 9600, and 19200 bps over two-pair, full-duplex lines. These lines can have different lengths, depending on the transmission speed and the wire gauge.

  The **DLC** has eight ports. The connection from the port to the **EIA** device is direct, which means that no multiplexing is involved. A single port of the **DLC** is equivalent in functionality to a data module and a digital line port. The **DLC** appears as a data module to the **DTE,** and as a digital line port to the server that runs Communication Manager.

  The **DLC** connects the following **EIA** 232C equipment to the system:

  — Printers

  — Non intelligent data terminals

  — Intelligent terminals and personal computers (**PC**s)

  — Host computers

  — Information Systems Network (**ISN**), **RS**-232C local area networks (**LAN**s), or other data switches

- To assigns a DCE interface for processor/trunk data modules, type **pdm**.

  Use the Processor/Trunk Data Module screen to assign Modular Processor Data Modules (MPDMs) and Modular Trunk Data Modules (MTDMs). Use one screen to assign MPDMs (700D), 7400B, 7400D or 8400B Data Module. Use another screen for MTDMs (700B, 700C, 700E, 7400A). You must complete one screen for each MPDM, 7400B, 7400D, 8400B or MTDM.

  The MPDM, 7400B, or 8400B Data Module provides a Data Communications Equipment (DCE) interface. Use the interface for a connection to equipment such as a data terminal, call detail recording (CDR) output device, on-premises administration terminal, Message Server, Property Management System (PMS), CM Messaging, and host computers. The MPDM, 7400B, or 8400B Data Module also provides a Digital Communications Protocol (DCP) interface to the digital switch. Note that DCE is the equipment on the network side of a communications link that provides all the functions that are required to make the binary serial data from the source or transmitter compatible with the communications channel.

  The MTDM provides an EIA DTE interface for connection to off-premises private line trunk facilities, or a switched telecommunications network and a DCP interface for connection to the digital switch.Note that DTE is the equipment that comprises the endpoints in a connection over a data circuit. For example, in a connection between a data terminal and a host computer, the terminal, the host, and their associated modems or data modules make up the DTE. The MTDM or the 7400A Data Module can also serve as part of a conversion resource for combined modem pooling.

18. Press **Enter** to save your changes.

Identifying the Inter Exchange Carrier

To identify the Inter Exchange Carrier (IXC) in the CDR record:

1. Type **`change ixc-codes`**. Press **Enter**.

   The system displays the Inter-Exchange Carrier Codes screens (Figure 117: Inter-Exchange Carrier Codes screen on page 593) and (Figure 118: Inter-Exchange Carrier Codes screen on page 593).

Figure 117: Inter-Exchange Carrier Codes screen

```
change ixc-codes                                                Page 1 of 2

                      INTER-EXCHANGE CARRIER CODES

       IXC Codes Assignments (Enter up to 15)
       CDR   IXC                          CDR   IXC
       IXC   Access                       IXC   Access
       Code  Number    IXC Name           Code  Number    IXC Name
       1:    _______   ________________    9:   _______   ________________
       2:    _______   ________________   10:   _______   ________________
       3:    _______   ________________   11:   _______   ________________
       4:    _______   ________________   12:   _______   ________________
       5:    _______   ________________   13:   _______   ________________
       6:    _______   ________________   14:   _______   ________________
       7:    _______   ________________   15:   _______   ________________
       8:    _______   ________________
```

Figure 118: Inter-Exchange Carrier Codes screen

```
change ixc-codes                                                Page 2 of 2

                          IXC Prefix             IXC Code Format
                     1.   ___                    ____
                     2.   ___                    ____
                     3.   ___                    ____
                     4.   ___                    ____
                     5.   ___                    ____
```

2. In the **IXC Access Number** field, type the digits that the user dials, or that AAR/ARS inserts, into the outpulsed digit string so the system can access the IXC. The system does not allow duplicate access numbers in the Inter-Exchange Carrier Codes screen.

   The system accepts a string of 2 to 11 numbers or the asterisk character (*****) in the **IXC Access Number** field.

3. In the **IXC Name** field, type a description of the IXC. The system accepts a 1 to 15 character string in the **IXC Name** field. You can also leave this field blank.

4. In the **IXC Code Format** field, type the format for the IXC code. The valid entries for this field are a:

   - 1 to 4 digit code
   - Asterisk (*)
   - Lower-case x

- Upper-case X
- String of 4 lower-case x's (xxxx) to indicate line one
- String of 3 lower-case x's (xxx) to indicate line two

5. In the **IXC Prefix** field, type the prefix for the IXC code. The valid entries for this field are a:
   - Prefix of 1 to 3 digits
   - Asterisk (*)
   - 101 to indicate line one
   - 10 to indicate line two
6. In the **CDR Account Code Access Code** field, type the access code that a user enters before the user enters a CDR account code.
7. Press **Enter** to save your changes.

Administering CDR for the paging ports

To administer CDR for the paging ports:

1. Type **`change paging loudspeaker`**. Press **Enter**.

   The system displays the Loudspeaker Paging screen (Figure 119: Loudspeaker Paging screen on page 594).

Figure 119: Loudspeaker Paging screen

```
change paging loudspeaker                                    Page   1 of 1
                            LOUDSPEAKER PAGING

                                      CDR? _
                  Voice Paging Timeout (sec): ___
                 Code Calling Playing Cycles: _

PAGING PORT ASSIGNMENTS
                    Voice Paging      Code Calling
 Zone  Port         TAC  COR  TN      TAC  COR  TN     Location:
   1: _______      ____ __   _       ____ __   _      ______________________________
   2: _______      ____ __   _       ____ __   _      ______________________________
   3: _______      ____ __   _       ____ __   _      ______________________________
   4: _______      ____ __   _       ____ __   _      ______________________________
   5: _______      ____ __   _       ____ __   _      ______________________________
   6: _______      ____ __   _       ____ __   _      ______________________________
   7: _______      ____ __   _       ____ __   _      ______________________________
   8: _______      ____ __   _       ____ __   _      ______________________________
   9: _______      ____ __   _       ____ __   _      ______________________________
 ALL: _______      ____ __   _       ____ __   _
```

2. In the **CDR** field, perform one of the following actions:
   - If you want the system to record CDR information on the paging ports, type **y**.
   - If you do not want the system to record CDR information on the paging ports, type **n**.
3. Press **Enter** to save your changes.

Administering the Intra-Switch CDR

To administer Intra-Switch CDR:

1. Type **`change intra-switch-cdr`**. Press **Enter**.

   The system displays the Intra-Switch CDR screen (Figure 120: Intra-Switch CDR screen on page 595).

Figure 120: Intra-Switch CDR screen

```
change intra-switch-cdr                                        Page   1 of 2
                          INTRA-SWITCH CDR

Assigned Members:   8    of 5000   administered
  1: 70103    19:          37:          55:          73:          91:
  2: 70105    20:          38:          56:          74:          92:
  3: 70112    21:          39:          57:          75:          93:
  4: 70115    22:          40:          58:          76:          94:
  5: 70120    23:          41:          59:          77:          95:
  6: 70122    24:          42:          60:          78:          96:
  7: 70124    25:          43:          61:          79:          97:
  8: 70126    26:          44:          62:          80:          98:
  9:          27:          45:          63:          81:          99:
 10:          28:          46:          64:          82:         100:
 11:          29:          47:          65:          83:         101:
 12:          30:          48:          66:          84:         102:
 13:          31:          49:          67:          85:         103:
 14:          32:          50:          68:          86:         104:
 15:          33:          51:          69:          87:         105:
 16:          34:          52:          70:          88:         106:
 17:          35:          53:          71:          89:         107:
 18:          36:          54:          72:          90:         108:
```

2. In the **Assigned Members** field, type the local extensions that you want to track with intraswitch CDR. The number of extensions that you can track can vary.
3. Press **Enter** to save your changes.

Administering Survivable CDR

Use the following high level steps to administer the Survivable CDR feature:

1. Create a new user account to allow the CDR adjunct access and permissions to retrieve CDR data files (see Creating a new user account on page 596).
2. Enable CDR storage on the hard disk (see Administering Survivable CDR for the main server on page 597).
3. If using this feature on the main server: Administer the **Primary Output Endpoint** field on the main's **`change system-parameters cdr`** SAT form to be **DISK** (see Administering Survivable CDR for the main server on page 597). When using Survivable CDR, only the **Primary Output Endpoint** field is available. Administration of the **Secondary Output Endpoint** field is blocked.
4. If you are using this feature on an LSP and an ESS server: Administer the **Enable CDR Storage on Disk** field on the **`change survivable-processor`** screen (see Administering Survivable CDR for an LSP or ESS server on page 598).

Creating a new user account

For the CDR adjunct to access the CDR data files, a new user account must be created on the main server. The new account is pushed to the LSP and/or ESS server when a filesync is performed.

To create a new user account:

1. On the server's Integrated Management Maintenance Web Page, click **Administrator Accounts** under the Security heading.

   The Administrator Accounts page displays.
2. Enter the login ID for the new user in the **Enter Login ID or Group Name** field.
3. Click the **Add Login** radio button and then click **Submit**.

   Administrator Logins -- Add Login page displays.
4. Enter the data in Table 70 in each field of the Administrator Logins -- Add Login page.

Table 70: CDR adjunct user account recommended options

Field Name	Recommended Option
Login Name	Any valid user name chosen by the administrator or installer
Login group	CDR_User
	1 of 2

Table 70: CDR adjunct user account recommended options (continued)

Field Name	Recommended Option
Shell:	Select CDR access only by clicking the associated radio button.
Lock this account	Leave blank
Date on which the account is disabled	Leave blank
Select type of authentication	Password
Enter key or password	Any valid password chosen by the administrator or installer
Re-enter key or password	Re-enter the above password
Force password/key change on first login	no
Maximum Number of days a password may be used (PASS_MAX_DAYS)	99999
Minimum number of days allowed between password changes (PASS_MIN_DAYS)	0
Number of days warning given before a password expires (PASS_WARN_AGE)	7
Days after password expires to lock account	-1
	2 of 2

5. Click **Add** to create the new user account.

Administering Survivable CDR for the main server

Use the following steps to administer the Survivable CDR feature for a main server:

1. On page one of the **`system-parameters cdr`** form (see Figure 121):
   a. **Enable CDR Storage on Disk?**: Possible entries for this field are **yes** or **no**. Entering **yes** in this field enables the Survivable CDR feature for the main, LSP, and ESS servers.
   If this field is set to **no**, the CDR functionality remains as legacy CDR.

b. **Primary Output Endpoint**: Possible entries for this field are **CDR1**, **CDR2**, and **DISK**. For the main server, the **Primary Output Endpoint** field must be set to **DISK**. When Survivable CDR is administered as **Disk** on the **Primary Output Endpoint** field, the **Secondary Output Endpoint** field is blocked.

Figure 121: CDR System Parameters screen

```
change system-parameters cdr                                    Page   1 of   2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 10                     CDR Date Format: month/day
      Primary Output Format: customized    Primary Output Endpoint: DISK

           Use ISDN Layouts? n                   Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? y                 Remove # From Called Number? n
Modified Circuit ID Display? n                             Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? n
      Disconnect Information in Place of FRL? y      Interworking Feat-flag? y
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                  Calls to Hunt Group - Record: group-ext
Record Called Vector Directory Number Instead of Group or Member? y
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? n
     Inc Trk Call Splitting? y                  Inc Attd Call Record? y
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 15
```

Administering Survivable CDR for an LSP or ESS server

Use the following steps to administer the Survivable CDR feature for an LSP or an ESS server:

Note:
The Survivable CDR feature is administered on the main server for the LSP and ESS servers.

Important:
An LSP or ESS server only stores Survivable CDR records if it is administered to support Survivable CDR and if it is controlling one or more gateways or port networks.

1. On the **`system-parameters cdr`** form:
   a. **Enable CDR Storage on Disk?**: Possible entries for this field are **yes** or **no**. Entering **yes** in this field enables the Survivable CDR feature for the main, LSP, and ESS servers. If this field is set to **no**, the CDR functionality remains legacy CDR.

2. Survivable-processor screen, page three (see Figure 122):
   a. **Service Type**: The **Service Type** field must be set to **CDR1** or **CDR2** to enable entries to the **Store to Dsk** field.
   b. **Store to Dsk**: Enter **y** to enable Survivable CDR for this LSP or ESS server. When the **Service Type** field is set to **CDR1** or **CDR2** and the **Store to Dsk** field is set to **yes**, all CDR data for the specific LSP or ESS server being administered will be sent to the hard disk rather than output to an IP link. LSP or ESS servers will only store CDR records to hard disk when the LSP or ESS server is controlling a gateway or port network.

Important:
You must complete the Survivable Processor screen on page 599 for ***each*** LSP or ESS server that will utilize the Survivable CDR feature.

Note:
The **Enable** field for a given line in the **`change survivable-processor`** screen must be set to 'o' (overwrite) to allow changes for that line.

Figure 122: Survivable Processor screen

```
change survivable-processor sv-ess8                              Page   3 of   4
                    SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local             Local    Remote            Remote
  Type              to dsk  Node              Port     Node              Port
  CDR1        i       y     st10clan26        0        cdr_1             9002
  CDR2        i       n     st10clan26        0        CDRterm_srv       5111
```

End-user procedures for Call Detail Recording

End-users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Call Detail Recording:

- Associating an account code with a call

To associate an account code with a call:

1. Dial the CDR account code access code that you assigned.
2. Dial an account code.
3. Dial a trunk access code (TAC) or an access code.

4. Dial the telephone number.

Considerations for Call Detail Recording

This section provides information about how the Call Detail Recording (CDR) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Detail Recording under all conditions. The following considerations apply to Call Detail Recording:

- Date and Time

  If you do not administer the time of day in your system, the software does not generate CDR records.

  If a call is in progress while you change the time of day information, the system does not record the duration of the call in the CDR record. Instead, the system records the numeric sequence 9999 in the CDR record. This sequence indicates that the call was in progress when you changed the time of day information.

- Dial plan

  If the dial plan in your system supports 6-digit or 7-digit extensions, only the formats that already support calling numbers that are longer than 7 digits support 6-digit or 7-digit extensions. Such numbers include expanded, unformatted, customized, and international ISDN calling numbers.

  All other calling number formats send only 5 digits. If the calling number is a 6-digit or a 7-digit extension, the system sends only the last 5 digits.

The following information applies to the port that the secondary CDR output device uses:

- The data that go to the secondary port must be the same as the data that go to the primary port. You can use the following record types for the secondary output:
  - LSU
  - Int-Direct
  - Int-Process
  - Unformatted
- If the system cannot send records to the primary CDR output device, the system discontinues sending records to the secondary port for 2 minutes. The secondary port must operate at the highest possible speed to prevent the loss of information.
- If the output buffer is full, the system busies out the secondary port for 2 minutes. This action makes system resources available to send data to the primary CDR port before the data is lost. The system continues to busy out the secondary port for 2-minute intervals until fewer than 400 records, or 1800 records for Release 5r and later, remain in the buffer.

- When QSIG Advice of Charge is set to receive charging information during a call, message activity is increased on the signaling channel, which has an impact on maximum call capacity.

Interactions for Call Detail Recording

This section provides information about how the Call Detail Recording (CDR) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call Detail Recording in any feature configuration.

- Abbreviated Dialing

  When a user uses either Abbreviated Dialing or a Facility Busy Indicator button to place a call, all the outpulsed digits appear on the record.

- Answer Detection

  CDR starts recording call duration at the time that the circuit pack detects the answer.

  Answer Detection provides more accurate call records where tone detection is possible, and Network Answer Supervision is not received.

- Attendant Console

  If an attendant-assisted call uses an outgoing trunk, the system records the primary extension of the user who requests the attendant service as the calling number in the CDR record. The system records the primary extension of the user, even if the attendant dialed an outside number.

  Condition code 1 indicates an attendant assisted the call.

  If the attendant allows through dialing, the system records the primary extension of the user who dialed the number as the calling party. Condition code 1 indicates that an attendant extended a trunk access code (TAC). Condition code 7 indicates that an attendant extended a Feature Access Code (FAC).

  If Incoming or Outgoing Attendant Call Record is enabled, the system produces a separate record for the attendant portion of incoming or outgoing calls that the attendant transfers.

  With attendant-assisted calls that require an account code, enter the account code before the TAC.

  If the attendant redirects an incoming call to an extension, the attendant can dial an account code before the attendant dials the extension number.

  There are no intraswitch-optioned attendant calls. However, the system generates intraswitch records for an intraswitch-optioned extension call to an the attendant or for a call from the attendant to an intraswitch-optioned extension. In the case of an attendant-assisted call that involves an intraswitch extension, the system records the extension of the user who called the attendant as the dialing number. The system records the extension to which the attendant extended the call as the dialed number. In this case, the record has condition code 0.

- CM Messaging

  The following example describes CDR for remote CM Messaging over a distributed communications system (DCS). If station A on node 1 forwards calls to CM Messaging on node 2, each switch produces a call record. The record from node 1 contains A as the dialed number. The record from node 2 contains CM Messaging as the dialed number.

  If the calling number is on a different switch within the DCS network, or the call comes in over ISDN, the system records the:

  – The actual calling number in the **Calling Number** field
  – The TAC of the trunk that brings the call into the local switch in the **Incoming Trunk Access Code** field of 24-word records

  If the system uses an outgoing trunk when a user forwards, transfers, or conferences an incoming call, the system generates two separate CDR records. The system generates a record for incoming usage, and a record for outgoing trunk usage. The system records CM Messaging as the calling number in the outgoing trunk usage record

  If Incoming Trunk Call Splitting is enabled, and Transfer out of AUDIX is used, CDR generates two records. The first record contains CM Messaging, the second record contains the transferred-to party.

- Authorization Codes

  The system records authorization codes in CDR records as follows:

  — The account codes do not exceed 5 digits in length for non-ISDN formats and ISDN LSU formats

  — The account codes do not exceed 4 digits in length for enhanced LSU formats

  The system does not record authorization codes in the 59-character CDR International Processing and International Direct records.

- Automatic Selection of Direct Inward Dialing (DID) Numbers

  If the system records an incoming call, the system records the DID extension number, not the room extension number.

- Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS)

  For ARS calls, the system records that the:

  — ARS call was made

  — Calling extension number

  — Facilities restriction level (FRL) of the calling extension

  — Called number

  — TAC of the trunk group that is used for the ARS call

  — Time of call completion

  — Call duration

  — Interexchange carrier (IXC) code, if any

  The system does not generate a CDR record if CDR is suppressed for the trunk group that ARS uses. If CDR is not suppressed, the system generates condition code 7. The system records the following information:

  — The ARS access code in the **Access Coded Dialed** field

  — The TAC for the trunk group that the call used in the **Access Code Used** field.

  If an AAR call is placed to a busy trunk group, and CDR is suppressed for that trunk group, the user hears the reorder tone, and the CDR record shows an ineffective call attempt.

  If an ARS call is an attendant-assisted call, the CDR record shows the call with condition code 7 instead of condition code of 1. Condition code 7 indicates an ARS call. Condition code 1 indicates an attendant-assisted call. The system generates these condition codes, because CDR is not notified until after the trunk is seized and, in this case, the trunk is not seized until the user dials the number.

  With the Forced Entry of Account Codes (FEAC) capability, the system does not use the class of service (COR) of the trunk group to determine if the user must enter an account code, if the system uses ARS to access the trunk.

- Automatic Callback

  When the Automatic Callback feature is used for an intraswitch call, the system does not generate a CDR record for the first call attempt, nor for the ringback. However, if intraswitch is enabled for either the calling user or the called user, the system generates a CDR record of the call, if the called user answers and completes the call.

- Automatic Circuit Assurance (ACA)

  ACA calls generate intraswitch CDR records if CDR monitors the terminating extension. The originating extension for ACA calls cannot be administered for intraswitch monitoring.

- Automatic Wakeup

  The system does not generate CDR intraswitch records for wake-up calls.

- Bridged Call Appearance

  The system does not record CDR information about the user who bridges onto a call. Instead, the system records the number that a user dialed in the **Dialed Number** field of the CDR record. The system records the duration of the call when the last party drops off the call.

  If the user originates a call over a bridged appearance, the call record contains the calling number of the bridged appearance extension, and not the extension number of the original, calling station.

- Busy Verification of Terminals and Trunks

  Attendants and users do not need to enter an account code to make a busy verification.

- Call-by-Call Service Selection

  When the system successfully makes a call on a Call-by-Call Service Selection trunk, the system translates the network-specific facility that the system uses for the call into an ISDN network service (INS) number. The system records the INS number in the **INS** field of the CDR record.

  If the system is unsuccessful in making a call on a Call-by-Call Service Selection trunk because of an administered trunk usage allocation plan, the system records the INS number in the **INS** field of the CDR Record with condition code *E*.

- CallVisor Adjunct-Switch Application Interface (ASAI)

  Call classification competes with CallVisor ASAI switch-classified calls for ports on the call classifier circuit pack. Answer Detection sends a report of a connect event to ASAI.

- Call Coverage

  If the system does not route a call to an off-network coverage point, the system records the extension number that the calling user dials as the dialed number when a user answers an incoming call or an intraswitch call at a covering extension.

  If the system routes a call to an off-network coverage point, the system records the number at the off-network location as the dialed number. The system records the extension that has the off-network location in its coverage path as the calling number.

- Call Forwarding All Calls

  If the system does not forward a call to an off-network location, the system records the number that the user dials as the dialed number.

  If the system forwards a call to an off-network location, the system records the number of the
  off-network location as the dialed number. The system records the extension from which the call was forwarded as the calling number.

  The system generates one CDR record for a forwarded intraswitch call. The dialed number in the record is the extension that the calling user dialed.

  The system generates two CDR records for a trunk call to a station that the system forwards to another trunk. The first record shows an incoming trunk call to the station. The second record shows an outgoing trunk call from the station.

  With the FEAC capability, the system cannot forward to a destination at which a user must enter an account code.

- Call Park

  When a user parks an incoming call or an intraswitch call, the system records the extension of the user as the dialed number in the CDR record. The system records the entire time that the incoming trunk is busy as the duration of the incoming call. The system records the time that the call started until the call ends as the call duration for an intraswitch call.

- Call Pickup

  The system records the number that the user dials as the dialed number when a member of a pickup group answers an incoming call or an intraswitch call.

- Call Prompting

  Call classification competes with Call Prompting for ports on the call classifier circuit pack.

- Call Vectoring

  You can administer CDR so the system records the vector directory number (VDN) extension instead of the extension of the Hunt Group or of the member. If you administer CDR so the system records the VDN extension, you override the Calls to Hunt Group - Record option of CDR for incoming call vectoring calls.

  Outgoing vector calls generate ordinary outgoing CDR records. The system records the originating extension as the calling number.

  The system records the duration of the call from the time that answer supervision is returned for incoming calls to a VDN.

  — If the vector returns answer supervision, and the call does not go to another extension, the system records the VDN extension as the called number in the CDR record. The vector can return answer supervision with an announcement, collect, disconnect, or wait with music command.

- If the call terminates to a hunt group, the system records the VDN, the hunt group extension, or the agent extension as the called number in the CDR record.
- If the call terminates to a trunk, CDR generates an:
  - Incoming record with the incoming TAC as the dialed number.
  - Outgoing record with the incoming TAC as the calling number and the digits that are dialed through the vector step as the dialed number.

If you administer member extension for CDR, the system records an incoming call to the station if the system successfully routes a call to the station with the **route-to** command.

The system does not generate ineffective call attempt records for unsuccessful Call Vectoring **route-to** commands.

If a vector interacts with an extension or a group that has Call Forwarding All Calls active, normal Call Forwarding and CDR interactions apply.

Some calls look like intraswitch calls. Such calls include, for example, a call for a station that is administered for intraswitch CDR to a VDN, which becomes an outgoing call on an outgoing trunk. The system does not generate instraswitch CDR records for calls that look like intraswitch calls, but that are not intraswitch calls. The system generates a record with condition code A, which indicates outgoing.

- Call Waiting Termination

  The system starts the call duration timer when a user answers an incoming call.

- Centralized Attendant Services (CAS)

  The system records the extension of the user who originates a call as the originator of a call, if a CAS attendant extends the call to the user, and CDR is not assigned to the RLT trunk group.

  The system records the RLT trunk as the originator of a call, if a CAS attendant extends the call to the user and CDR is assigned to the release-link trunk (RLT) trunk group.

  The system does not generate a CDR record, if a CAS attendant answers a call but does not extend the call to a user.

- CO Trunks

  The system records all incoming and outgoing calls on a central office (CO) trunk group, if CDR is assigned to the trunk group, and CDR is administered to record incoming calls.

- Conference

  The system records a conference call for CDR, if either of the following conditions is met:

  - The call uses at least one trunk that is eligible for CDR, and has two or more parties

– The call has at least one party that is optioned for intraswitch CDR.

The system records condition code C for each conference call CDR record.

The system generates a separate conference call CDR record for each outgoing trunk and each incoming trunk that serves the conference call. If you enable either, the system also generates a separate record for each internal party on the call.

For the outgoing portion of a conference call that involve multiple extensions, the system records the extension of the user who requests the outside dial tone to include another participant, as the calling party.

The system records the entire time that an incoming trunk or an outgoing trunk is used for a conference call, as the duration of the call.

The system generates a separate CDR record for each trunk that is used in a trunk-to-trunk transfer. If incoming trunk call splitting (ITCS) is active, the incoming trunk record shows the duration of the entire call.

The system starts a new CDR record whenever the originator of a conference call dials a nontrunk participant, if the conference call is optioned for intraswitch CDR. For example, station 1 is optioned for intraswitch CDR and calls station 2. Station 1 includes station 3 in the conference call. Station 1 drops from the call. Station 2 or station 3 drops from the call. The system generates two CDR records with condition code *C*. The system generates one record from station 1 to station 2, and another record from station 1 to station 3.

The system generates one record with condition code *C* for each dialed intraswitch conference participant, if any of the conference participants are optioned for intraswitch CDR. The system generates a record with condition code *C*, even if the originator of the conference is not optioned for intraswitch CDR. For example, station calls station 2, which is optioned for intraswitch CDR. Station 1 includes station 3 into the conference call. Station 1 drops from the call. Station 2 or station 3 drops from the call. The system generates one CDR record with condition code C from station 1 to station 2.

The system generates intraswitch conference call CDR records when both the calling party and the called party call drop from the call. The system records the call duration from the time that the called party answers the call until both the calling party and the called party drop from the call.

If an attendant originates a conference, the system generates CDR records only for the dialed numbers that correspond to any intraswitch optioned extensions.

- Distributed Communications System DCS

  The system does not pass station information throughout the DCS network for CDR records.

- Direct inward dial (DID) trunks

  If you administer the system to record incoming CDR information, and if you administer CDR for the trunk group, the system records all incoming calls on the DID trunk group.

- Emergency Access to the Attendant

  The system does not generate intraswitch CDR records for Emergency Access calls.

- Expert Agent Selection (EAS)

  You can assign a logical extension to an agent who can then use the logical extension to log in to a telephone. You can administer CDR so that the system records the logical extension of the agent as the called number. The system records the logical extension as the called number instead of the extension of the hunt-group or the hunt group member.

- Foreign Exchange (FX) Trunks

  If you want the system to generate CDR records for calls to FX trunks, you must administer your system to generate those records. You must also administer each trunk group so the system generates a CDR record for the trunk group.

- Hotline Service

  The system generates a CDR record of the stored number that is used on an outgoing or intraswitch Hotline call as if someone manually dialed the number.

- Hunt Groups

  You can administer CDR so the system records either the extension of the hunt group or the extension of the individual hunt group member as the called number.

- Intercept Treatment

  If the system routes an outgoing call or a tandem call to intercept treatment, the system records the number that the user dialed as the dialed number. The system also records condition code *F*.

- Inter-PBX Attendant Calls

  Table 71: Inter-PBS CDR information on page 608 shows the information that the system records if a user calls an Inter-PBX attendant, and the call uses a trunk group that has CDR assigned.

Table 71: Inter-PBS CDR information

CDR data field	Value
Condition Code	A
Access Code Dialed	Blank
Access Code Used	The TAC of the trunk that the call used
Dialed Digits	The Inter-PBX attendant access code

- ISDN

  The system sends an indication to the CDR device when the system receives a true answer supervision.

  The system crates a CDR record each time that the system networks an ISDN call. In this case, the answer supervision information that the system records might not be accurate. If you use unformatted or expanded record formats, the station identification number (SID) or the automatic number identification (ANI) appears in the CDR record, if the SID or ANI is sent.

- Last Number Dialed

  The system stores the CDR access code and the account code that the user dials as part of the Last Number Dialed. However, some digits might be lost, because of the limit on the number of digits that can be stored for the Last Number Dialed feature.

- Manual Originating Line Service

  If an attendant establishes an outgoing call for a user, and designates the call as a Manual Originating Line call, the system generates an attendant-assisted outgoing call CDR record. The system records the extension of the user who originated the call as the calling number, and applies condition code *1*.

- Multiple Listed Directory Numbers (LDNs)

  If the system records incoming call information, the system records the extension number or the TAC to which the attendant completes the call, as the called number of LDN calls.

  If the system records incoming call information, the system records the attendant extension as the dialed number, if the call terminates at the attendant console.

  You cannot administer LDNs for intraswitch CDR. However, the system generates an intraswitch CDR record for a call from an intraswitch-optioned extension to an LDN.

- Night Service

  The system records the extension number that is assigned to the attendants as the dialed number for night service calls.

- Off-Premises Station

  The system generates a CDR record for a call to an off-premises station when the:

  — Call involves an outgoing or an incoming trunk call.

  — Off-premises station is optioned for intraswitch CDR.

  — Other terminal that is involved in the call is optioned for intraswitch CDR.

- Personal Central Office Line (PCOL) trunks

  If the system records incoming calls, the system records the primary extension of the user who answers the call as the called number for incoming PCOL call.

  The system records an outgoing PCOL call as a call from the originating extension number through the trunk group that is associated with the PCOL.

  The system records the dialed number in the **Dialed Number** field for an outgoing PCOL call. The system does not record the TAC in the **Dialed Number** field for an outgoing PCOL call.

- Planned Interchange

  When any planned interchange occurs, the system might record calls that end within 10 to 20 seconds after the interchange as calls that have an invalid duration. A call with an invalid duration is a call with a duration of 9:59:9, and a condition code other than 4. These call records are invalid. Deviations in the clocks between the two processors, and the short duration of the calls, cause the invalid duration.

- Private Network Access

  The system records Private Network Access calls, if CDR is assigned for incoming or outgoing tie trunks.

- Remote Access

  The system records remote access calls if Remote Access is provided on a per-trunk-group basis, and you administered CDR for those trunks. The trunk group access code in the call record is the only indication that the record is for a remote access call.

- Ringback Queuing

  The system records condition code *8* for an outgoing call that is in a trunk queue before the call is complete. The system does not record the time that the call is in the queue.

  The system does not generate a CDR record if a call waits in a trunk queue, and the call is not successfully completed. The call is not completed successfully if the time that the call waits in the queue exceeds the wait limit for the queue, or if the calling party does not answer the callback.

- Security Violation Notification (SVN)

  The system generates a CDR record for a SVN call if the terminating extension is monitored. You cannot administer the originating extension for intraswitch monitoring.

- Service Observing

  The system does not generate CDR records for Service Observing calls.

- Tandem Tie-Trunk Switching

  The calling party on an incoming trunk can dial the CDR account code. The system records the TAC for the incoming trunk group in the **Calling Number** field in the CDR record. The system records the number that the user dials as the number dialed.

- Temporary Bridged Appearance

  A CDR record is unaffected if a second user, or subsequent user, bridges a call.

- Temporary Signaling Connections (TSCs)

  If you administer CDR to use ISDN layouts, the system records call-associated TSCs and TSC requests in the call record. If you administer CDR to record noncall-associated/ temporary-signaling connection (NCA TSCs) and TSC requests, the system generates separate CDR records for each type of TCS. The system records the TCS data in the **TSC Flag** field and **Packet Count** field.

- Tie-Trunk Access

  Tie-trunk calls are recorded if CDR is administered to record the trunk group, and to record incoming calls.

- Transfer

  If a user originates a call on an outgoing trunk and then transfers the call to another extension, the system records the originating extension as the calling party.

  If a user receives a call on an incoming trunk and then transfers the call to another extension, the system records the extension that originally received the call as the dialed number.

  If a user receives an intraswitch call and then transfers the call to another extension, the system records the extension that originally received the call as the dialed number.

  The system generates two CDR records if all the following conditions are met:

  — Call splitting is active.

  — A user receives or originates a trunk call.

– The user transfers the call to another extension

The system generates intraswitch CDR records for each call to or from an intraswitch optioned extension. For example, station A, which is intraswitch optioned, calls station B. Station A then transfers the call to station C. When either station B or station C drops, the system generates two CDR records with a condition code 0. The system generates a CDR record for a call from station A to station B, and a second record for the call from station A to station C.

The system generates intraswitch CDR transfer records when both the calling party and the called party drop from the call. The system records the call duration from the time that the called party answers the call until both the calling party and the called party drop the call.

The system generates an incoming trunk call CDR record if ITCS is enabled, and a user transfers the call to a local extension that is optioned for Intraswitch CDR. The system does not generate an intraswitch record.

When a user transfers a call to another extension, a users cannot dial an account code, unless the user has console permissions.

When a user transfers a call to a trunk, the user can dial an account code before the user dials the ARS or the TAC.

- Trunk-to-Trunk Transfer

  With CDR, the system processes a trunk-to-trunk transfer connection as a conference call. The system generates a separate CDR record for each trunk in the connection.

  You can administer CDR so that the system records unanswered trunk calls. You can administer each trunk group so the system records unanswered calls if the calls remain unanswered for an interval that you specify.

  If Incoming Trunk Call Splitting is active, the system generates a CDR record for a trunk-to-trunk transfer. The system generates a record of the incoming call, and a record of the outgoing call. The system records the duration of the outgoing call from the time that the user transfers the call until both parties drop the call. The system records the duration of the incoming call from the time that the user answers the call until both parties drop the call.

- Uniform Dial Plan (UDP)

  Table 72: Uniform dial plan CDR information on page 612 shows the information that the system records if a user uses a UDP extension to call another user, and the trunk group that the call uses has CDR assigned.

Table 72: Uniform dial plan CDR information

CDR data field	Value
Condition Code	7
Access Code Dialed	Blank

Table 72: Uniform dial plan CDR information

CDR data field	Value
Access Code Used	The TAC of the trunk that the call used
Dialed Digits	The UDP extension

- VDN Return Destination

  The system does not generate a CDR record for an incoming call until the originator drops from the call. The system creates a CDR record when all the following conditions are met:

  — A call goes to the return-destination VDN.

  — The originator has not dropped.

  — Vector processing, that is the return destination VDN, routes the call to an outgoing trunk.

  The system does not create a CDR record if vector processing routes a call from the return-destination VDN to an internal call. The system records only the first VDN that the caller accesses, regardless of the number of other extensions that are involved in the call.

  If the system routes an incoming VDN call to a station, the system includes the station in the CDR record. If the system routes an incoming VDN call to an outgoing trunk, the system includes the VDN in the CDR record.

Interactions for QSIG Supplementary Service - Advice of Charge

The following are the interactions for the QSIG Supplementary Service - Advice of Charge feature.

- Adjunct-Switch Application Interface (ASAI) - ASAI Advice of Charge and CDR may both receive charge information from the network about the same trunk.
- Call Detail Recording - In cases in which the CDR adjunct is to collect information at a switch other than the one directly connected to the PSTN, all switches in the PTN must be upgraded to be able to transport the QSIG messages at the served user switch.

  — When the **Charge Advice** field is set to either *end-on-request* or *during-on-request,* CDR records charge advice and displays it on the user's terminal.

  — For CDR Call Splitting to work properly, QSIG Advice of Charge must be set to receive charge information *during* the call. (Call Splitting applies to calls with endpoints within a CM system as parties of a call that also have a trunk endpoint in the call for which CDR is enabled.)

  - If Call Splitting is enabled, the CDR record associated with the final party on an outgoing call contains the ISDN call charge for the entire call, since no charge advice data is available until the final party drops off the call. The ISDN call charge in all earlier CDR records is 0 (zero). However, the Elapsed Time in the CDR records is correct and can be used to allocate the call charge among the parties on the call.
  - If Call Splitting is disabled, the CDR record associated with the party that made the initial outgoing call contains the ISDN call charge for the entire call.
  - For calls diverted to another switch, if Call Splitting is enabled when an outgoing call is transferred, a CDR record is issued for the initial portion of the call, and the **ISDN Call Charge** field reports the Advice of Charge information received thus far. Subsequent Advice of Charge information received from the network for the outgoing call is not sent to the switch to which the call is diverted.

- Call Transfer - An originating user can request a call transfer during a call in which Advice of Charge has been invoked. In this scenario:
  - Communication Manager, as an outgoing gateway, does not provide charge data to the transferring or transferred-to switch at the end of the call.
  - The gateway may or may not know the call is transferred unless it receives an invocation for an additional charge request after Call Transfer from the transferred-to switch. If an invocation is received, then only interim charge information can be sent to the originating switch.
  - If the interim charge information is used on the PSTN side, but the call continues after the transfer is complete, then final charge information is not interworked into the PTN to any switch. If the call continues on the PSTN side, any charge information received from the PSTN is not interworked into the PTN.
- Charge Advice Display - The charge information can additionally be displayed at the served user's calling endpoint, either automatically or manually.

Call Forwarding

Use the Call Forwarding feature to redirect calls to an:

- Internal extension
- Off-network number
- Attendant group

Detailed description of Call Forwarding

This section provides a detailed description of the Call Forwarding feature.

Call Forwarding supports the following capabilities:

- Call Forwarding All Calls
- Call Forward Busy/Don't Answer
- Call Forwarding Off-Net
- Call Forwarding Override

Call Forwarding All Calls

Users use the Call Forwarding All Calls capability to redirect any incoming calls to another destination. You can restrict access to the Call Forwarding All Calls capability to specific users.

A user cannot have both the Call Forwarding All Calls capability and the Call Forward Busy/ Don't Answer capability active at the same time.

The system forwards a call only once. For example, assume that extension A designates extension B as its forwarded-to destination, and that extension B designates extension C as its forwarded-to destination. When someone calls extension A, the system first attempts to ring the call at extension A. If the system is unable to ring the call at extension A, the system attempts to ring the call at extension B. If the system is unable to ring the call at extension B, the system redirects the call to the coverage path of extension A, if a coverage path is available at extension A, and if the coverage criteria of extension A are satisfied when applied at extension B. The system does not forward the call to extension C under any circumstances.

The system can forward an unlimited number of calls simultaneously.

Call Forwarding and FAC

Users use a Feature Access Code (FAC) or a Call Forward-All feature button to activate or deactivate Call Forwarding All Calls for their own telephone. Virtual extension users cannot activate or deactivate Call Forwarding All Calls. Users can activate or deactivate the Call Forwarding All Calls feature for the following entities:

- Another extension
- A virtual extension
- An Automatic Call Distribution (ACD) split

Call Forwarding and attendants

The attendant cannot have a Call Forwarding button.

The system does not forward calls to attendants. However the system does forward calls to an attendant group.

Only the attendant, or a telephone user with console permission, can activate the Call Forwarding All Calls capability for the following entities:

- A terminating extension group (TEG)
- A direct department calling (DDC) hunt group
- A uniform call distribution (UCD) hunt group
- Data modules

Attendants and users cannot activate or deactivate the Call Forwarding All Calls capability for a vector-controlled split under any circumstances.

Call Forward Busy/Don’t Answer

Users use the Call Forward Busy/Don’t Answer capability to redirect incoming calls to another destination when the user:

- Is busy on a call

  If the user is busy on a call, the system immediately forwards the call. The system does not cause the telephone to ring before the system forwards the call to another destination.

- Does not answer the call within the allowed time interval

  If the user does not answer the call, the telephone rings for the allowed time interval. At the end of the interval, the system forwards the call to another destination.

You can restrict access to the Call Forward Busy/Don’t Answer capability to specific users.

A user cannot have both the Call Forward Busy/Don’t Answer capability and the Call Forwarding All Calls capability active at the same time.

Users activate or deactivate the Call Forward Busy/Don’t Answer capability with an FAC or a Call Forward Busy/Don't Answer feature button. Attendants or users that have console permission can also activate or deactivate the feature for another extension with an FAC. Virtual extension users cannot activate or deactivate Call Forwarding Busy/Don’t Answer.

Call Forward Busy/Don't Answer cannot be activated for calls to hunt groups, data extensions, a TEG, or an Expert Agent Selection (EAS) agent.

Call Forwarding Off-Net

Users use the Call Forwarding Off-Net capability to forward calls to an off-network destination. However, you can restrict access to the Call Forwarding Off-Net capability to specific users.

If the Coverage of Calls Redirected Off-Net (CCRON) capability is enabled, and the called user has a coverage path, the system monitors a call for call progress tones. If no one answers the call at the off-network destination, or if the destination is busy, the system returns the call to the internal extension. For more information on the Call Coverage feature, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

The system can bring the call back for call-coverage processing if the coverage criteria of the principal are satisfied at the forwarded-to destination.

If the CCRON capability is enabled, but the called user does not have a coverage path, the system does not monitor a call for call progress tones. The system leaves the call at the off-network destination.

When the system redirects an incoming trunk call off the network, the system sets a timer. The timer prevents the system from redirecting the incoming trunk calls off the network until the timer either expires or is canceled. The timer prevents calls that are redirected off the network from being routed back to the original telephone number from the off-network destination. Calls that are routed back to the original telephone number in this situation effectively create a loop that seizes trunks until trunks are no longer available.

Call Forwarding Override

With the Call Forwarding Override capability, you can call, or transfer a call to a user who has the Call Forwarding feature active. Only the user who answers the forwarded call can use the Call Forwarding Override capability to transfer the call back to the called extension. For example, user A designates user B as the destination for forwarded calls. User B answers a call forwarded from the extension of user A, and uses the Call Forwarding Override capability to transfer the call back to user A.

If you enable the Call Forwarding Override capability on your system, the capability is available for all users.

Users cannot use the Call Forwarding Override capability to override a call when the system forwards a call from a data user or from a hunt group.

In Communication Manager 4.0 and earlier releases, Call Forward Override did not work if the forwarded-to party was not on the same Communication Manager server as the forwarding party. Starting in Communication Manager 5.0, this is now possible, as long as the call from the forwarded-to party provides the calling number in a format that Communication Manager can match with the forwarded-to number entered by the forwarding party. Trunk groups that can do this include ISDN-PRI, ISDN-BRI, H.323, and SIP.

Example 1: Ivan forwards his calls using UDP to extension 2346. An incoming QSIG call for Ivan arrives with the Calling Number "2346." The call is not forwarded, but rings Ivan's phone.

Example 2: Sylvia in Germany forwards her calls to a public network number in Frankfurt using ARS to 0-069-5354341. (The leading '0' is the ARS FAC, and the second '0' is National CPN Prefix.) An incoming call for Sylvia arrives with the Calling Number "49695354341." The "49" is recognized as the local country code and is skipped. Likewise, the ARS FAC and National CPN Prefix are recognized and skipped in the forwarded-to number. The remaining digits match, so the call is not forwarded, but rings Sylvia's phone.

Example 3: Mike in the U.S. forwards his calls to a private-network number at the Chicago office using AAR to 8-231-8592. (The leading '8' is the AAR FAC.) An incoming call for Mike arrives with the Calling Number "231-8592." The AAR FAC is recognized and skipped in the forwarded-to number. The remaining digits match, so the call is not forwarded, but rings Mike's phone.

Notifying users when their calls are redirected

You can administer a setting to notify users that they have a capability active that might redirect their calls. For example, if call forwarding is active for a user, you can administer a setting to play a special dial tone when the user goes off hook.

Coverage for unanswered forwarded calls

You can specify that unanswered forwarded calls have call coverage treatment. The system sends an unanswered forwarded call to coverage if you:

- Enable coverage for unanswered forwarded calls for your system
- Enable call forwarding capabilities for the user
- Assign a call coverage path for the user

Security

Users who do not have permission to make calls to an off-network destination cannot use the Call Forwarding feature to forward calls to an off-network destination.

Administering Call Forwarding

The following steps are part of the administration process for the Call Forwarding feature:

- Viewing user extensions that have the Call Forwarding capabilities active
- Assigning the Call Forwarding All Calls capability to a user
- Removing the Call Forwarding All Calls capability for a user
- Assigning the Call Forward Busy/Don't Answer capability to a user
- Removing the Call Forward Busy/Don't Answer capability for a user
- Assigning the Call Forwarding Off-Net capability to a user
- Removing the Call Forwarding Off-Net capability for a user
- Enabling the Call Forwarding Override capability for your system
- Disabling the Call Forwarding Override capability for your system

This section describes:

- Any prerequisites for administering the Call Forwarding feature
- The screens that you use to administer the Call Forwarding feature
- Complete administration for the Call Forwarding feature

Prerequisites for administering the Call Forwarding feature

You must complete the following actions before you can administer the Call Forwarding feature:

- Ensure that a class of service (COS) that enables your users to use the Call Forwarding feature exists on your system.

  The Call Forwarding feature requires a COS that allows:

  — Call Fwd-All Calls

  — Call Forwarding Busy/DA

  — Restrict Call Fwd-Off Net

  For information on COS administration, see the Class of Service feature.

- Ensure that Feature Access Codes (FACs) for Call Forwarding and Call Forward Busy/Don't Answer are available on your system, if you want users to use an FAC for either of the capabilities.

  The Call Forwarding feature requires the following FACs.

  — Call Forwarding Activation All

- Call Forwarding Activation Busy/DA

  For more information on FAC administration, see the Feature Access Code feature.

- Enable call coverage for unanswered forwarded calls, if you want the capability on your system.

To enable call coverage for unanswered forwarded calls:

1. Type **change system-parameters coverage-forwarding**. Press **Enter**.

   The system displays the System Parameters Call Coverage/Call Forwarding screen (Figure 123: System Parameters Call Coverage/Call Forwarding screen on page 620).

Figure 123: System Parameters Call Coverage/Call Forwarding screen

```
                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

                          CALL COVERAGE/FORWARDING PARAMETERS

          Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
       Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
                        Coverage - Caller Response Interval (seconds): 4
    Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls: 1

COVERAGE
                                       Keep Held SBA at Coverage Point? y
       External Coverage Treatment for Transferred Incoming Trunk Calls? n
        Immediate Redirection on Receipt of PROGRESS Inband Information? n
                                            Maintain SBA At Principal? y

                                         Station Hunt Before Coverage? n

FORWARDING
                                                Call Forward Override? y
                                              Coverage After Forwarding? y
```

2. Perform one of the following actions:
   - If the **Coverage After Forwarding** field is set to **y**, press **Cancel**.
   - If the **Coverage After Forwarding** field is set to **n**:
     - Type **y** in the field.
     - Press **Enter** to save your change.

Screens for administering Call Forwarding

Screen Name	Purpose	Fields
Class of Service	Enable Call Forwarding capabilities for users.	• **Call Fwd-All Calls** • **Call Forwarding Busy/DA** • **Restrict Call Fwd-Off Net**
Feature Access Code (FAC)	Assign a FAC for the Call Forwarding capabilities.	• **Call Forwarding Activation All** • **Call Forwarding Activation Busy/DA**
Station	Assign a Class of Service (COS) that has the Call Forwarding capabilities enabled.	**COS**
System-Parameters Coverage/ Forwarding	Enable the Call Forwarding Override capability.	• **Call Forward Override** • **Coverage After Forwarding**
System Parameters Customer-Options	Ensure that the system can forward calls to an off-network destination.	**Restrict Call Forward Off Net**

Viewing user extensions that have the Call Forwarding capabilities active

To view all the user extensions that have the Call Forwarding capabilities active:

1. Type **`list call-forwarding`**. Press **Enter**.

   This system lists the extensions, with the forwarded destination, that have an active call forwarding capability.

Note:

If you have a V1, V2, or V3 system, the **`list call-forwarding`** command is unavailable. However, you can use the **`display station`** command to view the call forwarding capabilities that are active for a single user extension.

Assigning the Call Forwarding All Calls capability to a user

To assign the Call Forwarding All Calls capability to a user:

1. Type **change station *n***, where ***n*** is the telephone extension number of the user. Press **Enter**.

   The system displays the Station screen (Figure 124: Station screen on page 622).

Figure 124: Station screen

```
                              STATION

Extension: 2054                              Lock Messages? n       BCC: 0
     Type: 7406D                             Security Code: 4196__   TN: 1
     Port: _____                           Coverage Path 1: t1_     COR: 1
     Name: ____________________________    Coverage Path 2: ___     COS: 1
                                           Hunt-to-Station: _______

STATION OPTIONS
             Data Module? n                Personalized Ringing Pattern: 1
          Display Module? n                     Message Lamp Ext: ________


                                             MM Complex Data Ext: ________
```

2. In the **COS** field, type the number of a COS that has the Call Forwarding All Calls capability enabled.
3. Press **Enter** to save your change.

Removing the Call Forwarding All Calls capability for a user

To remove the Call Forwarding All Calls capability from a user:

1. Type **change station *n***, where ***n*** is the user extension. Press **Enter**.

   The system displays the Station screen (Figure 124: Station screen on page 622).
2. In the **COS** field, type the number of a COS that does not have the Call Forwarding All Calls capability enabled.
3. Press **Enter** to save your change.

Assigning the Call Forward Busy/Don't Answer capability to a user

Prerequisites

You must complete the following actions before you can assign a COS that has the Call Forward Busy/Don't Answer capability enabled:

- Assign the Call Forward Busy/Don't Answer ring interval for calls that the system forwards to an internal extension.

To assign the Call Forward Busy/Don't Answer ring interval for calls that the system forwards to an internal extension.

1. Type **`change system-parameters coverage-forwarding`**. Press **Enter**.

   The system displays the System Parameters Call Coverage/Call Forwarding screen (Figure 125: System Parameters Call Coverage/Call Forwarding screen on page 623).

Figure 125: System Parameters Call Coverage/Call Forwarding screen

```
                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

                          CALL COVERAGE/FORWARDING PARAMETERS

          Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
        Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
                           Coverage - Caller Response Interval (seconds): 4
     Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls: 1

COVERAGE
                                       Keep Held SBA at Coverage Point? y
       External Coverage Treatment for Transferred Incoming Trunk Calls? n
        Immediate Redirection on Receipt of PROGRESS Inband Information? n
                                            Maintain SBA At Principal? y
             QSIG VALU Coverage Overrides QSIG Diversion with Rerouting? n
                                         Station Hunt Before Coverage? y

FORWARDING
                                                Call Forward Override? y
                                              Coverage After Forwarding? y
```

2. In the **Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings)** field, type the number of times that a telephone rings before the system forwards the call. The system uses this interval when the Call Forward Busy/Don't Answer capability is active for a user.
3. Press **Enter** to save your change.

To assign the Call Forward Busy/Don't Answer capability to a user:

1. Type **change station *n***, where ***n*** is the user telephone extension number. Press **Enter**.

   The system displays the Station screen (Figure 124: Station screen on page 622).
2. In the **COS** field, type the number of a COS that has the Call Forward Busy/Don't Answer capability enabled.
3. Press **Enter** to save your change.

Removing the Call Forward Busy/Don't Answer capability for a user

To remove the Call Forward Busy/Don't Answer capability for a user:

1. Type **change station *n***, where ***n*** is the user extension. Press **Enter**.

   The system displays the Station screen (Figure 124: Station screen on page 622).
2. In the **COS** field, type the number of a COS that does not have the Call Forward Busy/Don't Answer capability enabled.
3. Press **Enter** to save your change.

Assigning the Call Forwarding Off-Net capability to a user

Prerequisites

You must complete the following actions before you can assign a COS that has the Call Forwarding Off-Net capability enabled:

- Ensure that the Call Forwarding Off-Net capability is enabled on Optional Features screen.
- Ensure that the Call Forwarding Off-Net capability is enabled on the System-Parameters Call Coverage/Call Forwarding screen.
- Assign a ring interval for the Call Forward Busy/Don't Answer capability for calls that the system forwards to an off-network destination.

To ensure that the Call Forwarding Off-Net capability is enabled on the Optional Features screen:

- On the Optional Features screen, verify that the **Restrict Call Forward Off Net** field is set to **y.** To view the screen, type **`display system-parameters customer-options`**. Press **Enter**. If the **Restrict Call Forward Off Net** field is set to **n**, your system is not enabled for the Call Forwarding Off-Net capability. Contact your Avaya representative for before you continue with this procedure.

  For a complete description of the System Parameters Customer-Options screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509 for more information.

To ensure that Call Forwarding Off-Net capability is enabled on the System-Parameters Call Coverage/Call Forwarding screen:

1. Type **`change system-parameters coverage-forwarding`**. Press **Enter**.

   The system displays the System Parameters Call Coverage/Call Forwarding screens (Figure 126: System Parameters Call Coverage/Call Forwarding screen on page 625).

Figure 126: System Parameters Call Coverage/Call Forwarding screen

```
                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

                    COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)

                       Coverage Of Calls Redirected Off-Net Enabled? y
Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point? y
                                  Ignore Network Answer Supervision? n
                  Disable call classifier for CCRON over ISDN trunks? n
                   Disable call classifier for CCRON over SIP trunks? n
```

2. Click **next** until you see the **Coverage Of Calls Redirected Off-Net Enabled** field.
   - If the **Coverage Of Calls Redirected Off-Net Enabled** field is set to **y**, Press **Cancel**.
   - If the **Coverage Of Calls Redirected Off-Net Enabled** field is set to **n**:
     - Type **y** in the field.
     - Press **Enter** to save your change.

To Assign a ring interval for the Call Forward Busy/Don't Answer capability:

1. Type **`change system-parameters coverage-forwarding`**. Press **Enter**.

   The system displays the System Parameters Call Coverage/Call Forwarding screen (Figure 127: System Parameters Call Coverage/Call Forwarding screen on page 626).

Figure 127: System Parameters Call Coverage/Call Forwarding screen

```
                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

CALL COVERAGE/FORWARDING PARAMETERS

          Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
        Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
                        Coverage - Caller Response Interval (seconds): 4
     Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls: 1

COVERAGE
                                       Keep Held SBA at Coverage Point? y
       External Coverage Treatment for Transferred Incoming Trunk Calls? n
        Immediate Redirection on Receipt of PROGRESS Inband Information? n
                                            Maintain SBA At Principal? y
             QSIG VALU Coverage Overrides QSIG Diversion with Rerouting? n
                                          Station Hunt Before Coverage? y

FORWARDING
                                              Call Forward Override? y
                                            Coverage After Forwarding? y
```

2. In the **Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings)** field, type the number of times that a telephone rings before the system forwards the call. The system uses this interval when the Call Forward Busy/Don't Answer capability is active for a user, and the forwarded-to number is an off-network destination.
3. Press **Enter** to save your change.

To assign the Call Forwarding Off Net capability to a user:

1. Type **change station *n***, where ***n*** is the user telephone extension number. Press **Enter**.

   The system displays the Station screen (Figure 124: Station screen on page 622).
2. In the **COS** field, type the number of a COS that has the Call Forwarding Off-Net capability enabled.
3. Press **Enter** to save your change.

Removing the Call Forwarding Off-Net capability for a user

To remove the Call Forwarding Off Net capability for a user:

1. Type **change station *n***, where ***n*** is the user extension. Press **Enter**.

   The system displays the Station screen (Figure 124: Station screen on page 622).
2. In the **COS** field, type the number of a COS that does not have the Call Forwarding Off-Net capability enabled.

3. Press **Enter** to save your change.

Enabling the Call Forwarding Override capability for your system

To enable the Call Forwarding Override capability for your system:

1. Type **change system-parameters coverage-forwarding**. Press **Enter**.

   The system displays the System Parameters Call Coverage/Call Forwarding screen (Figure 128: System Parameters Call Coverage/Call Forwarding screen on page 627).

Figure 128: System Parameters Call Coverage/Call Forwarding screen

```
                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

                           CALL COVERAGE/FORWARDING PARAMETERS

          Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
        Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
                          Coverage - Caller Response Interval (seconds): 4
     Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls: 1

COVERAGE
                                        Keep Held SBA at Coverage Point? y
       External Coverage Treatment for Transferred Incoming Trunk Calls? n
        Immediate Redirection on Receipt of PROGRESS Inband Information? n
                                               Maintain SBA At Principal? y

                                           Station Hunt Before Coverage? n

FORWARDING
                                                   Call Forward Override? y
                                               Coverage After Forwarding? y
```

2. If the **Call Forward Override** field is set to **y**, press **Cancel**.
3. If the **Call Forward Override** field is set to **n**:
   - Type **y** in the field.
   - Press **Enter** to save your change.

Disabling the Call Forwarding Override capability for your system

To disable the Call Forwarding Override capability for your system:

1. Type **`change system-parameters coverage-forwarding`**. Press **Enter**.

   The system displays the System Parameters Call Coverage/Call Forwarding screen (Figure 128: System Parameters Call Coverage/Call Forwarding screen on page 627).
2. If the **Call Forward Override** field is set to **n**, press **Cancel**.
3. If the **Call Forward Override** field is set to **y**:
   - Type **n** in the field.
   - Press **Enter** to save your change.

End-user procedures for Call Forwarding

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Call Forwarding:

- Changing the Call Forwarding All Calls destination from an internal telephone
- Changing the Call Forward Busy/Don't Answer destination from an internal telephone
- Changing the forwarding destination when a user is at an off-network location
- Changing the Call Forward Busy/Don't Answer destination when a user is at an off-network location

Changing the Call Forwarding All Calls destination from an internal telephone

To change their call forwarding all calls destination:

1. Go off hook.
2. Dial the Feature Access Code (FAC) for Call Forwarding Activation All or press the Call Forwarding Activation All feature button.
3. Listen for a dial tone.
4. Dial the extension number of the destination.
5. Hang up the telephone after you hear the three-beep tone.

Changing the Call Forward Busy/Don’t Answer destination from an internal telephone

To change their call forwarding destination:

1. Go off hook.
2. Dial the FAC for Call Forward Busy/Don’t Answer or press the Call Forwarding/Busy Don’t Answer feature button.
3. Listen for a dial tone.
4. Dial the extension number of the destination.
5. Hang up the telephone after you hear the three-beep tone.

Changing the forwarding destination when a user is at an off-network location

To change their call forwarding destination:

1. Go off hook.
2. Dial the telecommuting extension number.
3. Dial the FAC for Extended Call Forward Activate All feature or press their Call Forwarding Activation All feature button.
4. Listen for a dial tone.
5. Dial the extension number and press the pound key (#) key.
6. Dial the security code and press the pound (#) key.
7. Listen for a dial tone.
8. Dial the extension of the destination.

   Use no more than 18 digits when you enter your off-network call forwarding destination telephone number. You must include the FAC for the Trunk Access Code (TAC) or Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS) among the 18 digits. Do not include the pound key (#) that you use to terminate a forwarded-to number among the 18 digits. For more information on the AAR and ARS features, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
9. Hang up the telephone after you hear the three-beep tone that the system generates to confirm the change

Changing the Call Forward Busy/Don’t Answer destination when a user is at an off-network location

To change the call forwarding destination:

1. Go off hook.
2. Dial the telecommuting extension number.
3. Dial the FAC for Extended Call Forward Activate Busy/Don’t Answer or press the Call Forward Activate Busy/Don’t Answer feature button.
4. Listen for a dial tone.
5. Dial the extension number and press the pound key (#).
6. Dials the security code and press the pound key (#).
7. Listen for a dial tone.
8. Dial the extension of the destination

   Use no more than 18 digits when you enter your off-network call forwarding destination telephone number. You must include the FAC for the Trunk Access Code (TAC) or Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS) among the 18 digits. Do not include the pound key (#) that you use to terminate a forwarded-to number among the 18 digits. For more information on the AAR and ARS features, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
9. Hang up the telephone after they hear the three-beep tone that the system generates to confirm the change

Call Log Enhancements

Log Forwarded Calls

The Log Forwarded Calls operation creates missed call log entry for calls that are redirected by a forwarding feature.

Missed call log entry for a redirected call shows the forwarding icon instead of the missed call icon in the display. So the user knows that the missed call is redirected and might have been answered already by another user.

The Log Forwarded Calls option applies to the following redirecting features:

- Call-Forward

- Enhanced Call Forward
- Coverage
- Goto-Cover
- Send-all-calls

Note:
The Log Forwarded Calls feature is available with Communication Manager Release 5.2, firmware version 3.0 and higher. It is available for 96xx H.323 IP series telephone only.

Administration of the Log Forwarded Calls option is only possible through the **LOGUNSEEN** parameter in the phone firmware settings file. With the setting of this parameter the logging of forwarded calls can be switched on and off.

Users wanting to have all calls logged and those not wanting to have the forwarded calls logged, the settings file of the firmware provides a new parameter for Log Forwarded Calls. The default setting is **No Logging Of Forwarded Calls**, because this is close to the current call log handling. The setting for logging of forwarded calls is only handled in the telephone and not in Communication Manager switching software.

Table 73 shows the logging of forwarded calls with the log forwarded calls active or not active settings parameter on the telephone. The busy/do not answer details are listed separately, even though this is one feature.

Table 73: Logging of forwarded calls

Feature	Call Forward Log	Call Log on forwarding user log fwd calls not active	Call Log on forwarding user log fwd calls active
Call-forward all	Yes	No	Missed
Enh-cfwd all	Yes	No	Missed
Send-all-calls	Yes	No	Missed
Goto-cover	Yes	No	Missed
Coverage all	No	No	No
Call-forward busy	Yes	No	Missed
Enh-cfwd busy	Yes	No	Missed
Coverage busy	No	No	Missed
Coverage DND	Yes	No	Missed
Call-forward no-ans	Yes	No	Missed
Enh-cfwd no-ans	Yes	No	Missed

Feature	Call Forward Log	Call Log on forwarding user log fwd calls not active	Call Log on forwarding user log fwd calls active
Coverage no-ans	No	No	Missed
Coverage active	No	No	Missed

Important:
Users cannot activate or deactivate the Coverage All feature. It is set and activated only by an administrator and will never create call log entries. So calls that are going to coverage all are not handled as forwarded calls in the call log.

Considerations

This section provides information about how the Call Forwarding feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Forwarding under all conditions.

- Call classifiers and tone plans for off-network calls

  If you send calls off the network and use the Call Classifier-Detector or the Tone-Clock (with Call Classifier-Tone Detector) circuit pack (the international version) for call classification and do not use the American tone plan, use the System-Parameters Country-Options screen to define specific country tones.

  If you use the Call Classifier-Detector or the Tone-Clock (with Call Classifier-Tone Detector) circuit pack (the international version) and do not use the System-Parameters Country-Options screen, your system downloads the American tone plan regardless of your geographical location.

- Save translation command

  If you use the **`save translation`** command, the software saves the user call forwarding information, including destination information, to tape.

Interactions

- Answer Detection

  The Answer Detection feature shares call-classifier resources with the Coverage of Calls Redirected Off-Net (CCRON) capability.

- Attendant Override of Diversion

  If an attendant uses the Call Forwarding Override to call a user who has the Call Forwarding feature active, the system sends the call to the user telephone. The system does not forward the call to the forwarded-to destination.

- Automatic Callback and Ringback Queuing

  A user cannot activate Automatic Callback if the Call Forwarding feature is active at the called extension. If the user activates Automatic Callback before the Call Forwarding feature is active at the called extension, the system redirects the callback call attempt to the forwarded destination.

- Bridging

  The system does not terminate calls to a bridged call appearance when the Call Forward Busy/Don't Answer capability is active at the user extension.

  Users cannot bridge onto an off-network call during the time the system is classifying the call.

- Call Coverage

  If the principal's (forwarding extension) redirection criteria are met at the designated (forwarded-to) destination, the forwarded call redirects to the principal's coverage path; the designated destination gets a temporary bridged appearance (except when it is off net), which remains active after the call is answered so that the designated extension can bridge onto the call if desired. The temporary bridge appearance remains until the caller hangs up.

  For calls redirected to QSIG networks, if coverage after forwarding is not enabled, the QSIG redirection takes precedence over the CCRON capability. However, if coverage after forwarding is enabled, CCRON takes precedence, enabling the call to be tracked back to the network to follow the coverage path.

  When the Cover All Calls capability is active, and either the Call Forwarding All Calls capability or the Call Forwarding Off-Net capabilities is active, the system:

  - Forwards incoming priority call
  - Redirects all nonpriority calls according to the user coverage path
  - Does not redirect non-priority calls off of the network

- Call Detail Recording (CDR)

  When the system forwards a call off the network:

- The CDR records the forwarded-from number.
- The system generates a CDR record only after the call is answered at the off-network destination.

If the forced entry of account codes is required, the system does not forward calls to an off-network destination.

- Call Park

  When a user activates Call Forwarding, and then activates Call Park, the system parks the call at the user extension. The system does not forward the call.

  When the system forwards a call, and the forwarded-to extension user parks the call, the system usually parks the call at the forwarded-to extension. The system does not usually park the call at the called extension.

- Call Pickup/Directed Call Pickup

  If you enable a Temporary Bridged Appearance for the Call Pickup capability, the system maintains a temporary bridged appearance when the forwarded-from user and the forwarded-to user are members of the same call pickup group.

- Call Prompting

  The Call Prompting feature shares call-classifier resources with the Coverage of Calls Redirected Off-Net capability.

- Call Visor Adjunct Switch Application Interface (ASAI)

  The Call Visor ASAI feature shares call-classifier resources with the Coverage of Calls Redirected Off-Net (CCRON) capability.

- Conference

  Users cannot use the Conference feature to add another user to an off-network call while the system classifies the call.

  The system does not classify a call when the system routes a call to an off-network destination if any of the conference participants is on hold while the conference is initiated. The system does not classify the call even if the Coverage of Calls Redirected Off Net capability is active.

- Expert Agent Selection (EAS)

  Agents who are logged in at an extension, and who have EAS enabled, cannot activate or deactivate Call Forwarding. If the agent logs out of the extension, the agent can activate or deactivate Call Forwarding for the extension. If the agent logs out of the extension and the agent activates Call Forwarding for the extension, the system forwards calls that are made to the extension.

- Hold

  The system does not classify a call when the system routes a forwarded call to an off-network destination if any party on the call is on hold. The system does not classify the call even if the Coverage of Calls Redirected Off Net capability is active.

- Intercom-Automatic

  When a user presses an Intercom-Automatic button, and Call Forwarding is active at the user extension that is associated with that button, the system forwards the Intercom-Automatic feature along with the call. However, if the system forwards the call to an off-network destination, the system does not also forward the Intercom-Automatic feature.

- Interflow

  The system uses the Call Forwarding All Calls capability and the Interflow feature to redirect Automatic Call Distribution (ACD) calls to an ACD split on another system.

- Intraflow

  The system uses the Call Forwarding feature to route ACD calls from a split to another destination on the same switch.

- Leave Word Calling (LWC)

  LWC cannot be activated toward a telephone that has Call Forwarding activated. If LWC was activated before the user of the called phone activated Call Forwarding, the callback call attempt is redirected to the forwarded-to party.

- Multifrequency Compelled (MFC) Signaling

  MFC Signaling shares call classification resources with the Coverage of Calls Redirected Off-Net capability.

- Personal Central Office Line (PCOL)

  The system does not forward PCOL calls.

- QSIG

  If a call is forwarded over an ISDN-PRI trunk that is administered with supplementary service protocol "b" (QSIG), then additional call information might be displayed.

- Send All Calls

  If both Send All Calls and Call Forwarding All Calls are active at an extension, the system:

  — Redirects calls to coverage immediately, if the system can do so

  — Forwards other calls, such as Priority Calls

  If a user has both Send All Calls and Call Forwarding All Calls activate, calls to that extension that can immediately be redirected to coverage are redirected. However, other calls, such as Priority Calls, are forwarded to the designated extension.

  Activation of Send All Calls at the forwarded-to extension does not affect calls that are forwarded to that extension.

- Temporary Bridged Appearance

  The system maintains a temporary bridged appearance for calls that are ringing on the network. If the caller hangs up, or someone answers the call, the system drops the temporary bridged appearance.

  The system does not maintain a temporary bridged appearance when the system forwards calls to an off-network destination.

- Traffic Reports Removed

  Use the list measurement tone-receiver traffic report to obtain information on port usage for the Traffic Reports Removed feature.

- Transfer

  Users cannot transfer a call that the system routes to an off-network destination while the system classifies the call.

Call Park

Use the Call Park feature to retrieve a call that is on hold, from any other telephone within the system. For example, a user can answer a call at one extension, put the call on hold, and then retrieve the call at another extension. Or the user can answer a call at any telephone after an attendant or another user pages the user.

Detailed description of Call Park

This section provides a detailed description of the Call Park feature.

You can set a system-wide expiration interval for parked calls. If no one answers the call before the interval expires, the system redirects the call.

The system redirects a parked call to the attendant if the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screens is set to **n**. The system redirects a parked call to the user who parked the call if the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screens is set to **y**.

If you do not administer an attendant or a night service extension, and if you did not administer the Night Service-Trunk Answer from Any Station capability, the system ignores the expiration interval, and the call remains parked.

If two parties are connected on a parked call, a third party can create a three-way conference, if the third party answers the call before the interval expires.

The attendant console group can have common shared extensions that the attendant console group uses exclusively for the Call Park feature. The system does not assign the common shared extensions to a telephone. The system stores the common shared extensions in the system translations, and parks calls at the extensions.

The common shared extensions are particularly useful when an attendant pages a user at the request of another user. The attendant parks the calling user on a common shared extension, and announces the extension. The status lamp that is associated with the extension indicates "call parked" or "no call parked," instead of an active status or an or idle status.

Administering Call Park

The following steps are part of the administration process for the Call Park feature:

- Assigning a call park button to a multiple-call appearance telephone

This section describes:

- Any prerequisites for administering the Call Park feature
- The screens that you use to administer the Call Park feature
- Complete administration procedures for the Call Park feature

Prerequisites for administering the Call Park feature

You must complete the following actions before you can administer the Call Park feature:

- Ensure that Feature Access Codes (FACs) for Call Park are available on your system.
- Administer the Feature-Related System Parameters screens to specify:
  - The minutes that the system leaves a call parked at any extension on your system.
  - That the system routes calls that exceed the call park timeout limit back to the originator of the call.
- Define the common shared extensions on your system.

To ensure that a FAC for Call Park is available on your system:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen (Figure 129: Feature Access Code screen on page 639).

Figure 129: Feature Access Code screen

```
change feature-access-codes                                    Page   1 of   8
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *00
         Abbreviated Dialing List2 Access Code: *01
         Abbreviated Dialing List3 Access Code: *02
Abbreviated Dial - Prgm Group List Access Code: *03
                      Announcement Access Code: *04
                       Answer Back Access Code: *05

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: *9    Access Code 2: 9
                Automatic Callback Activation: *06    Deactivation: #06
Call Forwarding Activation Busy/DA: *07    All: *08    Deactivation: #09
                         Call Park Access Code: *10
                       Call Pickup Access Code: *11
CAS Remote Hold/Answer Hold-Unhold Access Code: *50
                  CDR Account Code Access Code: *12
                        Change COR Access Code:
                   Change Coverage Access Code: *13
                   Contact Closure   Open Code:          Close Code:
                   Contact Closure  Pulse Code:
```

2. Perform one of the following actions:
   - If the **Answer Back Access Code** field and the **Call Park Access Code** field each contain an FAC, your system already has the FACs that are necessary for the Call Pickup Feature. Press **Cancel**.
   - If either the **Answer Back Access Code** field or the **Call Park Access Code** field do not contain a FAC**,** type a FAC in the field. Press **Enter** to save your changes.

     For more information on the Feature Access Code feature, including how to change or deactivate an FAC, see *Administering Avaya Aura™ Communication Manager,* 03-300509.

To administer the Feature-Related System Parameters screen for the Call Park feature:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen (Figure 130: Feature-Related System Parameters screen on page 640.

Figure 130: Feature-Related System Parameters screen

```
change system-parameters features                              Page 1 of 13
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 3
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
                        DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

2. In the **Call Park Timeout Interval (minutes)** field, type the number of minutes that you want the system to park a call at an extension.
3. Click **Next** until you see the **Deluxe Paging and Call Park Timeout to Originator** field (Figure 131: Feature-Related System Parameters screen on page 641).

Figure 131: Feature-Related System Parameters screen

```
change system-parameters features                              Page   3 of  13
                        FEATURE-RELATED SYSTEM PARAMETERS
                     Reserved Slots for Attendant Priority Queue: 5
                                      Time before Off-hook Alert: 10
                          Emergency Access Redirection Extension:
            Number of Emergency Calls Allowed in Attendant Queue: 5
                                          Call Pickup Alerting? n
                     Temporary Bridged Appearance on Call Pickup? y
                                   Call Pickup on Intercom Calls? y
                                           Directed Call Pickup? n
                                     Extended Group Call Pickup: none
               Deluxe Paging and Call Park Timeout to Originator? n
   Controlled Outward Restriction Intercept Treatment: tone
  Controlled Termination Restriction (Do Not Disturb): tone
            Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS        Authorization Codes Enabled? y
                                       Authorization Code Length: 7
                          Authorization Code Cancellation Symbol: #
                                        Attendant Time Out Flag? n
                                     Display Authorization Code? y
                  Controlled Toll Restriction Replaces: none
```

4. In the **Deluxe Paging and Call Park Timeout to Originator?** field, perform one of the following actions:
   - If you want the system to route a parked call, that exceeds the number of minutes that you specified in the **Call Park Timeout Interval (minutes)** field, to the attendant, type **n**. The system provides **n** as the default entry for this field.
   - If you want the system to route a parked call, that exceeds the number of minutes that you specified in the **Call Park Timeout Interval (minutes)** field, to the originator of the call, type **y**.
5. Press **Enter** to save your changes.

To define the common shared extensions on your system:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 132: Console Parameters screen on page 642).

Figure 132: Console Parameters screen

```
change console-parameters                                    Page 2 of 5
                              CONSOLE PARAMETERS

TIMING
  Time Reminder on Hold (sec): 30          Return Call Timeout (sec): 30
  Time in Queue Warning (sec):

  INCOMING CALL REMINDERS
      No Answer Timeout (sec):                        Alerting (sec):
                               Secondary Alert on Held Reminder Calls? y

ABBREVIATED DIALING
     List1:                   List2:                   List3:
             SAC Notification? n

                           COMMON SHARED EXTENSIONS
            Starting Extension:                 Count:
```

2. Click **next** until you see the **Common Shared Extensions** area.
3. In the **Starting Extension** field, type an extension at which you want the attendant to park a call.
4. In the **Count** field, type the number of extensions that you want the attendants to have available to park calls. The system uses the information in the **Starting Extension** field and the **Count** field to determine which extensions are available for attendants to park a call. For example, if you type **4300** in the **Starting Extension** field and you type **3** in the **Count** field, the system provides the three consecutive extensions 4300, 4301, and 4302 to park calls.
5. Press **Enter** to save your changes.

Screens for administering Call Park

Screen name	Purpose	Fields
Console-Parameters	Specify the extensions where an attendant can park a call.	• **Starting Extension** • **Count**
Feature Access Code (FAC)	Define the system-wide FACs to use to park a call, and to answer a parked call.	• **Answer Back Access Code** • **Call Park Access Code**

Screen name	Purpose	Fields
Feature-Related System Parameters	Specify the number of minutes that the system parks a call on your system.	• **Call Park Timeout Interval**
	Specify that the system return a call that exceeds the timeout to the originator of the call.	• **Deluxe Paging and Call Park Timeout to Originator**
Station	Assign a call park button to a user with a multiple-call appearance telephone.	**Button Assignments**

Assigning a call park button to a multiple-call appearance telephone

To assign a call park button to a user of a multiple-call appearance telephone:

1. Type **`change station n`** where ***n*** is the telephone number of the extension to which you want to assign a call park button. Press **Enter**.

   The system displays the Station screen for the extension that you requested.

2. Click **Next** until you see the **Button Assignments** area (Figure 133: Station screen on page 644).

Figure 133: Station screen

```
change station 20001                                        Page   3 of   4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          5:
 2: call-appr                          6:
 3: call-appr                          7:
 4: call-park                          8:
```

3. Type **call-park** next to the number of the button that you want the user to use to park a call.
4. Press **Enter** to save your changes.

End-user procedures for Call Park

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities.
This section includes the following end-user procedures for Call Park.

Note:
These procedures apply only if you are using the Call Park feature with a Feature Access Code (FAC).

- Using Call Park from a single-line telephone
- Using Call Park from a multiple-call appearance telephone
- Using Call Park from an attendant console
- Retrieving a parked call

Using Call Park from a single-line telephone

To use the Call Park feature from a single-line telephone:

1. Flash the switch hook.
2. Dial the Feature Access Code (FAC) for Call Park.
3. Hang up.

Using Call Park from a multiple-call appearance telephone

To use the Call Park feature from a multiple-call appearance telephone:

1. Press the transfer button or the conference button.
2. Dial the FAC for Call Park.
3. Press the transfer button or the conference button.

Using Call Park from an attendant console

To use the Call Park feature from an attendant console:

1. Press the start button.
2. Dial the FAC for Call Park.
3. Dial the extension where the attendant wants to park the call.
4. Press the release button.

   An attendant can also use the Direct Extension Selection with Busy Lamp Field capability with the Call Park feature. For more information on the Direct Extension Selection with Busy Lamp feature, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Retrieving a parked call

To use the Call Park feature to retrieve a call, perform one of the following actions:

1. Press the same call park button that was used to park the call.
2. Dial the FAC to retrieve parked calls.

Considerations for Call Park

This section provides information about how the Call Park feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Park under all conditions. The following considerations apply to Call Park:

- A User can park only one call at an extension at one time, even if the extension has multiple call appearances. A user can park a conference calls that has two to five participates. A user cannot park a conference call that has six participants. The sixth position must remain open so someone can retrieve the call.
- Neither a user nor an attendant can park a call on a group extension. If a group member parks a call, the system parks the call at the extension of the group member. Group members can belong to the following groups:
  - A coverage answer group
  - A uniform call distribution (UCD) hunt group
  - A direct department calling (DDC) hunt group
  - A terminating extension group (TEG)
- If all appearances on a parked telephone are busy and no attendant or night-service extensions are configured when the call park timeout expires, the system:
  - Drops the call if a coverage path does not exist.
  - Does not drop the call if a coverage path exists.

Interactions for Call Park

This section provides information about how the Call Park feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call Park in any feature configuration.

- Abbreviated Dialing

  A user presses the Abbreviated Dialing button to park calls, or retrieve calls that are parked.

- Attendant Console

  Assign the common shared extensions to the optional Attendant Selector Console in the 00 through 09 block of numbers, on the bottom row, in any hundreds group so that the attendant can easily identify the extensions. The lamp that is associated with the number indicates "call parked" or "no call parked," rather than a busy status or an idle status. For more information on the Attendant features, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

- Automatic Wakeup

  Neither a user nor an attendant can park Automatic Wakeup calls.

- Bridged Call Appearance

  If a user, that is active on a bridged call appearance, activates Call Park, the system parks the call on the primary extension associated with the bridged call appearance.

- Call Vectoring
  - Neither a user nor an attendant can park a call on a vector directory number (VDN) extension.
  - Neither a user nor an attendant can park a call that is undergoing vector processing.

- Code Calling Access

  The system automatically parks a user or an attendant on the extension of the party that is paged when the user or attendant:
  - Is using the Paging feature.
  - Dials the Code Calling Access Feature Access Code (FAC)
  - Dials the extension of the party that is paged

- Conference

  Both users and attendants can park Conference calls.

- Data Privacy and Data Restriction

  The system automatically deactivates the Data Privacy feature and the Data Restriction feature when a user or attendant parks a call.

- Drop

  If a user receives an external call, and the user pushes the **drop** button after the user parks the call, the call is no longer parked.

  If a user receives an internal call, and the user pushes the **drop** button after the user parks the call, the call remains parked. The system drops the call only when the user who parks the call hangs up.

- Loudspeaker Paging Access

  Neither a user nor an attendant can park calls to paging zones.

- Remote Access

  A Remote Access caller cannot park a call. However, the Code Calling Access feature, an answering attendant, or a telephone user can park an incoming Remote Access call.

- Tenant Partitioning

  If an attendant parks a call on a common shared extension, and tenant partitioning is *not* active, the system routes the call to the attendant group when the call exceeds the call park timeout.

  If an attendant parks a call on a shared extension, and tenant partitioning is active, the system routes the call to the attendant who parked the call when the call exceeds the park timeout interval.

  The system functions as described in the preceding circumstances regardless of whether the **Deluxe Paging and Call Park Timeout to Originator** field of the Feature-Related System-Parameters screen is set to **y** or **n**.

- Transfer

  If the **Transfer Upon Hang-up** field on the Feature Related System-Parameter***s*** screen is set to **y**, a user does not need to press the **Transfer** button a second time to park a call.

Call Pickup

Use the Call Pickup feature to allow users to answer calls for one another. The Call Pickup feature requires that users be members of the same pickup group.

- With the related Extended Call Pickup capability, users in one pickup group can answer the telephones for users in another pickup group.
- With the related Directed Call Pickup capability, users can specify what other telephone they want to answer. Pickup groups are not needed with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this capability.

Detailed description of Call Pickup

This section provides a detailed description of the Call Pickup feature.

With Call Pickup, you create one or more pickup groups. A pickup group is a collection, or list, of individual telephone extensions. A pickup group is the way to connect individual extensions together. For example, if you want everyone in the payroll department to be able to answer calls to any other payroll extension, you can create a pickup group that contains all of the payroll extensions.

A user extension can belong to only one pickup group. Also, the maximum number of pickup groups may be limited by your system configuration.

Using their own telephones, all members in a pickup group can answer a call that is ringing at another group member telephone. If more than one telephone is ringing, the system selects the extension that has been ringing the longest.

Throughout this procedure on pickup groups and extended pickup groups (see Extended Call Pickup on page 651), there are examples that make Call Pickup easier to understand.

Call Pickup Alerting

Members of a call pickup group know that another group member is receiving a call in two ways:

- Group members can hear the other telephone ring.
- The Call Pickup button status lamp on the telephones of all the group members flash.

Note:
You must activate Call Pickup Alerting in your system, and assign a Call Pickup button to the telephones of each pickup group member, before the Call Pickup button status lamps work properly.

For information how to set up Call Pickup Alerting, see Enabling Call Pickup Alerting on page 656.

If the **Call Pickup Alerting** field on the Feature-Related System Parameters screen is set to **n**, members of the call pickup group must rely only on ringing to know when another group member receives a call. Pickup group members must be located close enough that they can hear the ringing of the other telephones.

To answer a call, a pickup group member can either press the Call Pickup button on the telephone, or dial the Call Pickup Feature Access Code (FAC). For more information, see Assigning a Call Pickup button to a user telephone on page 657, and Assigning a Call Pickup Feature Access Code on page 658.

The **Call Pickup Alerting** field on the Feature-Related System Parameters screen determines how the Call Pickup button status lamps operate.

- If the **Call Pickup Alerting** field is set to **n**, the Call Pickup Button status lamps on all pickup group member telephones do not flash when a call comes in. When a pickup group member hears the telephone of another group member ring and presses the Call Pickup button to answer the call, the:
  - Call Pickup button status lamp of the answering group member becomes steadily lit for the duration of the call.
  - Telephone of the called group member stops ringing.
- If the **Call Pickup Alerting** field is set to **y**, the Call Pickup Button status lamps on all pickup group member telephones flash when a call comes in. When a pickup group member sees the Call Pickup button status lamp flash and presses the Call Pickup button to answer the call, the:
  - Call Pickup button status lamp of the answering group member goes out for the duration of the call.
  - Call Pickup button status lamp of the called group member goes out.
  - Call Pickup button status lamps of the other pickup group members go out.
  - Telephone of the called group member stops ringing.

If another call comes into the pickup group while a group member is talking on a pickup call, the member on the pickup call cannot answer the incoming call. If the group member who is already on a pickup call attempts to answer the incoming call to another telephone using Call Pickup, the Call Pickup button status lamp "flutters" for a few seconds. The fluttering status lamp indicates denial of service. The call that the member is currently on is not interrupted.

In all scenarios, the call appearance button on the telephone of the called group member:

- Stays steadily lit if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to **y**. (For an example of this field, see Figure 134: Feature-Related System Parameters screen on page 656.) The called group member can join the call in progress by pressing the lit call appearance button. The person who picked up the call can either stay on the call or hang up.
- Goes out if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to **n**. The called group member cannot join the call in progress.

The system uses an algorithm to select what call is answered when multiple calls ring or alert in a call pickup group at the same time. The system searches the extensions of the call pickup group until the system finds an extension with a call that is eligible to be answered with Call Pickup. The system selects this call to be answered. The next time that a group member answers a call with Call Pickup, the system bypasses the extension that was answered most recently, and starts the search at the next extension.

For example, if a group member attempts to use Call Pickup when two calls are ringing at extension A and one call is ringing at extension B, the system selects the calls in the following order:

1. One of the calls to extension A
2. The call to extension B
3. The remaining call to extension A

The system also determines which call that a group member answers when multiple calls ring or alert at the same telephone. The system selects the call with the lowest call appearance, which is usually the call appearance that is nearest to the top of the telephone.

For example, when calls ring or alert at the second and the third call appearances, the system selects the call on the second call appearance for the user to answer.

Call Pickup supports the following capabilities:

- Extended Call Pickup
- Directed Call Pickup

Extended Call Pickup

With Extended Call Pickup, you can define one or more extended pickup groups. An extended pickup group is the way to connect individual pickup groups together.

There are two types of extended pickup groups: simple and flexible. You administer the type of extended pickup groups on a system-wide basis. You cannot have both simple and flexible extended pickup groups on your system at the same time.

Based on the type of extended pickup group that you administer, members in one pickup group can answer calls to another pickup group.

For more information, see Setting up simple extended pickup groups on page 662, Setting up flexible extended pickup groups on page 666, and Changing extended pickup groups on page 670.

Directed Call Pickup

With Directed Call Pickup, users specify what ringing telephone they want to answer. A pickup group is not required with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this feature.

For more information, see Setting up Directed Call Pickup on page 671.

Enhanced Call Pickup Alerting

In Communication Manager Release 5.2, Call Pickup Alerting is enhanced to provide display of calling and called party information for all members of the pickup group and administrable alerting options. This feature works on DCP and IP (H.323) telephones but not on IP (SIP) telephones.

When Enhanced Call Pickup is activated, the displays of all members of the pickup group are updated when another group member receives a call. The calling and called party information is provided, enabling a member to decide whether to pick up the call or not. If a button is configured for call pickup, anytime the **call-pkup** button is pressed, details of call to be picked are shown.

The following alerting options are available:

- Intercom ring
- Silent if busy (if the user is busy on another call, the audible alerting is skipped.)
- half-ring
- continuous
- single if busy
- no ring
- single ring

The timing of the display and audible notifications are separately administrable.You must enable Call Pickup Alerting in your system.

For more information, see Enabling Enhanced Call Pickup Alerting on page 657.

Administering Call Pickup

The following steps are part of the administration process for the Call Pickup feature:

- Administering Call Pickup
  - Setting up Call Pickup
  - Enabling Call Pickup Alerting
  - Assigning a Call Pickup button to a user telephone
  - Assigning a Call Pickup Feature Access Code
- Maintaining Call Pickup
  - Removing a user from a pickup group
  - Deleting pickup groups
  - Changing a Call Pickup button on a user telephone
  - Removing a Call Pickup button from a user telephone
- Administering Extended Call Pickup
  - Setting up simple extended pickup groups
  - Setting up flexible extended pickup groups
- Maintaining Extended Call Pickup
  - Removing a pickup group from an extended pickup group
  - Changing extended pickup groups
- Administering Directed Call Pickup
  - Setting up Directed Call Pickup
- Maintaining Directed Call Pickup
  - Removing Directed Call Pickup from a user
- Administering Enhanced Call Pickup
  - Enabling Enhanced Call Pickup Alerting

Screens for administering Call Pickup

Screen Name	Purpose	Fields
Class of Restriction	Create a Class of Restriction (COR) for persons to use the Directed Call Pickup capability.	• **Can Be Picked Up By Directed Call Pickup?** • **Can Use Directed Call Pickup?**
Extended Pickup Group	Combine pickup groups into an extended pickup group.	**Pickup Group Number**
Extended Pickup Groups	View how many extended pickup groups you have on your system.	All
Feature Access Code (FAC)	Assign pickup codes.	• **Call Pickup Access Code** • **Directed Call Pickup Access Code** • **Extended Group Call Pickup Access Code**
Feature-Related System Parameters	Allow the called pickup group member to join the call in progress that another group member has picked up.	**Temporary Bridged Appearance on Call Pickup**
	Enable Call Pickup Alerting	**Call Pickup Alerting**
	Enable the Directed Call Pickup capability.	**Directed Call Pickup**
	Enable the Extended Group Pickup capability.	**Extended Group Call Pickup**
	Enable the Enhanced Call Pickup Alerting capability.	Enhanced Call Pickup Alerting
Pickup Group	Assign a user to a pickup group.	• **Extended Group Number** (only if you set your system for flexible extended pickup groups) • **Group Name** • **Extension**
Station	Assign a Call Pickup button or a Directed Call Pickup button to a user extension.	**Button Assignments** area
	Assign a COR that allows Directed Call Pickup to a user extension.	**COR**

Setting up Call Pickup

The first step in setting up any call pickup system is to create pickup groups and assign users to the groups. You can create one or many pickup groups, depending on your needs. A user extension can belong to only one pickup group.

In this exercise, you will:

- Add a pickup group and assign users to the pickup group.
- Enable Call Pickup alerting.
- Assign a Call Pickup button to each extension in the pickup group.
- Assign a Feature Access Code (FAC).

Adding pickup groups

To add users to a new call pickup group:

1. Type **`add pickup-group next`**. Press **Enter**.

   The system displays the Pickup Group screen. The system also assigns the next available **Group Number** for the new pickup group.

   Note:
   The **Extended Group Number** field is not shown in this example because the system is set for **none** or **simple** extended pickup groups. For more information, see Setting up simple extended pickup groups on page 662. If the **Extended Group Number** field is visible on this screen (see Figure 141: Pickup Group screen on page 668), then your system is set up for **flexible** extended pickup groups. For more information, see Setting up flexible extended pickup groups on page 666.

2. Type a name for this pickup group in the **Group Name** field.
3. Type the extension of each group member.

   Up to 50 extensions can belong to one pickup group.

4. Press **Enter** to save your changes.

   The system automatically completes the **Name** field when you press **Enter**.

Examples: This procedure shows how to set up a new pickup group 11 for Accounting. For the rest of these procedures, let us say that you also set up these pickup groups:

- 12 for Billing
- 13 for Credit Services
- 14 for Delinquency Payments
- 15 for Executives

- 16 for Finance

Enabling Call Pickup Alerting

Call Pickup Alerting allows members of pickup groups to know visually when the telephone of another member is ringing. Use Call Pickup Alerting if the telephones of other pickup group members are too far away to be heard. You must enable Call Pickup Alerting in your system.

To enable Call Pickup Alerting:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Call Pickup Alerting** field (Figure 134: Feature-Related System Parameters screen).

Figure 134: Feature-Related System Parameters screen

```
change system-parameters features                              Page  18 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

IP PARAMETERS

                    Direct IP-IP Audio Connections? y
                              IP Audio Hairpinning? y
                           Synchronization over IP? n

CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                   Call Pickup on Intercom Calls? y     Call Pickup Alerting? n
     Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? n
                       Extended Group Call Pickup: none
                   Enhanced Call Pickup Alerting? y
Enhanced Call Pickup Delay Timer (sec.) Display: 5     Audible Notification: 5


                        Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? n
```

3. Set the **Call Pickup Alerting** field to **y**.
4. Press **Enter** to save your changes.

Enabling Enhanced Call Pickup Alerting

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Enhanced Call Pickup Alerting** field. (Figure 134: Feature-Related System Parameters screen).

3. Set the **Enhanced Call Pickup Alerting** field to **y**.

4. Press **Enter** to save your changes.

Note:

The **Enhanced Call Pickup Delay Timer (sec.) Display** and **Audible Notification** fields are displayed only if **Enhanced Call Pickup Alerting** is set to **y**. To administer the alerting options for a button, you must set the button assignment using the **change station *n*** command.

Assigning a Call Pickup button to a user telephone

After you define one or more pickup groups, assign a Call Pickup button for each extension in each pickup group. Users in a pickup group can press the assigned Call Pickup button to answer calls to any other extension in their pickup group.

To assign a Call Pickup button for each extension:

1. Type **change station *n***, where ***n*** is an extension in the pickup group. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 135: Station screen on page 658).

Figure 135: Station screen

```
change station 1234                                          Page 3 of 4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:


ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                             7:
 2: call-appr                             8:dir-pkup
 3: call-appr                             9:call-pkup
 4:                                      10:dn-dst
 5:                                      11:goto-cover
 6:                                      12:send-calls Ext:
```

3. Move to the button number that you want to use for Call Pickup. You can use any of the available buttons.
4. Type **call-pkup** after the button number.
5. Press **Enter** to save your changes.
6. Repeat this procedure for each member of each pickup group.
7. Notify each user what button to use for Call Pickup.

Assigning a Call Pickup Feature Access Code

After you define one or more pickup groups, assign and give each member the Call Pickup Feature Access Code (FAC). Instead of using the Call Pickup button, users in a pickup group can dial the assigned FAC to answer calls to any other extension in their pickup group.

To create a pickup group Feature Access Code (FAC):

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 136: Feature Access Code screen on page 659).

Figure 136: Feature Access Code screen

```
change feature-access-codes                                          Page 1 of 8
                            FEATURE ACCESS CODE (FAC)

         Abbreviated Dialing List1 Access Code: *00
         Abbreviated Dialing List2 Access Code: *01
         Abbreviated Dialing List3 Access Code: *02
Abbreviated Dial - Prgm Group List Access Code: *03
                      Announcement Access Code: *04
                       Answer Back Access Code: *05

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: *9    Access Code 2: 9
                Automatic Callback Activation: *06    Deactivation: #06
Call Forwarding Activation Busy/DA: *07    All: *08    Deactivation: #09
                        Call Park Access Code: *10
                      Call Pickup Access Code: *11
CAS Remote Hold/Answer Hold-Unhold Access Code: *50
                  CDR Account Code Access Code: *12
                        Change COR Access Code:
                   Change Coverage Access Code: *13
                   Contact Closure   Open Code:          Close Code:
                   Contact Closure  Pulse Code:
```

2. In the **Call Pickup Access Code** field, type the desired FAC.

   Make sure that the FAC complies with your dial plan.
3. Press **Enter** to save your changes.
4. Communicate the FAC with each member of each pickup group.

Removing a user from a pickup group

To remove a user from a pickup group:

1. Type **change pickup-group** ***n***, where ***n*** is the number of the pickup group. Press **Enter**.

   The system displays the Pickup Group screen.
2. Move to the extension that you want to remove.
3. Press **Clear** or **Delete**, depending on your system.
4. Press **Enter** to save your changes.

Deleting pickup groups

Before deleting a pickup group, you must verify if the pickup group is a member of any simple or flexible extended pickup group. If so, you must first delete the pickup group from all extended pickup groups. For more information on extended pickup groups, see Setting up simple extended pickup groups on page 662, and Setting up flexible extended pickup groups on page 666.

Follow these three steps to delete a pickup group:

- Get a list of all extended pickup groups.
- Verify and delete the pickup group from all extended pickup groups.
- Delete the pickup group.

Getting a list of extended pickup groups

To get a list of all extended pickup groups:

1. Type **`list extended-pickup-group`**. Press **Enter**.

   The system displays the Extended Pickup Groups screen (Figure 137: Extended Pickup Groups screen on page 660).

Figure 137: Extended Pickup Groups screen

```
                    EXTENDED PICKUP GROUPS

                     Group            Number of
                     Number           Members

                     1                3
                     2                2
                     3                4
                     4                3
```

2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
3. Press **Cancel**.

Removing a pickup group from an extended pickup group

You must remove the pickup group from all extended pickup groups.

- If your system is set up for **simple** extended pickup groups, the pickup group can be a member of only one extended pickup group.

- If your system is set up for **flexible** extended pickup groups, the pickup group can be a member of many extended pickup groups.
- If your system is set up for no extended pickup groups (**none**) or has no extended pickup groups assigned, you can skip this section and see Deleting the pickup group.

To remove a pickup group from an extended pickup group:

1. Type **change extended-pickup-group** *n*, where *n* is the extended pickup group that you want to check. Press **Enter**.

   The system displays the Extended Pickup Group screen (see Extended Pickup Group screen on page 665).

2. Perform one of the following actions:
   - If the pickup group that you want to delete is *not* a member of this extended pickup group, press **Cancel**.
   - If the pickup group that you want to delete is a member of this extended pickup group:
     - Select the pickup group.
     - Press **Clear** or **Delete**, depending on your system.
     - Press **Enter** to save your changes.
3. Repeat this procedure for each extended pickup group.

Deleting the pickup group

To delete the pickup group:

1. Type **remove pickup-group** *n*, where *n* is the number of the pickup group that you want to delete. Press **Enter**.

   The system displays the Pickup Group screen.

2. Press **Enter**. The system deletes the pickup group.

Changing a Call Pickup button on a user telephone

To change a call pickup button on a user telephone:

1. Type **change station** *n*, where *n* is the extension that you want to change. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (see Station screen on page 658).
3. Move to the existing **call-pkup** button.
4. Press **Clear** or **Delete**, depending on your system.
5. Move to the button number that you want to use for call pickup.

6. Type **call-pkup** after the button number.
7. Press **Enter** to save your changes.

Removing a Call Pickup button from a user telephone

To remove a call pickup button from a user telephone:

1. Type **`change station n`**, where ***n*** is the extension that you want to change. Press **Enter**.

   The system displays the Station screen.
2. Click **Next** until you see the **Button Assignments** area (see Station screen on page 658).
3. Move to the existing **call-pkup** button.
4. Press **Clear** or **Delete**, depending on your system.
5. Press **Enter** to save your changes.

Setting up simple extended pickup groups

What if you want to have members in one pickup group be able to answer calls for another pickup group? In our example, what if you want members in the Credit Services pickup group 13 to answer calls in the Delinquency Payments pickup group 14? You can do that by setting up extended pickup groups.

If you want members of pickup group 13 to answer calls for pickup group 14, *and* if you want members of pickup group 14 to answer calls for pickup group 13, set your system for simple extended pickup groups.

Simple extended pickup groups allow members of two or more individual pickup groups to answer each others calls. In a simple extended pickup group, an individual pickup group can be assigned to only one extended pickup group.

All members of one pickup group can answer the calls to the other pickup groups within the simple extended pickup group.

CAUTION:
Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for simple extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add pickup groups, if needed

- Assign two pickup groups to an extended pickup group.

Creating simple extended pickup groups

To create system-wide simple extended pickup groups:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Extended Group Call Pickup** field (Figure 138: Feature-Related System Parameters screen on page 663).

Figure 138: Feature-Related System Parameters screen

```
                    FEATURE-RELATED SYSTEM PARAMETERS

                  Reserved Slots for Attendant Priority Queue: 5
                                  Time before Off-hook Alert: 10
                       Emergency Access Redirection Extension:
          Number of Emergency Calls Allowed in Attendant Queue: 5
                                       Call Pickup Alerting? n
                  Temporary Bridged Appearance on Call Pickup? y
                                Call Pickup on Intercom Calls? y
                                         Directed Call Pickup? y
                                    Extended Group Call Pickup: simple
             Deluxe Paging and Call Park Timeout to Originator? n
   Controlled Outward Restriction Intercept Treatment: tone
  Controlled Termination Restriction (Do Not Disturb): tone
           Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS        Authorization Codes Enabled? y
                                       Authorization Code Length: 7
                        Authorization Code Cancellation Symbol: #
                                          Attendant Time Out Flag? n
                                    Display Authorization Code? y
                Controlled Toll Restriction Replaces: none
```

3. In the **Extended Group Call Pickup** field, type **simple**.
4. Press **Enter** to save your changes.

   Your system is now set up for simple extended pickup groups.

Creating an extended pickup group Feature Access Code

Users in an extended pickup group must dial an assigned Feature Access Code (FAC), followed by a 1-digit or 2-digit Pickup Numbers, to answer calls to an extension in another pickup group. Pickup groups must be in the same extended pickup group. Users cannot use a call pickup button with Extended Call Pickup.

To create an extended pickup group FAC:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Click **Next** until you see the **Extended Group Call Pickup Access Code** field (Figure 139: Feature Access Code (FAC) screen on page 664).

Figure 139: Feature Access Code (FAC) screen

```
                        FEATURE ACCESS CODE (FAC)

                Data Origination Access Code: *17
                    Data Privacy Access Code: *18
            Directed Call Pickup Access Code: *19
   Emergency Access to Attendant Access Code: *20
                  Enhanced EC500 Activation:        Deactivation:
Extended Call Fwd Activate Busy D/A *21  All: *22    Deactivation: #22
      Extended Group Call Pickup Access Code: *39
             Facility Test Calls Access Code: *24
                           Flash Access Code: *25
           Group Control Restrict Activation: *26    Deactivation: #26
                  Hunt Group Busy Activation: *27    Deactivation: #27
                           ISDN Access Code:
              Last Number Dialed Access Code: *29
   Leave Word Calling Message Retrieval Lock: *30
 Leave Word Calling Message Retrieval Unlock: *31
          Leave Word Calling Send A Message: *32
        Leave Word Calling Cancel A Message: *33
            Malicious Call Trace Activation:        Deactivation:
       Meet-me Conference Access Code Change:
```

3. Perform one of the following actions:
   - If the **Extended Group Call Pickup Access Code** field contains a FAC**,** press **Cancel**.
   - If the **Extended Group Call Pickup Access Code** field does not contain a FAC:
     - Type the desired FAC.

       Make sure that the FAC complies with your dial plan.
     - Press **Enter** to save your changes.
4. Communicate the FAC, the list of pickup numbers, and the pickup group to which each pickup number is associated, to each pickup group member who is part of the extended pickup group. For information on pickup numbers, see Pickup Numbers on page 666.

To create individual pickup groups:

1. If you need to create any pickup groups, see Setting up Call Pickup on page 655.

Assigning pickup groups to a simple extended pickup group

To assign pickup groups to a simple extended pickup group:

1. Type **change extended-pickup-group *n***, where ***n*** is a number of the extended pickup group. In this example, type **change extended-pickup-group 4**. Press **Enter**.

   The system displays the Extended Pickup Group screen for extended pickup group 4 (see Figure 140: Extended Pickup Group screen on page 665).

Figure 140: Extended Pickup Group screen

```
change extended-pickup-group 4                                  Page 1 of 1
                              EXTENDED PICKUP GROUP

                            Extended Group Number: 4

Pickup   Pickup Group                          Pickup   Pickup Group
Number     Number                              Number     Number

 0:      13                                    13:      _____
 1:      14                                    14:      _____
 2:      _____                                 15:      _____
 3:      _____                                 16:      _____
 4:      _____                                 17:      _____
 5:      _____                                 18:      _____
 6:      _____                                 19:      _____
 7:      _____                                 20:      _____
 8:      _____                                 21:      _____
 9:      _____                                 22:      _____
10:      _____                                 23:      _____
11:      _____                                 24:      _____
12:      _____
```

2. In the **Pickup Group Number** column, type the numbers of the pickup groups that you want to link together. In this example, add pickup group 13 (Credit Services) and pickup group 14 (Delinquency Payments).
3. Press **Enter** to save your changes.

Example: Pickup groups 13 and 14 are now linked together in extended pickup group 4. In addition to answering calls to their own pickup group:

- All members of pickup group 13 can answer calls to pickup group 14.
- All members of pickup group 14 can answer calls to pickup group 13.

Pickup Numbers

The **Pickup Number** column that is associated with the **Pickup Group Number** is the unique number that users must dial after dialing the **Extended Group Call Pickup Access Code** FAC to answer a call in that pickup group.

For example, let us say that the **Extended Group Call Pickup Access Code** FAC is ***39**. In the above example:

- A user in pickup group 13 must dial ***391** to answer a call to pickup group 14, because pickup group 14 is assigned to **Pickup Number 1**.
- A user in pickup group 14 must dial ***390** to answer a call to pickup group 13, because pickup group 13 is assigned to **Pickup Number 0**.

Note:

To minimize the number of digits that a user has to dial, first assign pickup groups to **Pickup Numbers** 0 to 9.

- By assigning **Pickup Numbers** 0 to 9, all users only needs to dial a single digit (**0** to **9**) after the FAC to answer the call.
- If you assign a number greater than 9 (10 to 24) to *any* pickup group, *all* users must dial two digits (**00** to **24**) after the FAC to answer the call.

Setting up flexible extended pickup groups

If you want members of a pickup group to answer calls for another pickup group, but you *do not* want the other pickup group to answer your calls, set your system for flexible extended pickup groups.

Flexible extended pickup groups still allow members of one or more individual pickup groups to answer calls of another pickup group. However, the reverse scenario is not always true. With flexible extended pickup groups, you can prevent members of one or more pickup groups from answering the calls to another pickup group.

Flexible extended pickup groups allows more control over what pickup groups can answer calls for other pickup groups. Unlike simple extended pickup groups, an individual pickup group can be in multiple flexible extended pickup groups.

The system displays the **Extended Group Number** field on the Pickup Group screen only when you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to **flexible**. When you populate the **Extended Group Number** field on the Pickup Group screen, you are associating, or "pointing," that pickup group to an extended pickup group. By pointing to an extended pickup group, members of the pickup group can answer calls made to any member of that extended pickup group.

A specific pickup group does *not* have to be a member of the extended pickup group that the pickup group points to. To help clarify flexible extended pickup groups, see the Example in this section.

CAUTION:
Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for flexible extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add or change pickup groups, and "point" a pickup group to an extended pickup group.

Creating flexible extended pickup groups

To create system-wide flexible extended pickup groups:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Extended Group Call Pickup** field (see Feature-Related System Parameters screen on page 663).

3. In the **Extended Group Call Pickup** field, type **flexible**.

4. Press **Enter** to save your changes.

   Your system is now set up for flexible extended pickup groups.

To create an extended pickup group FAC, see Creating an extended pickup group Feature Access Code on page 663.

To associate individual pickup groups with an extended pickup group:

1. Type **`change pickup-group n`**, where ***n*** is a pickup group number. In this example, let us change pickup group 15 (Executives). Type **`change pickup-group 15`**. Press **Enter**.

   The system displays the Pickup Group screen (Figure 141: Pickup Group screen on page 668). Notice that the system displays the **Extended Group Number** field on the Pickup Group screen. This field appears because you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to **flexible**.

Figure 141: Pickup Group screen

```
change pickup-group 15                                          Page 1 of 4
                                   PICKUP GROUP

           Group Number: 15
             Group Name: Executives
GROUP MEMBER ASSIGNMENTS

    Extension      Name
 1: 5431010        James Martin
 2: 5439711        Susan Crawford-Smith
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
```

Important:
If you change your system from simple to flexible extended pickup groups (see Changing extended pickup groups on page 670), the system automatically populates the **Extended Group Number** field on the Pickup Group screen for each pickup group member. For example, pickup groups 13 and 14 are members of extended pickup group 4. If you change the system from simple to flexible extended pickup groups, the system automatically populates the **Extended Group Number** field to **4** on the Pickup Group screen for these two pickup groups.

You are not required to keep the number that the system automatically populates in the **Extended Group Number** field. You can change the number in the **Extended Group Number** field to another pickup group number. You can also make the field blank.

2. If you want to associate, or "point", the pickup group to an extended pickup group, type the number of the extended pickup group for which this pickup group can answer calls in the **Extended Group Number** field. In this example, manually associate pickup group 15 (Executives) to extended pickup group 4. For this example, let us say that you followed the same procedure for pickup group 16 (Finance).

Note:

You do not have to populate the **Extended Group Number** field. You can leave the **Extended Group Number** field blank. You can just as easily point the pickup group to a different extended pickup group. For example, you can point pickup group 13 (Credit Services) to extended pickup group 2, even though pickup group 13 is not a member of extended pickup group 2.

As you will see in the Example on page 670, this means that members in pickup group 13 can answer calls to any member that is in extended pickup group 2. The reverse is not true, however. Members that are in extended pickup group 2 cannot answer calls to pickup group 13.

3. Press **Enter** to save your changes.

Assigning pickup groups to a flexible extended pickup group

To assign pickup groups to a flexible extended pickup group:

1. Type **`change extended-pickup-group n`**, where ***n*** is the number of the extended pickup group. In this example, type **`change extended-pickup-group 4`**. Press **Enter**.

   The system displays the Extended Pickup Group screen for extended pickup group 4 (see Figure 142: Extended Pickup Group screen on page 669).

Figure 142: Extended Pickup Group screen

```
change extended-pickup-group 4                          Page   1 of  1
                              EXTENDED PICKUP GROUP

                            Extended Group Number: 4

Pickup   Pickup Group                          Pickup   Pickup Group
Number     Number                              Number     Number

 0:      13                                    13:      _____
 1:      14                                    14:      _____
 2:      16                                    15:      _____
 3:      _____                                 16:      _____
 4:      _____                                 17:      _____
 5:      _____                                 18:      _____
 6:      _____                                 19:      _____
 7:      _____                                 20:      _____
 8:      _____                                 21:      _____
 9:      _____                                 22:      _____
10:      _____                                 23:      _____
11:      _____                                 24:      _____
12:      _____
```

2. Add pickup group 16 (Finance) to this extended pickup group. For information how to complete this screen, see Figure 140: Extended Pickup Group screen on page 665.
3. Press **Enter** to save your changes.

Example: Here is how flexible extended pickup groups work.

Notice that pickup groups 13, 14, and 16 are now members of extended pickup group 4. On the Pickup Group screen for pickup groups 13, 14, and 16, you also pointed each pickup group to extended pickup group 4.

Pickup group 15 (Executives) is *not* a member of extended pickup group 4. However, on the Pickup Group screen for group 15 (Figure 141), you pointed pickup group 15 to extended pickup group 4.

In addition to answering calls to their own pickup group:

- Any member of pickup group 13 can answer calls to pickup groups 14 and 16.
- Any member of pickup group 14 can answer calls to pickup groups 13 and 16.
- Any member of pickup group 16 can answer calls to pickup groups 13 and 14.
- Any member of pickup group 15 can answer calls to pickup groups 13, 14, and 16 because pickup group 15 points to extended pickup group 4.
- Any member of pickup groups 13, 14 and 16 *cannot* answer calls to pickup group 15 because pickup group 15 is not a member of extended pickup group 4.

Changing extended pickup groups

You define extended pickup groups on a system-wide basis. The system cannot support both simple and flexible extended pickup groups at the same time. You can, however, change your extended pickup groups from one type to another.

Changing from simple to flexible

If you want to change all extended pickup groups from simple to flexible, you can easily make the change. See Creating flexible extended pickup groups on page 667. The system automatically populates the **Extended Group Number** field on the Pickup Group screen for all pickup groups that are part of an extended pickup group.

Changing from flexible to simple

The process is more complex to change all extended pickup groups from flexible to simple. Before you can change the extended pickup group from flexible to simple, you must first delete all of the individual pickup groups from all of the extended pickup groups. Then you can change the extended pickup group from flexible to simple (see Creating simple extended pickup groups on page 663). After that step, you must re-administer all of the extended pickup groups again.

Setting up Directed Call Pickup

If you do not want to set up pickup groups and extended pickup groups, but still want selected people to answer other telephones, use Directed Call Pickup. Before a person can use this feature, you must enable Directed Call Pickup on your system.

- Telephones that can be answered by another extension using Directed Call Pickup must have a Class of Restriction (COR) that allows this feature.
- Telephones that can answer another extension using Directed Call Pickup must have a COR that allows this feature.

In this exercise, you will:

- Determine if Directed Call Pickup is enabled on your system.
- Create one or more Classes of Restriction (COR) that allow Directed Call Pickup.
- Assign the COR to individual extensions.
- Assign a Directed Call Pickup button to each extension that is assigned the COR.
- Assign a Feature Access Code (FAC).

Prerequisites

Before you can assign Directed Call Pickup to a user, you must ensure that Directed Call Pickup is available on your system.

To ensure that Directed Call Pickup is available on your system:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Directed Call Pickup?** field (Figure 143: Feature-Related System Parameters screen on page 672).

Figure 143: Feature-Related System Parameters screen

```
                          FEATURE-RELATED SYSTEM PARAMETERS

                     Reserved Slots for Attendant Priority Queue: 5
                                       Time before Off-hook Alert: 10
                           Emergency Access Redirection Extension:
            Number of Emergency Calls Allowed in Attendant Queue: 5
                                          Call Pickup Alerting? n
                     Temporary Bridged Appearance on Call Pickup? y
                                   Call Pickup on Intercom Calls? y
                                          Directed Call Pickup? y
                                      Extended Group Call Pickup: none
               Deluxe Paging and Call Park Timeout to Originator? n
   Controlled Outward Restriction Intercept Treatment: tone
  Controlled Termination Restriction (Do Not Disturb): tone
            Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS        Authorization Codes Enabled? y
                                       Authorization Code Length: 7
                           Authorization Code Cancellation Symbol: #
                                         Attendant Time Out Flag? n
                                      Display Authorization Code? y
                  Controlled Toll Restriction Replaces: none
```

3. Perform one of the following actions:
   - If the **Directed Call Pickup?** field is set to **y**, your system is set up for Directed Call Pickup. Press **Cancel**.
   - If the **Directed Call Pickup?** field is set to **n**:
     - Type **y** in the field.
     - Press **Enter** to save your changes.

Creating Classes of Restriction for Directed Call Pickup

You must create one or more Classes of Restriction (COR) that allow Directed Call Pickup. All users to whom you assign a COR can then use Directed Call Pickup.

There are three ways to set up a COR for Directed Call Pickup. You can create a COR where users can:

- Only have their extensions answered by Directed Call Pickup. Users with this COR cannot pick up other extensions.
- Only pick up other extensions using Directed Call Pickup. Users with this COR cannot have their extensions answered by other users.
- Both have their extensions answered by Directed Call Pickup and pick up other extensions.

To create a COR that allows Directed Call Pickup:

1. Type **change cor *n***, where ***n*** is the COR that you want to change. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 144: Class of Restriction screen on page 673).

Figure 144: Class of Restriction screen

```
change cor 9                                                    Page 1 of 4
                              CLASS OF RESTRICTION

               COR Number: 9
          COR Description: Directed Call Pickup COR

                      FRL: 7                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: all        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? n
         Send ANI for MFE? n             Add/Remove Agent Skills? y
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? y
                         Can Be Picked Up By Directed Call Pickup? y
                                     Can Use Directed Call Pickup? n
                                     Group Controlled Restriction: inactive
```

2. Perform one of the following actions:

   - To create one or more CORs where the extensions can only be picked up by the Directed Call Pickup feature, but not be able to pick up other extensions:
     - Type **y** in the **Can Be Picked Up By Directed Call Pickup?** field.
     - Leave the **Can Use Directed Call Pickup?** field set to **n**.

       Any extension to which you assign this COR can only be picked up by the Directed Call Pickup feature. Figure 144 shows this example.
   - To create one or more CORs where the extensions can only use the Directed Call Pickup feature to pick up other extensions, but not be picked up by other extensions:
     - Leave the **Can Be Picked Up By Directed Call Pickup?** field set to **n**.
     - Type **y** in the **Can Use Directed Call Pickup?** field.

       Any extension to which you assign this COR can only use the Directed Call Pickup feature to pick up other extensions.

- To create one or more CORs where the extensions can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions:
  - Type **y** in the **Can Be Picked Up By Directed Call Pickup?** field.
  - Type **y** in the **Can Use Directed Call Pickup?** field.

    Any extension to which you assign this COR can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions.

3. Press **Enter** to save your changes.

For more information on Class of Restriction (COR), see the "Class of Restriction" feature.

Assigning a Class of Restriction to a user

You must assign a COR to user extensions before anyone can use Directed Call Pickup.

To modify an extension to allow Directed Call Pickup:

1. Type **`change station n`**, where ***n*** is the extension that you want to change. Press **Enter**.

   The system displays the Station screen (Figure 145: Station screen on page 674).

Figure 145: Station screen

```
add station next                                          Page 1 of X
                              STATION

Extension:                    Lock Messages? n                      BCC: 0
     Type:                    Security Code:                         TN: 1
     Port:                  Coverage Path 1:                        COR: 9
     Name:                  Coverage Path 2:                        COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                         Message Lamp Ext: 1014
           Speakerphone: 2-way                   Mute button enabled? y
       Display Language? English
                   Model:                          Expansion Module?

 Survivable GK Node Name:                          Media Complex Ext:
          Survivable COR:                               IP Softphone? y
   Survivable Trunk Dest?                         Remote Office Phone? y
                                                   IP Video Softphone?
                                                             IP Video?
```

2. In the **COR** field, type the appropriate COR that allows the Directed Call Pickup capabilities.

3. Press **Enter** to save your changes.

Assigning a Directed Call Pickup button

Assign a Directed Call Pickup button to all extensions that share a COR where the **Can Use Directed Call Pickup?** field is set to **y**.

To assign a Directed Call Pickup button for each extension in the COR:

1. Type **change station *n***, where ***n*** is an extension to which you have assigned the Directed Call Pickup COR. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (see Figure 135: Station screen on page 658).
3. Move to the button number that you want to use for Directed Call Pickup. You can use any of the available buttons.
4. Type **dir-pkup** after the button number.
5. Press **Enter** to save your changes.
6. Repeat this procedure for each member of the COR who can pick up other extensions using Directed Call Pickup.
7. Notify each user what button to use for Directed Call Pickup.

Assigning a Directed Call Pickup Feature Access Code

Also assign a Directed Call Pickup Feature Access Code (FAC). Give the FAC to each user whose extension shares a COR where the **Can Use Directed Call Pickup?** field is set to **y**.

Instead of using the Directed Call Pickup button, users can dial the assigned FAC to answer calls using Directed Call Pickup.

To create a Directed Call Pickup Feature Access Code (FAC):

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Click **Next** until you see the **Directed Call Pickup Access Code** field (Figure 146: Feature Access Code screen on page 676).

Figure 146: Feature Access Code screen

```
change feature-access-codes                                          Page  2  of 8
                            FEATURE ACCESS CODE (FAC)
                  Data Origination Access Code:
                      Data Privacy Access Code:
              Directed Call Pickup Access Code: 101
    Emergency Access to Attendant Access Code:
                   Enhanced EC500 Activation:        Deactivation:
    Extended Call Fwd Activate Busy D/A_  All:       Deactivation:
       Extended Group Call Pickup Access Code:
              Facility Test Calls Access Code:
                           Flash Access Code:
            Group Control Restrict Activation:       Deactivation:
                  Hunt Group Busy Activation:        Deactivation:
                               ISDN Access Code:
                Last Number Dialed Access Code:
   Leave Word Calling Message Retrieval Lock:
  Leave Word Calling Message Retrieval Unlock:
            Leave Word Calling Send A Message: #66
          Leave Word Calling Cancel A Message: *66
              Malicious Call Trace Activation:       Deactivation:
        Meet-me Conference Access Code Change:
```

3. Perform one of the following actions:
   - If the **Directed Call Pickup Access Code** field already contains a code**,** press **Cancel**.
   - If the **Directed Call Pickup Access Code** field does not contain a code:
     - Type a code in the field. Make sure that the code you type conforms to your dial plan.
     - Press **Enter** to save your change.
4. Communicate the FAC with each member of the COR that can pick up other extensions using Directed Call Pickup.

Removing Directed Call Pickup from a user

To remove Directed Call Pickup from a user:

1. Type **`change station`** ***`n`***, where ***`n`*** is the extension of the user. Press **Enter**.

   The system displays the Station screen (see Station screen on page 674).
2. In the **COR** field, type a different COR that does not have Directed Call Pickup permissions.

3. Click **Next** until you see the **Button Assignments** section (see Station screen on page 658).
4. Move to the button number that contains **dir-pkup**.
5. Click **Clear** or **Delete**, depending on your system.
6. Press **Enter** to save your changes.

End-user procedures for Call Pickup

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Call Pickup:

- Using Call Pickup to answer a call of another user
- Using Extended Group Pickup to answer a call of another user

To use Call Pickup to answer a call of another user:

1. Go off hook.
2. Perform one of the following actions:
   - Press the **call-pkup** Call Pickup button.
   - Dial the Call Pickup FAC.

To use Extended Group Pickup to answer a call of another user:

1. Go off hook.
2. Dial the Extended Group Pickup FAC.
3. Dial the unique Pickup Number of the pickup group in the extended pickup group.

   Each pickup group within an extended pickup group has a unique Pickup Number.

End-user procedures for Directed Call Pickup

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Directed Call Pickup:

Note:
This procedure assumes that the system is set up for Directed Call Pickup, and that the extension of the user and the extension of the recipient have the correct COR to use Directed Call Pickup. This procedure is for those extensions where the **Can Use Directed Call Pickup?** field on the Class of Restriction screen is set to **y**. For more information, see Setting up Directed Call Pickup on page 671.

To use Directed Call Pickup to answer a call of another user:

1. Go off hook.
2. Perform one of the following actions:
   - Press the **dir-pkup** Directed Call Pickup button.
   - Dial the Directed Call Pickup FAC.
3. Wait for dial tone.
4. Dial the extension that you want to pick up.

Considerations for Call Pickup

This section provides information about how the Call Pickup feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Pickup under all conditions.

- Exclusion is not supported for call pickup calls.
- A member of a pickup group who makes a call to another group member cannot use Call Pickup to answer the call.
- You can use the Team Button feature for call pick up. For more information, see the feature description on Team Button.

Interactions for Call Pickup

This section provides information about how the Call Pickup feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call Pickup in any feature configuration.

- Abbreviated Dialing

  A user can use a single Abbreviated Dial button to store either:

  – Both the Feature Access Code (FAC) for Directed Call Pickup and a telephone number

- Only the FAC for Directed Call Pickup

- Attendant

  An attendant can use the Directed Call Pickup capability to answer calls. However, other users cannot use the Directed Call Pickup capability to answer a call that alerts at an attendant console.

- Automatic Callback and Ringback Queuing

  Neither the call pickup group members nor the Directed Call Pickup users can answer a Callback calls

- Bridged Call Appearance

  Calls that are made to a primary telephone, alerting at bridged appearances of the primary telephone, can only be answered by pickup group members of the primary number.

  - If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to **n**, the primary appearance and all bridged appearances of the call are dropped after Call Pickup is used to answer the call.
  - If the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to **y**, the primary and bridged call appearance lamps stay lit after Call Pickup is used to answer the call.
  - If the primary telephone and the bridged telephone are both in the same pickup group, members in the pickup group can answer a call that is made to the primary telephone that is ringing at the bridging user's telephone. This can be done instead of selecting the bridged appearance button.
  - If the primary telephone and the bridged call appearance are not in the same pickup group, members who are in the same pickup group as the bridged call appearance telephone cannot answer a call that is made to the primary telephone.
  - If Call Pickup Alerting is active, and a bridged call appearance rings on the telephone of a member of a call pickup group that is also getting a direct call, other group members cannot answer the direct call.
  - If Call Pickup Alerting is not active, and a bridged call appearance rings at the telephone of a member of a call pickup group that is also getting a direct call, other group members can answer the direct call.
  - You cannot use the Directed Call Pickup capability to answer a call that alerts at a bridged call appearance. You can use Directed Call Pickup to answer the call using the primary extension.

- Call Coverage

  If a user has a call-coverage temporary bridged appearance, the user can use Directed Call Pickup to answer a redirected call that alerts at the telephone of another covering user.

- Call Detail Recording (CDR)

  CDR records the extension number that the caller dials.

- Call Forwarding

  If the Temporary Bridged Appearance capability on the Call Pickup feature is enabled, the system maintains a temporary bridged appearance if the forwarded-to extension belongs to the same call pickup group as the forwarded-from extension. If the Temporary Bridged Appearance capability on the Call Pickup feature is not enabled, the system does not maintain a temporary bridged appearance.

- Call Pickup Alerting

  When a pickup group member uses the Directed Call Pickup capability to answer a ringing call of another group member, and the call is the only call that is ringing for any member of the pickup group, the call pickup alerting lamp goes out.

- Call Waiting

  A user cannot use the Call Pickup capability to answer a Call Waiting call.

- Class of Restriction (COR)

  The Call Pickup and Directed Call Pickup features override any restrictions that are set by the **Calling Permissions** fields on the Class of Restriction screen.

- Conference

  If call pickup alerting is enabled, and a user uses the Conference feature after the user answers the call, the call pickup status lamp goes out. If additional calls come into the pickup group, the status lamp of the user flashes.

- Consult

  If the Temporary Bridged Appearance capability is not enabled for the Call Pickup feature, the system presents a Consult call from the covering user as an idle call appearance.

- Expert Agent Selection (EAS)

  EAS agents use the Directed Call Pickup capability to:

  – Have other agents answer their calls

  – Answer the calls of other agents

  The Class of Restriction (COR) of the agent overrides the COR of the extension where the agent is logged in.

  If an agent is logged in to a telephone extension, and if the Directed Call Pickup capability is active for both the agent and the extension, the user can use either the agent Login ID or the telephone extension to answer the call with Directed Call Pickup.

Call Waiting Termination

Use the Call Waiting Termination feature to automatically notify a user with a single-line telephone who is active on a call, that a second call is waiting.

Detailed description of Call Waiting Termination

This section provides a detailed description of the Call Waiting Termination feature.

Users with a single-line telephone can place a call on hold to answer a waiting call. After a user answers the call that is waiting, the user can return to the call that is held, or the user can toggle back and forth between the two calls. A user with a single-line telephone can connect to only one call at a time.

Call Waiting tones

When a call is waiting for a user, the user hears:

- One quick burst of tone when a call from another user is waiting
- Two quick bursts of tone when an outside call, or a call that is handled by an attendant, is waiting
- Three quick bursts of tone when a priority call is waiting

Note that the system does not support special ring tones over direct inward dialing (DID) facilities.

A priority call can wait for the telephone to become idle even if Call Waiting Termination is not activated. However, if an attendant handles the call, the user hears a busy tone, unless the **Attendant Call Waiting Indication** field on the Station screen is set to **y**.

You assign Call Waiting Termination on a per-telephone basis. For a virtual extension, you assign Call Waiting Termination on the physical telephone.

Administering Call Waiting Termination

The following steps are part of the administration process for the Call Waiting Termination feature:

- Assigning Call Waiting Termination

This section describes:

- Any prerequisites for administering the Call Waiting Termination feature
- The screens that you use to administer the Call Waiting Termination feature
- Complete administration procedures for the Call Waiting Termination feature

Prerequisites for administering Call Waiting Termination

You must complete the following actions before you can administer the Call Waiting Termination feature:

- Administer the Feature-Related System Parameters screen to support the Call Waiting Termination feature on your system.

To administer the Feature-Related System Parameters screen to support the Call Waiting Termination feature on your system:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Repetitive Call Waiting Tone** field (Figure 147: Feature-Related System Parameters screen on page 683).

Figure 147: Feature-Related System Parameters screen

```
change system-parameters features                              Page  10 of 14
                        FEATURE-RELATED SYSTEM PARAMETERS

                 Pull Transfer: y          Update Transferred Ring Pattern? n
         Outpulse Without Tone? y            Wait Answer Supervision Timer? n
         Misoperation Alerting? n             Repetitive Call Waiting Tone? y
    Allow Conference via Flash? y    Repetitive Call Waiting Interval (sec): 4
 Vector Disconnect Timer (min):      Network Feedback During Tone Detection? y
   Hear Zip Tone Following VOA? y   System Updates Time On Station Displays? y
      Intercept Treatment On Failed Trunk Transfers? n
                    Station Tone Forward Disconnect: silence
                              Level Of Tone Detection: precise
          Charge Display Update Frequency (seconds): 30
        Date Format on 607/2420/4600/6400 Terminals: mm/dd/yy
Onhook Dialing on 607/2420/4600/6400/8400 Terminals? y




ITALIAN DCS PROTOCOL
  Italian Protocol Enabled? n
```

3. In the **Repetitive Call Waiting Tone** field, perform one of the following actions:
   - If you want the users and the attendants to hear a repetitive call waiting tone when the users and attendants use the Call Waiting Termination feature, type **y.**
   - If you do not want the users and the attendants to hear a repetitive call waiting tone when the users and the attendants use the Call Waiting Termination feature, type **n**.
4. In the **Repetitive Call Waiting Interval (sec)** field, type the number of seconds between the repetitive call waiting tones.
5. Press **Enter** to save your changes.

Screens for administering Call Waiting Termination

Screen name	Purpose	Fields
Feature-Related System Parameters	Specify that a user or an attendant hears a repetitive tone when a call is waiting.	**Repetitive Call Waiting Tone?**
	Specify the number of seconds between each repetitive call waiting tone.	**Repetitive Call Waiting Interval (sec)**

Screen name	Purpose	Fields
Station	Enable the Call Waiting Termination feature for a user.	**Call Waiting Indication**
	Enable the Call Waiting Termination feature for an attendant.	**Att. Call Waiting Indication**

Assigning Call Waiting Termination

To assign the Call Waiting Termination feature to a user or an attendant:

1. Type **change station *n***, where ***n*** is the extension to which you want to assign the Call Waiting Termination feature. Press **Enter**.

   The system displays the Station screen for the extension that you requested.

2. Click **Next** until you see the **Call Waiting Indication** field (Figure 148: Station screen on page 684).

Figure 148: Station screen

```
change station 20001                                          Page 2 of 3

                                    STATION
FEATURE OPTIONS
           LWC Reception: spe
          LWC Activation? y                      Coverage Msg Retrieval? y
  LWC Log External Calls? n                                Auto Answer: none
            CDR Privacy? n                           Data Restriction? n
   Redirect Notification? y                     Call Waiting Indication? y
 Per Button Ring Control? n                 Att. Call Waiting Indication? y
   Bridged Call Alerting? n                    Distinctive Audible Alert? y
        Switchhook Flash? y                          Adjunct Supervision? y
    Ignore Rotary Digits? n
        H.320 Conversion? n        Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic
    MWI Served User Type:
              AUDIX Name:
                                              Coverage After Forwarding? s

                                         Direct IP-IP Audio Connections? y
 Emergency Location Ext: 103                       IP Audio Hairpinning? y
     Precedence Call Waiting? y
```

3. In the **Call Waiting Indication** field, perform one of the following actions:
   - If you want to activate Call Waiting Termination for the user, type **y**.

     If you set the **Call Waiting Indication** field to **y**, calls that a user or an attendant originate, and calls that originate from the outside, wait at the single-line telephone if the telephone is busy. The system sends a distinctive call-waiting tone to the user.

     The system denies the Call Waiting Termination feature to a user if any of the following conditions are true:

     — **Data Restriction** field on the Station screen is set to **y**

     — **Switchhook Flash** field on the Station screen is set to **n**

     — Class of Service that you assign to the user activates the Data Privacy feature for the user

   - If you want to deactivate Call Waiting Termination for the user, type **n**.
4. In the **Att. Call Waiting Indication** field, perform one of the following actions:
   - Type **y** to activate Attendant Call Waiting Termination for the user.

     If you set the **Att. Call Waiting Indication** field to **y**, calls that an attendant originates, or that an attendant extends, wait at the single-line telephone if the telephone is busy. The system sends a distinctive call-waiting tone to the user.

     The system denies the Call Waiting Termination feature to a user if any of the following conditions are true:

     — **Data Restriction** field on the Station screen is set to **y.**

     — **Switchhook Flash** field on the Station screen is set to **n**.

     — Class of Service (COS) that you assign to the user activates the Data Privacy feature for the user.

   - Type **n** to deactivate Call Waiting Termination for the user.
5. Press **Enter** to save your changes.

Considerations for Call Waiting Termination

This section provides information about how the Call Waiting Termination feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Call Waiting Termination under all conditions. The following considerations apply to Call Waiting Termination:

- Call Waiting is available only for users who have single-line telephones. Calls to multiple-appearance telephones do not wait, because the system routes these calls to an idle call appearance.

- An analog telephone user must place the active call on soft hold, and dial the Answer Hold-Unhold Feature Access Code, to answer the waiting call.
- If you activate Call Waiting for a user of an analog single-line telephone, and the user starts a conference call, the system denies the Call Waiting feature to the user while the user is on the conference call.

Interactions for Call Waiting Termination

This section provides information about how the Call Waiting Termination feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call Waiting Termination in any feature configuration.

- The system denies the use of the Call Waiting Termination feature when any of the following conditions or features are active at a single-line telephone:
  - Another Call Waiting call
  - Automatic Callback (to or from the telephone)
  - Data Privacy
  - Data Restriction
- Call Pickup and Directed Call Pickup

  A member of a call pickup group cannot use the Call Pickup feature or the Directed Call Pickup capability to pick up a Call Waiting call.

Call-by-Call Service Selection

Use the Call-by-Call (CBC) Service Selection feature to allow a single ISDN trunk group to carry calls to several services. Call-by-Call Service Selection eliminates the need to dedicate each trunk group to a specific service. With Call-by-Call Service Selection, you can set up various voice and data services and features for a particular call.

Call-by-Call Service Selection provides the following benefits:

- Cost reduction. Since many services share the same trunks, this feature can reduce the total number of trunks that you must use.
- Improved service. Features and services are less likely to be blocked.
- Simplified networking. This feature simplifies network engineering. Instead of a per-service basis, you can analyze trunking needs based on total traffic.
- Tracking. Call-by-Call Service Selection calls are measurable.

Detailed description of Call-by-Call Service Selection

This section provides a detailed description of the Call-by-Call (CBC) Service Selection feature.

Call-by-Call Service Selection uses the same route patterns and route preferences as Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), and Generalized Route Selection (GRS). The system uses information that is assigned in the AAR, ARS, GRS route patterns to determine what service or facility to use on an outgoing Call-by-Call Service Selection call.

You can administer a variety of services to use a single trunk group. The system distributes traffic over all available trunks for increased efficiency. Then you can assign services that are used on incoming and outgoing Call-by-Call Service Selection calls.

Using Country Protocol 1, you can integrate services such as MEGACOM, ACCUNET, and INWATS onto a single ISDN trunk group, with flexible assignment of trunks to each service. Calls such as an incoming 800 service call that requires through-switching as an outgoing WATS call can be routed over the same facility.

Figure 149: Call-by-Call Service Selection example on page 688 shows an example of Call-by-Call Service Selection.

Figure 149: Call-by-Call Service Selection example

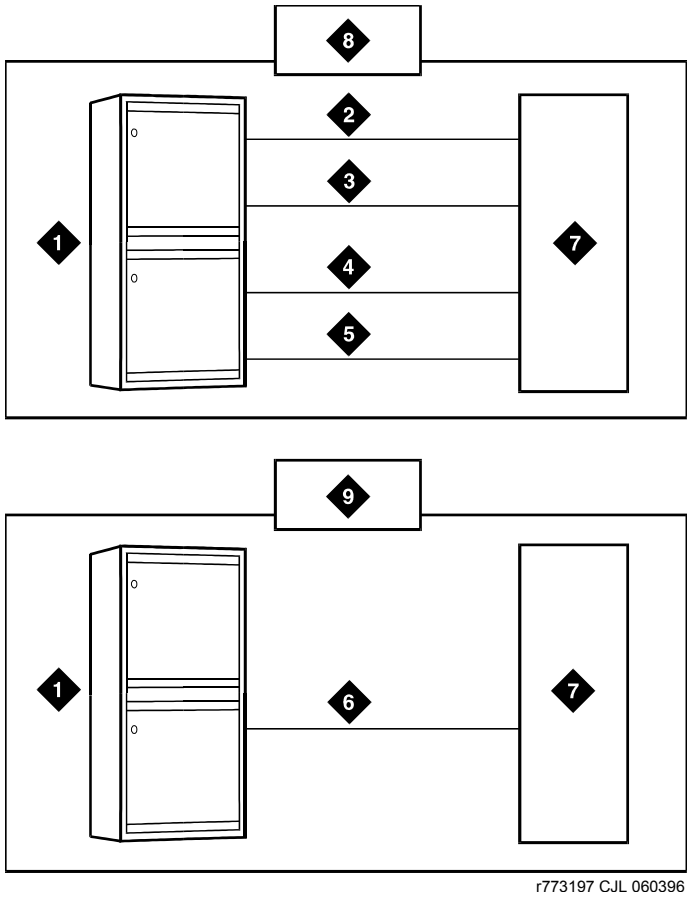


Figure notes:

1. Avaya S8*XXX* Server
2. MEGACOM trunk group
3. MEGACOM 800 trunk group
4. Software-defined network (SDN) trunk group
5. OUTWATS trunk group
6. Call-by-Call Service Selection trunk group
7. Public switched network
8. Without Call-by-Call Service Selection
9. With Call-by-Call Service Selection

ISDN messages and information elements for usage allocation

Call-by-Call Service Selection allows the system to specify service types on a call-by-call basis. To specify service types, you assign incoming calls to an ISDN Call-By-Call trunk group based on the number of the called party.

You can also specify service types in a SETUP message. This message indicates that the originating system intends to use the specified service or facility to initiate a call. The SETUP message can contain units called *Information Elements* (IE) that specify call-related information. Call-by-Call Service Selection uses the following IEs:

- Network-Specific Facility (NSF). Indicates which facilities or services are used to complete the call. NSF is usually not used outside the US and Canada.

  The system also checks all incoming ISDN trunk calls for the presence of an NSF IE. If an NSF IE is present, the system ensures that the requested service is compatible with the trunk administration before the system accepts the call.

  For an outgoing CBC trunk group, the system uses the service or the feature that is specified on the selected route pattern for the call to construct the NSF IE.

  If an associated NSF does not exist for the specified service or feature, the system does not send an NSF IE. For example, SETUP messages for incoming and outgoing calls that are classified only by a called-party number do not contain an NSF IE.

- Transit Network Selection. Indicates which interexchange carrier (IXC) the system uses on an inter-LATA call.

  If a call requires both the service or the feature and the IXC to be specified, the system sends the IXC information in the NSF IE, instead of in the Transit Network Selection IE.

Usage Allocation Plans

You can assign Usage Allocation Plans (UAPs) to provide more control over a Call-by-Call Service Selection trunk group. You can allocate a minimum and a maximum number of channels for incoming and outgoing called numbers, privileged users, and voice and data calls.

With a UAP, you can set the:

- Maximum number of trunks that each service can use at any given time. The sum for all services can exceed the total number of trunk group members. For example, for a 15-member trunk group, you can administer a maximum of seven MEGACOM service calls, six MEGACOM 800 service calls, and eight software-defined network (SDN) calls. This ensures that a specific service does not dominate all trunk group members, yet allows for fluctuations in demand.
- Minimum number of trunks that must always be available for each service. The sum for all services cannot exceed the total number of trunk group members. For example, for a 10-member trunk group that provides access to MEGACOM service, MEGACOM 800 service, and SDN service, the minimum number of trunks to use for each of these services cannot add up to more than 10.

When these UAP limits are exceeded, the system rejects the call, even if a trunk is available. On outgoing calls, the calling party hears a reorder tone, unless other routing preferences are available.

You can assign either a *fixed* or a *scheduled* UAP for each Call-by-Call Service Selection trunk group.

- With a fixed UAP, one plan applies at all times.
- With a scheduled UAP, you can administer different plans to apply at different times of the day and on different days of the week. You can assign as many as six activation times and associated plans for each day of the week.

You can administer a simple fixed UAP, or a flexible UAP with many scheduling options. You can even start out with no UAP, and then build the UAP as needed.

Incoming call-handling treatment

Call-by-Call Service Selection provides special incoming call-handling treatment for ISDN and SIP trunk groups. The system handles an incoming call on an ISDN or SIP trunk according to a treatment table that you administer for the trunk group. Depending on the platform that you use, the table allows for a different number of combinations of call treatments.

The system selects the treatment for an incoming call based on the first three columns of the Incoming Call-Handling Treatment (ICHT) screen. When the attributes of an incoming call match these specifications, the system treats the call according to the corresponding entries in the next four columns of the table. If an incoming call matches more than one set of specifications, the most restrictive case applies. The following table lists the possible cases from most restrictive to least restrictive.

	Service or feature	Called len	Called number
Most restrictive	Specified	Specified	*x* leading digits specified
	Specified	Specified	*y* leading digits specified, where *y* < *x*
	Specified	Specified	Not specified
	Specified	Not specified	Not specified
	"Other"	Specified	*x* leading digits specified
	"Other"	Specified	y leading digits specified, where *y* < *x*
	"Other"	Specified	Not specified
Least restrictive	"Other"	Not specified	Not specified

Call Detail Recording

On successful call attempts that use ISDN CBC trunk groups, Call Detail Recording (CDR) records the NSF that the NSF IEs of the call specify. CDR refers to this information as the ISDN Network Service (INS). The value that is passed to CDR is the 3-digit equivalent of the NSF IE. The system also records NSF information for Facility Type 2 calls that use ISDN Call-by-Call trunk groups, if the NSF is available in the incoming SETUP message.

If an outgoing Call-by-Call Service Selection call uses an interexchange carrier other than the presubscribed common carrier, CDR records the 3-digit or the 4-digit Interexchange Carrier (IXC) Code . CDR might not record the IXC properly if the dialed-code format differs from the US IXC code formats.

When a Call-by-Call Service Selection call is rejected because of a UAP, CDR records the cause as an ineffective call attempt. The NSF recording also occurs for the user-defined Facility Type 2. However, the NSF recording occurs only if the NSF is available in the incoming SETUP message.

Administering Call-by-Call Service Selection

You administer Call-by-Call Service Selection on a per-trunk-group basis.

The following steps are part of the administration process for the Call-by-Call Service Selection feature:

- Setting up a trunk group for CBC
- Administering incoming call handling treatment
- Administering route patterns for the CBC trunk group
- Administering network facilities

This section describes:

- Any prerequisites for administering the Call-by-Call Service Selection feature
- The screens that you use to administer the Call-by-Call Service Selection feature
- Complete administration procedures for the Call-by-Call Service Selection feature

Prerequisites for administering Call-by-Call Service Selection

You must complete the following actions before you can administer the Call-by-Call Service Selection feature:

- View the Optional Features screen, and ensure that the following fields are set to **y**:
  - **ISDN**
  - **ISDN-BRI Trunks**
  - **Usage Allocation Enhancements**

  If any of these fields is set to **n**, your system might not be enabled for the Call-by-Call Service Selection feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Call-by-Call Service Selection

Screen name	Purpose	Fields
Optional Features	Ensure that the proper license fields are set to **y**.	• **ISDN-PRI** • **ISDN-BRI Trunks** • **Usage Allocation Enhancements**
ISDN Trunk Group	Indicate the service for which this trunk group is dedicated.	• **Service Type** • **Usage Alloc** • All fields on the **CBC** Trunk Group Usage Allocation page • All fields on the CBC Trunk Group Usage Allocation Plan Assignment Schedule page
Incoming Call Handling Treatment	Specify call handling for ISDN and SIP trunk groups.	• All fields on the Incoming Call Handling Treatment (ICHT) Table screen
Route Pattern	Administer the route patterns to use with this trunk group.	• **IXC** • **Service/Feature** • **Band**
Network-Facilities	Administer network facilities for Call-by-call Service Selection.	All

Setting up a trunk group for CBC

To set up a trunk group for Call-by-Call Service Selection:

1. Type **`change trunk-group n`**, where ***n*** is the ISDN trunk group that you want to designate for Call-by-Call Service Selection. If you want to add a new trunk group, type **`add trunk-group x`**, where ***x*** is the next unused trunk group number.

   The system displays the ISDN Trunk Group screen.
2. In the **Group Type** field, type **isdn**. The system displays additional ISDN-specific fields.
3. In the **Service Type** field, type **cbc** for Call-by-call Service Selection.
4. In the **Usage Alloc?** field, type **y** to allocate the service that the trunk group provides.
5. Click **Next** until you see the CBC Trunk Group Usage Allocation page.

6. In the **Service/Feature** field under the **Usage Allocation Plan 1** column, type the name of the service for which you want to allocate CBC trunk service. You can administer up to three (UAPs) for each trunk.
7. In the **Min # Chan** and **Max # Chan** fields, type a minimum number and a maximum number of channels for incoming and outgoing called numbers, privileged users, and voice and data calls.
8. Repeat steps 8 and 9 for each service for which you want to allocate CBC trunk service.
9. Click **Next** until you see the CBC Trunk Group Usage Allocation Plan Assignment Schedule page.
10. In the **Fixed** field, perform one of the following actions:
    - If you want a specific UAP to be activated at all times for this trunk group, type **y**. If you type **y**, the **Allocation Plan Number** field appears.
    - If you do not want a fixed UAP to be activated at all times for this trunk group, type **n**.
11. In the **Allocation Plan Number** field, type the number of the UAP that you want to be activated at all times for this trunk group.
12. In the **Scheduled** field, type **y** if you want to administer a schedule that can change up to six times a day for each day of the week.
13. For each day of the week, use the **Act Time** and the **Plan #** fields to type the activation time, and the type of UAP to use at different times of the day.
14. Press **Enter** to save your changes.

Administering incoming call handling treatment

To administer incoming call handling treatment for a CBC trunk group:

1. Type **`change inc-call-handling-trmt`**. The system displays the Incoming Call Handling Treatment screen (Figure 150: Incoming Call Handling Treatment screen on page 694).

Figure 150: Incoming Call Handling Treatment screen

```
change inc-call-handling-trmt                                    Page y of x

INCOMING CALL HANDLING TREATMENT
     Service/    Called     Called       Del     Insert         Per Call     Night
     Feature      Len       Number                              CPN/BN       Serv
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
    _____________ ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
   _____________  ___   _____________   ___   _____________ __________   _______
```

2. Complete the fields on the Incoming Call Handling Treatment screen for each Call-by-Call Service Selection service.

Note:

For SIP trunk groups, the **Per Call CPN/BN** and **Night Serv** fields do not appear on the Incoming Call Handling Treatment screen. For more information on the Incoming Call Handling Treatment screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Administering route patterns for the CBC trunk group

To administer route patterns for a CBC trunk group:

1. Type **change route-pattern *n***, where ***n*** is the number of the route pattern that you want to administer.

   The system displays the Route Pattern screen (Figure 151: Route Pattern screen on page 695).

Figure 151: Route Pattern screen

```
change route-pattern 1                                          Page 1 of X
                              Pattern Number: 1_

                                  No.                                    DCS/
  Grp. FRL NPA Pfx Hop Toll Del   Inserted
                                  QSIG  IXC
   No.          Mrk Lmt List Dgts  Digits                              Intw
1: ___   _  ___  _  __   __   __  ____________________________________  n   user
2: ___   _  ___  _  __   __   __  ____________________________________  n   user
3: ___   _  ___  _  __   __   __  ____________________________________  n   user
4: ___   _  ___  _  __   __   __  ____________________________________  n   user
5: ___   _  ___  _  __   __   __  ____________________________________  n   user
6: ___   _  ___  _  __   __   __  ____________________________________  n   user

      BCC VALUE  TSC CA-TSC   ITC BCIE Service/Feature BAND  No. Numbering LAR
     0 1 2 3 4 W     Request                                  Dgts   Format
                                                           Subaddress
 1: y y y y y n  y  none  ___ both ept outwats-bnd____ ____  _    ______  none
 2: y y y y y n  y           rest     ________________       _    ______  next
 3: y y y y y n  y           rest     ________________       _    ______  rehu
 4: y y y y y n  y           rest     ________________       _    ______  none
 5: y y y y y n  y           rest     ________________       _    ______  none
 6: y y y y y n  y           rest     ________________       _    ______  none
```

2. In the **IXC** (Interexchange Carrier) field, identify the carrier, such as AT&T, that the system uses for calls that are routed over an IXC, and for Call Detail Recording (CDR). This field can also be left blank.
3. In the **Service/Feature** fields, type the name of the service that is associated with this route pattern.
4. If the value in the **Service/Feature** field is **outwats-bnd**, use the **Band** field to enter a number that represents the OUTWATS band number (US only).
5. Press **Enter** to save your changes.

Note:
For more information on the Route Pattern screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Administering network facilities

The Network Facilities screen supports the Call-by-Call Service Selection feature for ISDN trunks. Only Avaya personnel can administer these predefined services and features. If the **Usage Allocation Enhancement** field on the Optional Features screen is set to **y**, you can administer the **Additional Services/Features** fields.

To administer network facilities:

1. Type **change isdn network-facilities**. Press **Enter**.

   The system displays the Network Facilities screen (Figure 152: Network Facilities screen on page 696).

Figure 152: Network Facilities screen

```
change isdn network-facilities                                  Page 1 of X
                          NETWORK-FACILITIES
                        Facility                                 Facility
          Name          Type   Coding                Name        Type Coding
       sub-operator      0     00110             mega800          1   00010
       operator          0     00101             megacom          1   00011
       outwats-bnd       1     00001             inwats           1   00100
       sdn               1     00001             wats-max-bnd     1   00101
       accunet           1     00110             lds              1   00111
       i800              1     01000             multiquest       1   10000
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
       _______________   _     ______            _______________  _   _____
```

2. In the **Name** field, type up to 15 alphanumeric characters to specify the name of the indicated service or feature.
3. In the **Facility Type** field, perform one of the following actions:
   - If the associated entry is a feature, type **0**.
   - If the associated entry is a service, type **1**.
   - If the associated entry is of type **incoming**, type **2**.
   - If the associated entry is of type **outgoing**, type **3**.

Note:
You can administer types 2 and 3 if the **Usage Allocation Enhancements** field on the Optional Features screen is set to **y**.

If the **Facility Type** field is set to either **0** or **1**, the **Facility Coding** field displays five binary values. These values specify the ISDN encoding value of the associated service or feature.

4. Press **Enter** to save your changes.

Interactions for Call-by-Call Service Selection

This section provides information about how the Call-by-Call Service Selection feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Call-by-Call Service Selection in any feature configuration.

- Call Detail Recording (CDR)

  On successful call attempts that use ISDN Call-By-Call trunk groups, CDR records the Network-Specific Facility (NSF) that is specified by the NSF IE of the call. CDR refers to this information as the ISDN Network Service (INS). The value that is passed to CDR is the 3-digit equivalent of the NSF IE. NSF information for Facility Type 2 calls, which is used with ISDN Call-by-Call trunk groups, is also recorded if the NSF is available in the incoming SETUP message.

  If an outgoing Call-by-Call Service Selection call uses an interexchange carrier (IXC) other than the presubscribed common carrier, CDR records the 3-digit or the 4-digit IXC code . CDR might not record the IXC code properly if the dialed-code format differs from the IXC formats that are used in the US.

  When a Call-by-Call Service Selection call is rejected because of a Usage Allocation Plan (UAP), CDR records the cause as an ineffective call attempt. The NSF recording also occurs for the user-defined Facility Type 2 call. However, the NSF recording occurs only if the NSF is available in the incoming SETUP message.

- Generalized Route Selection (GRS)

  Call-by-Call Service Selection uses the same routing tables and routing preferences that GRS uses.

- Multiquest Flexible Billing

  Do not use a service or a facility with the Facility Type set to 2 or 3. NSF processing is not performed for Facility Type 2. An NSF is not included in the outgoing SETUP message for Facility Type 3.

- Time-of-Day Routing

  Any Time-of-Day Routing administration that affects routing preference also affects Call-by-Call Service Selection. Use Time-of-Day Routing to vary the IXC, based on the time of day and the day of week.

- Traffic Measurements

  The system provides traffic measurements for each service that is administered for an ISDN Call-by-Call Service Selection trunk group.

Caller ID

Use the Caller ID feature to interpret calling party information that is signaled over ISDN or H.323 trunks, and displaying the calling party number on your display telephone. Caller ID is also known as Incoming Call Line Identification (ICLID).

Detailed description of Caller ID

This section provides a detailed description of the Caller ID feature.

The Caller ID feature displays calling party information on your display telephone that is signaled over ISDN or H.323 trunks.

- For a description about calling party information that is signaled over multifrequency (MF) or Session Initiation Protocol (SIP) trunks to your display telephone, see the "Automatic Number Identification" feature.
- For a description about calling party information that is signaled over Centralized Automatic Message Accounting (CAMA) trunks to your local emergency rapid response organization, see the "E911" feature.

Communication Manager stores and displays up to 15 characters of caller ID information, which the central office (CO) sends on incoming calls. If the information is longer than 15 characters, the software truncates the information to 15 characters. If the caller ID information is not received, the system displays the trunk group name and the trunk access code (TAC).

In the US, the CO sends both calling party name and calling party number, if this information is available. In Japan, the CO sends only the calling party number. This information is sent on a CO loop-start trunk in the US. In Japan, this information is sent on either a CO loop-start trunk, a Direct Inward Dialing (DID) trunk, or a Direct Inward and Outward Dialing (DIOD) trunk.

Caller ID supports the following capabilities:

- Caller ID on analog trunks
- Caller ID on digital trunks

Caller ID on analog trunks

Caller ID on analog trunks is also known as Bellcore Calling Name ID. This capability allows the system to accept calling name information from a local exchange carrier (LEC) network that supports the Bellcore calling name specification. The system can also send calling name information in the correct format if Bellcore calling name ID is properly administered. The following caller ID protocols are supported:

- Bellcore (default). US protocol (Bellcore transmission protocol with 212 modem protocol)
- V23-Bell. Bahrain protocol (Bellcore transmission protocol with V.23 modem protocol)

Caller ID on digital trunks

In the US, a CO can send the calling party name and the calling party number over digital trunks for display on digital telephones. The display of the calling party name and the calling party number works with all Communication Manager Digital Communications Protocol (DCP) and Basic Rate Interface (BRI) digital telephones that have either a 40-character or a 32-character alphanumeric display.

Administering Caller ID

The following steps are part of the administration process for the Caller ID feature:

- Displaying Caller ID information

This section describes:

- Any prerequisites for administering the Caller ID feature
- The screens that you use to administer the Caller ID feature
- Complete administration procedures for the Caller ID feature

Prerequisites for administering Caller ID

You must complete the following actions before you can administer the Caller ID feature:

- View the Optional Features screen, and ensure that the **G3 Version** field is set to **V6** or later, and that the **Analog Trunk Incoming Call ID** field is set to **y**. If the **G3 Version** field is not set to **V6** or later, or if the **Analog Trunk Incoming Call ID** field is set to **n,** your software is not enabled for the Caller ID feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Caller ID

Screen name	Purpose	Fields
Optional Features	Ensure that the **Analog Trunk Incoming Call ID** field is set to **y**.	**Analog Trunk Incoming Call ID**
Trunk Group	Set this field to **120** for Caller ID.	**Incoming seizure (msec)**
	Set up the trunk group to receive caller ID information.	**Receive Analog Incoming Call ID**
	Set to **incoming** or **two-way.**	**Direction**

Displaying Caller ID information

To set up a trunk group to receive calling party information and display the calling party name and the calling party number on the telephone display of the called party:

1. Type **`change trunk group n`**, where ***n*** is the number of the trunk group for which you want to set up Caller ID. If you want to set up a new trunk group, type **`add trunk group next`**.

   The system displays the Trunk Group screen.
2. In the **Group Type** field, type **co**, **did**, or **diod**.
3. In the **Direction** field, type **incoming** or **two-way**.

Note:
When the **Group Type** is **diod**, the **Direction** field defaults to **two-way**. When the **Group Type** is **did**, the **Direction** field is hidden, because all calls are incoming.

4. Click **Next** until you see the Trunk Features section.
5. In the **Receive Analog Incoming Call ID** field, type **Bellcore** for the US, or **NTT** for Japan.
6. Click **Next** until you see the **Administrable Timers** section.

7. In the **Incoming Seizure (msec)** field, type **120**.
8. Press **Enter** to save your changes.

Considerations for Caller ID

This section provides information about how the Caller ID feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Caller ID under all conditions. The following considerations apply to Caller ID:

- If you use Incoming Caller ID on analog trunks that are connected to a Direct Inward and Outward Dialing (DIOD) central office (CO) trunk circuit pack, do not put these trunks in an outgoing Automatic Alternate Routing (AAR) or an Automatic Route Selection (ARS) route pattern. The loop-start trunks that the DIOD CO trunk circuit pack supports do not provide answer supervision. Thus the potential for toll fraud exists.

Interactions for Caller ID

This section provides information about how the Caller ID feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Caller ID in any feature configuration.

- Attendant Display Features

  A call that is redirected to either the attendant or the attendant queue causes the display on the station of the attendant to match that of the station display of the connected party.

- Automatic Display of Incoming Call Identification

  If a new call comes in while the station user is off-hook and connected to a call, the display automatically shows the new incoming call identity for 30 seconds. After 30 seconds, the display returns to the identity of the original call. If the system redirects the call after a few rings, the display returns to the identity of the original call. If the system shows a new incoming call, and then that call drops, the display returns to the identity of the original call.

- Bridged Call

  The system shows incoming call identity on both the primary station and the bridged station.

- Call Forwarding
  - Forwarded-From Station Display

    The system does not show any information on the station of the called principal.

  - Forwarded-To Station Display

    The system shows the identity of the calling party and the called party, and the reason (R) code. If the forwarded-to station is on a different switch, the system does not forward the called party information.

- Call Pickup
  - Called Party Station Display

    Shows the identity of the calling party.

  - Answering Party Station Display

    If Call Pick-Up answers a Caller ID call, the system shows the identities of both the calling party and the called party.

- Call Coverage
  - Called Party Display

    The display of the called party shows the identity of the calling party until the coverage party answers the call. If the coverage party answers the call, the station display of the called party goes blank. If the called party temporarily bridges in after the coverage party answers the call, the displays of the coverage party and the called party change to indicate a conference call.

  - Coverage User Station Display

    The station display of the coverage user shows the same display as the station display of the connected party.

- Call Vector Routing

  When a Caller ID call coming from analog trunks transfers to a Vector Directory Number (VDN), the incoming calling number is directed to that VDN so call vector routing can be based on the caller ID information.

  The Automatic Number Identification (ANI) that is received for the incoming call, by way of inband signaling or ISDN, is forwarded with a route-to step over a trunk that supports inband or ISDN ANI delivery.

- Distributed Communications System (DCS)

  If Communication Manager has both DCS and Integrated Services Digital Network (ISDN) displays, the system shows the caller ID information in DCS formats.

- Hold

  When Hold is activated, the display becomes blank. The party who activates the Hold then reads the identity of the newly connected party. The display of the held station remains unchanged. When the party deactivates the Hold, the system refreshes the display to indicate the current state of the call.

- Malicious Call Trace (MCT)

  When MCT is activated for a particular call, the system displays incoming calling numbers to controller stations.

- Tandem Operations

  The system passes the calling party name and the calling party number to the terminating server over ISDN trunks with DCS Plus (+).

- Transfer

  When the system transfers an Caller ID call, the display of the transferred-from station becomes blank. The display of the transferred-to station shows the identity of the transferred-from party if the transfer is not yet complete. Once the transfer is complete, the transferred-to station shows the identity of the calling party.

Centralized Attendant Service

Use the Centralized Attendant Service (CAS) feature to allow attendants within a private network to serve all branch locations from a central or a main location. Each branch in a centralized attendant service has its own listed directory number (LDN) or other type of access from the public network. With this feature, the system routes incoming calls to a branch, and calls that users make directly to the attendants, to the centralized attendant. CAS uses release link trunks (RLT) to direct calls. RLT is not used when QSIG CAS is used.

Detailed description of Centralized Attendant Service

This section provides a detailed description of the Centralized Attendant Service (CAS) feature.

With Centralized Attendant Service (CAS), you can provide attendant services in a private network from a central location.

The CAS main system operates independently of the individual CAS branch systems. The operation for CAS main system traffic is identical to the operation of a stand-alone system.

Each branch in a CAS network connects to the main office through RLTs. These trunks provide paths to:

- Send incoming attendant-seeking trunk calls at the branch to the main location for processing and extend the calls back to the branch. Both parts of a call use the same trunk.
- Return timed-out waiting and held calls from the branch to the main location.
- Route calls from the branch to the main location.

Two queues are associated with CAS calls. One queue is at the main office, and the other queue is at the branch. If idle RLTs are available from the branch to the main location, RLTs are seized. CAS calls are then queued at the main location, along with other attendant-seeking calls. If all RLTs are in use, CAS calls to the attendant are queued at the branch in an RLT queue. The length of the queue can vary from 1 to 100 calls. You set the length of the queue when you administer the RLT group.

Backup service provides for all CAS calls to be sent to a backup extension in the branch if:

- All RLTs maintenance-busy
- All RLTs are out of service
- The attendant presses a Backup button that is not lit

To activate this feature and to provide notification that backup service is in effect, assign the backup extension to a Backup button and an associated status lamp.

- The status lamp remains lit as long as backup service is in effect.
- To deactivate the CAS feature, the attendant presses the Backup button while the status lamp is lit. The system does not send calls to the backup extension unless all RLTs are maintenance-busy, or out of service.

The attendant can put a CAS call from a branch on Remote Hold. The branch holds the call, and drops the RLT. After a timeout, which is the same as the timed reminder for an attendant-held call, the branch automatically attempts to route the call back to the attendant. The returning call can queue for the RLT. Attendants can use Remote Hold when the attendant must put a call on hold to prevent the unnecessary use of RLTs.

Centralized Attendant Service (CAS) supports the following capabilities:

- Branch-generated call identification tones

Branch-generated call identification tones

The branch in a CAS network generates call identification tones, and transmits the tones to the CAS attendant through RLTs. These tones indicate the type of call from the branch, or the status of a call extended to or held at the branch. The attendant hears these tones in the console handset before the attendant is connected to the caller.

The following identification tones might vary by country.

- Incoming trunk calls: 480 Hz (100 ms), 440 Hz (100 ms), 480 Hz (100 ms) in sequence. The attendant hears this tone immediately after the attendant lifts the handset.
- Calls from a branch telephone to the main attendant, or calls that are transferred by a branch telephone to the main attendant 440 Hz (100 ms), silence (100 ms), 440 Hz (100 ms) in sequence. The attendant hears this tone immediately after the attendant lifts the handset.
- Calls that the system extends to an idle telephone, or recall on Does Not Answer: The attendant hears ringback tone (300 ms), and then connection to the normal ringing cycle.
- Calls that the system extends to a busy telephone, automatically waiting, or recall on Attendant Call Waiting: 440 Hz (100 ms).
- Calls that the system extends to a busy telephone, waiting denied, or not provided: A busy tone.
- Remote Hold or Remote Hold recall: A series of four to six cycles of 440 Hz (50 ms), and then silence (50 ms).
- Recall on Does Not Answer: A burst of ringback tones (300 ms), and then connection to normal ringback at any point in the cycle.

- Recall from a call that is on Remote Hold: A series of four to six cycles of 440 Hz (50 ms), and then silence (50 ms).
- Recall from a call that is waiting at a single line telephone: A burst of 440 Hz (100 ms).

The centralized attendant at the main location has access, through RLTs, to all outgoing trunk facilities at the branches in a CAS network. To extend an incoming LDN call to an outgoing trunk at a branch, an attendant can dial the access code, and then allow the caller to dial the rest of the number. The attendant can also dial the complete outgoing number.

Calls that are extended to busy single-line telephones at the branch wait automatically. If a call is in queue, the user hears a busy signal. When Station Hunting and Send All Calls is administered, the system routes the call along the administered path. If any extended call is waiting, and is unanswered within an administered interval, the branch system returns the call to the attendant. Call Waiting does not apply to multiappearance telephones. If no appearances are available, busy tone is sent to the attendant, who tells the caller that the line is busy.

The system also routes calls from telephones at the branch to an attendant over RLTs that are seized by the branch system. To reach the attendant, a branch caller dials the attendant-group access code. This access code is administrable. The default is 0. The conversation between the branch caller and the attendant ties up the seized RLT, but calls of this type are usually short.

Administering Centralized Attendant Service

This section contains prerequisites and the screens for administering the Centralized Attendant Service (CAS) feature.

Prerequisites for administering Centralized Attendant Service

You must complete the following actions before you can administer the Centralized Attendant Service (CAS) feature:

- Set up the attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
- On the Optional Features screen, ensure that the **Async. Transfer Mode (ATM) PNC** field is set to **y**. If this field is set to **n**, contact your Avaya representative before you continue with these procedures.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Centralized Attendant Service

Screen name	Purpose	Fields
Optional Features	Enable port network connectivity (PNC).	**Async. Transfer Mode (ATM) PNC**
Attendant Console	Assign feature buttons.	Any available button field in the **Feature Button Assignments** area.
Console-Parameters	Set up parameters for CAS.	• **CAS** • **RLT Trunk Group Number** • **Timed Reminder on Hold** • **Return Call TImeout (sec)**
Station	On a multiappearance telephone, assign feature buttons.	Any available button field in the **Feature Button Assignments** area.
Trunk Group	Set up a release link trunk (RLT) group.	All
Feature Access Code (FAC)	Set up a Feature Access Code (FAC) for CAS Remote Hold.	**CAS Remote Hold/Answer Hold-Unhold Access Code**

Reports for Centralized Attendant Service

The following reports provide information about the Centralized Attendant Service (CAS) feature:

- None

Considerations for Centralized Attendant Service

This section provides information about how the Centralized Attendant Service (CAS) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Centralized Attendant Service (CAS) under all conditions. The following considerations apply to Centralized Attendant Service (CAS):

- In a CAS network, systems can function either as branches or as the main location. A branch can connect to only one main location.
- CAS reduces the number of attendants that are required at a branch. For example, a chain of department stores can have a centralized attendant at the main store to handle calls for all of the branch stores.
- A branch can have an attendant. Access to the branch attendant must be by way of an individual attendant extension. Incoming trunk calls in a CAS network can bypass branch attendants. The centralized attendant can route these incoming trunk calls back to the branch attendant.
- Branch calls terminate on the CAS main system based day-destination or night-service destination of the incoming RLT trunk group. An attendant console might not always answer or extend incoming CAS calls.

  If someone other than an attendant answers a CAS call, that person can either press the Flash button on a multiappearance telephone, or flash the switch hook on a single-line telephone, to extend the call back to the branch. The branch reaction to flash signals and the branch application of tones is the same whether an attendant, or someone other than an attendant, answers or extends the call.
- If an extended call returns unanswered to the main attendant, the called party at the branch does not drop. The called party at the branch continues to be alerted until the caller releases. This process allows the attendant to talk to the caller, and then extend the call again, if the caller wants, without redialing the number.
- If an extended CAS call recall times out and goes to coverage, but is unanswered, the branch leaves the extended-to party ringing. The system drops coverage.
- When an analog telephone call goes to coverage, the telephone drops from the call. This process is the exception to the branch leaving the extended-to party ringing. If the main attendant extends a call to an analog telephone, and that call goes to coverage and later returns to the main attendant, the call is treated as an incoming LDN call. If the user requests, the attendant must reextend the call.
- On an incoming CAS call to the main attendant, the system displays the **Name** field from the Trunk Group screen for that RLT to the attendant. Therefore, you must administer the **Name** field on the Trunk Group screen to provide meaningful branch identification information.
- The Music-on-Hold feature at a branch applies to two stages of LDN calls: during call extension, and when the call is on Remote Hold.

Interactions for Centralized Attendant Service

This section provides information about how the Centralized Attendant Service (CAS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Centralized Attendant Service (CAS) in any feature configuration.

- Abbreviated Dialing

  The main attendant can use an Abbreviated Dialing button to extend CAS calls after the attendant obtains branch dial tone.

- Attendant Auto-Manual Splitting

  The Split lamp and button do not function on CAS calls to the main location that are extended through RLTs. Attendant conference does not function on CAS calls.

- Attendant Control of Trunk Group Access

  If a branch attendant has control of an outgoing RLT trunk group, the system routes new attendant-seeking calls to the branch attendant.

- Attendant Override of Diversion

  Use Attendant Override of Diversion with CAS.

- Attendant Serial Calling

  Attendant Serial Calling does not work for CAS calls.

- Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS)

  You can use AAR and ARS to route CAS calls.

- Automatic Circuit Assurance (ACA)

  When CAS is activated, the **ACA Referral Calls** field on the Feature-Related System Parameters screen must be set to **local**. The system interprets a referral destination of 0 as the local attendant, if a local attendant exists. The CAS attendant cannot activate or deactivate ACA referral calls at a branch location.

- Busy-Indicator Buttons

  Busy indicators can identify incoming calls over an RLT. You can also use Busy indicators to dial after the attendant starts to extend a call.

- Call Coverage

  Use Call Coverage to redirect calls to a centralized attendant. Do not redirect calls to a CAS backup extension for backup service through Send All Calls to the coverage path of the backup extension.

- Call Detail Recording (CDR)

  If the CAS main RLT has the CDR option selected, the system generates CDR records for incoming CAS calls.

- Call Forwarding

  Do not forward calls to a CAS extension.

- Call Park

  If a CAS attendant parks a call and the call returns to the attendant after the Call Park expiration interval, the attendant hears incoming trunk-call notification.

- Class of Restriction (COR)

  Since COR information is not passed over RLTs, fully restricted service allows all CAS calls. Therefore, CAS allows the system to complete a public network call to a fully restricted telephone.

- Distributed Communications System (DCS) operation

  If an RLT trunk group is administered as a DCS trunk, the DCS message displays instead of the name of the incoming RLT trunk group on an incoming CAS call to the attendant. When the attendant answers the call, the attendant hears call identification tones. These tones indicate that the call is a CAS call. The attendant must use a Trunk-Name button to obtain the name of the RLT trunk group.

- DXS and DTGS Buttons

  DXS and DTGS buttons at the main attendant console can be used with CAS. With the DXS button, the attendant hears ringback tone after a delay of a few seconds.

- Emergency Access to the Attendant

  For CAS Branch Emergency Access calls that generate by a Feature Access Code, the system routes Off-Hook Alert to the branch attendant group. If there is no attendant in the branch, the system routes the call to the administered Emergency Access Redirection Extension of the branch. When the branch system is in CAS Backup Service, the system routes the calls to the backup telephone. The call is treated as a normal call.

- Hunt Groups

  If the system directs an incoming CAS call to a hunt group, the system does not redirect the call to the coverage path of the hunt group. Depending on the circumstances, the attendant can get a busy tone or ringing.

- Last Number Dialed (LND)

  An attendant cannot extend calls with the LND feature.

- Leave Word Calling (LWC)

  If a message is left for a branch user, and the attendant at the CAS system tries to retrieve the message, permission is denied.

- Night Service, Night Console Service

  When the attendant places the CAS main location in Night Service, CAS calls terminate at the CAS main night-service destination. When an attendant places a branch location in Night Service, the system routes the CAS calls to the branch night console, to the LDN night telephone, or to the TAAS telephone.

- Night Service, Trunk Answer from Any Station (TAAS)

  In a multisystem DCS environment with CAS, transferring incoming trunk calls through Night Service Extension or TAAS varies. Such a transfer depends on the:

  - Home system of the transferred-to telephone
  - Home system of the connected trunk
  - Type of night-service function that is chosen. The type of night-service function can be Night Service Extension, TAAS, or both Night Service Extension and TAAS.

- Extending a CAS call by a nonattendant

  CAS branch calls terminate at the CAS main location, based on the day-destination or the night-service destination of the incoming RLT trunk group. You can also answer a CAS call with the TAAS feature.

  Usually, a nonattendant presses the Flash button to extend a CAS call. However, if the nonattendant does not have a Flash button, a nonattendant can extend the call in one of the following ways:

  - Multiappearance telephone users can press the Conference or Transfer button, and then dial the extension. To complete the call, the user drops the call. To drop the extended-to party, the user presses the Conference or Transfer button again.
  - Single line telephone users can flash the switch hook, and then dial the extension. To complete the call, the user drops the call. To drop the extended-to party, the user flashes the switch hook again.

- Holding a CAS call by a nonattendant

  A nonattendant with a multiappearance telephone can press the Hold button to hold a CAS call.

- Releasing a CAS call by a nonattendant

  A nonattendant can drop the RLT by going on-hook, and then use the Disconnect or Drop button. A nonattendant can also drop the RLT by selecting another call appearance.

- Nonattendant. Display Trunk Name

  If a nonattendant with a display telephone presses the Trunk Name button while the nonattendant is active on a trunk call, the system displays the value in the **Name** field from the Trunk Group screen.

- Security Violation Notification (SVN)

  CAS attendants cannot receive referral calls from branch locations.

- Timed Reminder

  You can set the timer value for recalling held calls at the attendant console on the Console screen.

  If an attendant at the CAS main location transfers a call from a branch to an extension at the main location, the timed reminder does not apply. The call does not return to the attendant if unanswered. If a branch call is unanswered, the branch timed reminder times out, and the system routes the call to a new RLT trunk, and back to a CAS main attendant.

- Trunk-Name button

  Use the Trunk-Name button when you make an outgoing call over a trunk that is administered to have no outgoing display.

Class of Restriction

Use the Class of Restriction (COR) feature to:

- Define different levels of call origination and termination privileges
- Apply administration settings to all objects that share the same COR number
- Identify what CORs can be service observed, and what CORs can be a service observer

Detailed description of Class of Restriction

This section provides a detailed description of the Class of Restriction (COR) feature.

You can use CORs to restrict communication between point A and point B. For example, a user tries to establish a communication path between point A and point B. The system checks whether the CORs have permission to communicate with one another. If the CORs have permission, the system completes the call. If the CORs do not have permission, the system does not complete the call. You control the level of restriction that the COR provides.

CORs also have other applications. You can apply administration settings to a COR, and then assign that COR to objects or facilities in the system. This use of CORs makes it easier to administer functions across a wide range of objects. CORs are assigned to a variety of objects, such as:

- Telephones
- Trunks
- Agent login IDs
- Data modules

Finally, you can set up CORs that are service observing and service observed. You can assign a COR to be a service observer. Then you identify what other CORs that the user can observe. You can also set up a COR to be serviced observed.

To set up a COR, you select a COR number, from **0** to **995** (CORs 996 through 999 are reserved for use by the software). You then assign a name for the COR that clearly reflects either the purpose or the members of the COR. You then use the Class of Restriction screens to select what restrictions, if any, apply to the COR. After you set up a COR, you assign the COR number to objects on your system.

Note:
Your system might use only one COR or as many as necessary to control calling privileges. You can assign up to 995 different CORs.

Many objects can share the same COR number. You must administer a COR for the following objects:

- Agent login IDs
- Access endpoints
- Announcements and audio sources
- Attendant consoles
- Authorization codes
- Console parameters
- Hunt groups
- Loudspeaker paging
- Data modules
- Remote access (each barrier code has a COR)
- Telephones
- Terminating Extension Groups (TEGs)
- Trunk groups
- Vector Directory Numbers (VDNs

Note:

The **Outgoing Trunk Disconnect Timer (minutes)** field on the Class of Restriction screen provides the capability to disconnect an outgoing trunk automatically after an administrable amount of time. This field defaults to blank (outgoing trunk calls are only disconnected when dropped by one or all parties), or you can enter a timer value in number of minutes to apply to outgoing trunk calls if the initiating party belongs to this COR. For more information on values for the fields, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Mask CLI/Station Name for Internal Calls

A typical Communication Manager internal call generally provides calling/called party numbers and administered text name string, which are displayed on the involved parties' terminals.

Beginning with Communication Manager Release 4.0, the Mask CLI/Station Name for Internal Calls feature provides a new station capability (through proper COR administration) of masking off such information and replacing it with a "hard-coded," system-wide text string, "Info Restricted," which will be displayed on the party's terminal. In addition, the feature shall provide a means of administering that the CPN/Name information not be masked-off when the call is made.

Currently Communication Manager can block calling party number and name to be sent to the network with proper trunk/station administration.

This new feature, Mask CLI/Station Name for Internal Calls takes a similar approach to these existing Communication Manager capabilities whenever it is applicable for internal calls.

The Class of Restriction screen has a new field called **Mask CPN/NAME for Internal Calls**. Enter **y** to hide the display of calling/called party numbers and administered name on internal calls.
The Class of Service screen also has a new field called **Masking CPN/Name Override**. Setting **y** on this field allows users to override the Mask CLI/Station Name for Internal Calls capability.

For more information on these fields, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Note:
This feature does not work for SIP stations.

Strategy for assigning CORs

When you administer your system, the best strategy is to assign CORs to similar groups or objects. For example, you might create a unique COR for each type of user or facility, such as:

- Call center agents
- Account executives
- Supervisors
- Administrative assistants
- Paging zones
- Data modules

You might also want to create a unique COR for each type of restriction.

You can assign the same COR to more than one object. Objects with the same COR might be similar objects, such as two telephones, or different objects, such as a telephone and a trunk group.

To enhance your system security, you can:

- Assign a separate COR to incoming trunk groups and outgoing trunk groups, and then restrict calls between the two groups.
- Set appropriate calling party restrictions and Facility Restriction Levels (FRLs) to limit the calling permissions as much as possible.

Types of restrictions

Calling party restrictions

Calling party restrictions define the privileges for telephones that make outbound calls. If you do not need to restrict telephones that make outbound calls, assign a COR with the **Calling Party Restriction** field set to **none**.

You can use calling party restrictions for:

- Unrestricted telephones
- Trunk groups
- Terminating Extension Groups (TEGs)
- Uniform Call Distribution (UCD) groups
- Direct Department Calling (DDC) groups
- Data modules
- Attendant groups
- Individual attendant extensions

All-Toll restrictions and TAC-Toll restrictions

Toll restrictions prevent users from placing public network calls to certain toll-call numbers. You assign toll restrictions to outgoing trunk groups on the Trunk Group screen. You disable Trunk Access Code (TAC)-toll restrictions for specific outgoing trunk groups on the Trunk Group screen.

Origination restrictions

You can use origination restrictions to prohibit users from originating calls. These users can still receive calls.

Outward restrictions

You can use outward restrictions to prevent users from placing calls to the public network. These users can still place calls to other telephone users, to the attendant, and over tie trunks. If necessary, an attendant or an unrestricted telephone user can extend a call to an outside number for an outward-restricted telephone user.

Calls that come into a trunk are denied if the:

- **Calling Party Restriction** field on the Class of Restriction screen is set to **outward**
- Calls use the Automatic Alternate Routing (AAR) or the Automatic Route Selection (ARS) feature

Called party restrictions

Called party restrictions define the privileges for telephones that receive inbound calls. If you do not need to restrict telephones that receive inbound calls, assign a COR with the **Called Party Restriction** field set to **none**.

You can use called party restrictions for:

- Unrestricted telephones
- Trunk groups
- Terminating Extension Groups (TEGs)
- Uniform Call Distribution (UCD) groups
- Direct Department Calling (DDC) groups
- Data modules
- Attendant groups
- Individual attendant extensions

Even if the system redirects a call from one telephone to another, the system checks for called party restrictions only at the called telephone. For example, if a called telephone with no restrictions activates the Call Forwarding feature to a restricted telephone, the system still completes the call.

Inward restrictions

You can use inward restrictions to allow users to receive only internal calls. With inward restrictions, users at assigned telephones cannot receive:

- Public network calls
- Attendant originated calls
- Attendant extended calls

The system checks only the COR of the originally called telephone, unless you administer a three-way COR on conference calls and transfer calls. The system routes denied calls to:

- Intercept tone
- A recorded announcement
- The attendant, for Direct Inward Dialing (DID) calls

Manual terminating line restrictions

You can use manual terminating line restrictions to allow users to receive calls only from an attendant, or calls that an attendant extends. The system can redirect calls to a telephone with manual terminating line restrictions. The system checks only the COR of the originally called telephone.

The system routes the following calls to the attendant:

- Local central office (CO) calls
- Foreign exchange (FX) calls

The system redirects Direct Inward Dialing (DID) calls to:

- Intercept tone
- A recorded announcement
- The attendant

Public restrictions

Public restrictions prohibit users from receiving public network calls. The system routes denied calls to:

- Intercept tone
- A recorded announcement
- The attendant

Public restrictions still allow users to receive internal calls from other telephones, or calls that are extended from the attendant.

Termination restrictions

You can use termination restrictions to prohibit users from receiving any calls. These users can still originate calls. The system routes DID or Advanced Private-Line Termination calls to a recorded announcement or to the attendant.

Fully restricted service

With fully restricted service, users cannot make or receive public network calls. Users who have fully restricted service cannot use authorization codes to deactivate this feature.

COR-to-COR restrictions

You can restrict calls from one COR to another COR. You can use COR-to-COR calling restrictions to prohibit user access to specific telephones or specific trunk groups, such as CO trunk groups. Any or all trunk groups can be in a trunk-restriction COR. The system routes restricted calls to intercept tone.

Note:

COR-to-COR calling restrictions from a station to a trunk do not apply when Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or Uniform Dial Plan (UDP) is used to place the call. In these cases, use Facility Restriction Levels (FRLs) to block groups of users from accessing specific trunk groups.

Administering Class of Restriction

The following steps are part of the administration process for the Class of Restriction (COR) feature:

- Displaying administered CORs
- Setting up a COR
- Allowing users to change their own COR

This section describes:

- The screens that you use to administer the Class of Restriction feature
- Complete administration procedures for the Class of Restriction feature

Screens for administering Class of Restriction

Screen name	Purpose	Fields
Class of Restriction Information	List what CORs are administered on your system.	All
Class of Restriction	• Apply administration settings to all objects that share the same COR number. • Restrict the types of calls that a user can make and receive. • Identify what CORs can be service observed, or be a service observer.	All
Optional Features	Ensure that users can change their own COR without assistance from an administrator.	**Change COR by FAC**
Feature Access Code (FAC)	Assign a Feature Access Code (FAC) so that the user can change their own COR without assistance from an administrator.	**Change COR Access Code**
Feature-Related System Parameters	Assign a password that is required before a user can change their own COR.	**Password to Change COR by FAC**

Displaying administered CORs

To list what CORs are administered on your system:

1. Type **list cor**. Press **Enter**.

   The system displays the Class of Restriction Information screen (Figure 153: Class of Restriction Information screen on page 722).

Figure 153: Class of Restriction Information screen

```
list cor                                                    Page 1 of x
                        CLASS OF RESTRICTION INFORMATION

                    COR   COR Description

                     0
                     1
                     2
                     3
                     4
                     5
                     6
                     7
                     8
                     9
                    10     Supervisor observer
                    11
                    12
                    13
                    14
```

2. Click **Next** continually to see all the CORs.
3. After you review this information, press **Cancel**.

Setting up a COR

To set up a COR:

1. Type **change cor *n***, where ***n*** is the number of a specific COR. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 154: Class of Restriction screen, page 1 on page 723).

Figure 154: Class of Restriction screen, page 1

```
change cor 10                                                Page 1 of x
                              CLASS OF RESTRICTION

               COR Number: 10
          COR Description: Supervisor observer

                      FRL: 0                                    APLT? y
  Can Be Service Observed? n                Calling Party Restriction: none
Can Be A Service Observer? y                 Called Party Restriction: none
        Time of Day Chart: 1              Forced Entry of Account Codes? n
         Priority Queuing? n                      Direct Agent Calling? y
     Restriction Override: none              Facility Access Trunk Test? n
     Restricted Call List? n                      Can Change Coverage? n

            Access to MCT? y                  Fully Restricted Service? n
Group II Category For MFC: 7                  Hear VDN of Origin Annc.? n
         Send ANI for MFE? n                   Add/Remove Agent Skills? y
            MF ANI Prefix: ______             Automatic Charge Display? n
Hear System Music on Hold? y    PASTE (Display PBX Data on telephone)? n
                             Can Be Picked Up By Directed Call Pickup? n
                                        Can Use Directed Call Pickup? n
                                        Group Controlled Restriction: inactive
```

2. In the **COR Description** field, type a name for this COR. Assign a name for the COR that clearly reflects either the purpose or the members of the COR.
3. Complete all the applicable fields on page 1 of this screen. Specifically, you must:
   - Right-click the **Calling Party Restriction** field to see a list of options. Select an appropriate item from the list.
   - Right-click the **Called Party Restriction** field to see a list of options. Select an appropriate item from the list.
4. Press **Enter** to save your changes.
5. Click **Next** to see the next screen (Figure 155: Class of Restriction screen, page 2 on page 724).

Figure 155: Class of Restriction screen, page 2

```
change cor 10                                                Page 2 of 4
                              CLASS OF RESTRICTION

                      MF Incoming Call Trace: n
                Brazil Collect Call Blocking? n
                      Block Transfer Display? n
Block Exchanged Conference/Transfer Display? n
                      Remote Logout of Agent? n


                             Station Lock COR: 9
Outgoing Trunk Disconnect Timer (minutes):
```

6. Complete all the applicable fields on page 2 of this screen.
7. Press **Enter** to save your changes.
8. Click **Next** to see the next screen (Figure 156: Class of Restriction screen, page 3 on page 724).

   The numbers represent the available CORs. All fields default to **y**.

Figure 156: Class of Restriction screen, page 3

```
change cor 10                                                Page 3 of x
                              CLASS OF RESTRICTION


CALLING PERMISSION (Enter "y" to grant permission to call specified COR)

  0? y     12? y     24? y     36? y     48? y     60? y     72? y     84? y
  1? y     13? y     25? y     37? y     49? y     61? y     73? y     85? y
  2? y     14? y     26? y     38? y     50? y     62? y     74? y     86? y
  3? y     15? y     27? y     39? y     51? y     63? y     75? y     87? y
  4? y     16? y     28? y     40? y     52? y     64? y     76? y     88? y
  5? y     17? y     29? y     41? y     53? y     65? y     77? y     89? y
  6? y     18? y     30? y     42? y     54? y     66? y     78? y     90? y
  7? y     19? y     31? y     43? n     55? y     67? y     79? y     91? y
  8? y     20? y     32? y     44? y     56? y     68? y     80? y     92? y
  9? y     21? y     33? y     45? y     57? y     69? y     81? y     93? y
 10? y     22? y     34? y     46? y     58? y     70? y     82? y     94? y
 11? y     23? y     35? y     47? y     59? y     71? y     83? y     95? y
```

9. To restrict a user who is assigned this COR from calling someone in another COR, change the Calling Permission of the COR number to **n**.

   In this example, a user who is assigned COR 10 cannot call a user who is assigned COR 43.

10. Press **Enter** to save your changes.

11. Click **Next** to see the last screen (Figure 157: Class of Restriction screen, page 4 on page 725).

    The numbers represent the available CORs. All fields default to **y**. Complete this screen only if you set the **Can Be A Service Observer** field on page 1 to **y**. If the **Can Be A Service Observer** field is set to **n**, you can skip this screen.

    If a specified COR is set to **y**, but the **Can Be Service Observed** field on page 1 of that COR is set to **n**, that COR cannot be service observed.

Figure 157: Class of Restriction screen, page 4

```
change cor 10                                                  Page 4 of x
                              CLASS OF RESTRICTION


SERVICE OBSERVING PERMISSIONS
(Enter "y" to grant permission to service observe the specified COR)
  0? y      12? y     24? y     36? y     48? y     60? y     72? y     84? y
  1? y      13? y     25? y     37? y     49? y     61? y     73? y     85? y
  2? y      14? y     26? y     38? y     50? y     62? y     74? y     86? y
  3? y      15? y     27? y     39? y     51? y     63? y     75? y     87? y
  4? y      16? y     28? y     40? y     52? y     64? y     76? y     88? y
  5? y      17? y     29? y     41? y     53? y     65? y     77? y     89? y
  6? y      18? y     30? y     42? y     54? y     66? y     78? y     90? y
  7? y      19? n     31? y     43? y     55? y     67? y     79? y     91? y
  8? y      20? y     32? y     44? y     56? y     68? y     80? y     92? y
  9? y      21? y     33? y     45? y     57? y     69? y     81? y     93? y
 10? y      22? y     34? y     46? y     58? y     70? y     82? y     94? y
 11? y      23? y     35? y     47? y     59? y     71? y     83? y     95? y
```

12. To indicate what COR cannot be service observed, change the value of the COR number to **n**.

    In this example, a user who is assigned COR 10 cannot service observe a user who is assigned COR 19.

13. Press **Enter** to save your changes.

Allowing users to change their own COR

You can allow users to change their own COR from the telephone through a Feature Access Code (FAC). Users can change from the existing COR to any other COR. To restrict this feature, you can also require that users enter a password before the users can change their own COR.

Note:
Administrators can also allow users to change only between two predetermined CORs. For more information, see the "Station Lock" feature.

To allow users to change their own COR to any other COR, you must complete the following procedures:

- Assigning a FAC
- Assigning a password

Prerequisites

You must complete the following actions before you can allow users to change their own COR:

- On the Optional Features screen, ensure that the **Change COR by FAC** field is set to **y**. If this field is not set to **y**, users cannot change their own COR. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Assigning a FAC

To assign a Feature Access Code (FAC):

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 158: Feature Access Code (FAC) screen on page 727).

Figure 158: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 1 of x

                                FEATURE ACCESS CODE (FAC)

         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
                      Announcement Access Code: ____
                       Answer Back Access Code: ____
                         Attendant Access Code: ____
      Auto Alternate Routing (AAR) Access Code: ____
    Auto Route Selection (ARS) - Access Code 1: ____     Access Code 2: ____
                 Automatic Callback Activation: ____      Deactivation: ____
Call Forwarding Activation Busy/DA: ____   All: ____      Deactivation: ____
                         Call Park Access Code: ____
                       Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                  CDR Account Code Access Code: ____
                        Change COR Access Code: *55
                   Change Coverage Access Code: ____
                   Contact Closure   Open Code: ____       Close Code: ____
                   Contact Closure  Pulse Code: ____
```

2. In the **Change COR Access Code** field, type a FAC that conforms to your dial plan.
3. Press **Enter** to save your changes.
4. Ensure that you notify all users of the assigned FAC.

Assigning a password

To assign a password:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you see the **Password to Change COR by FAC** field (Figure 159: Feature-Related System Parameters screen on page 728).

Figure 159: Feature-Related System Parameters screen

```
change system-parameters features                              Page 10 of x
                        FEATURE-RELATED SYSTEM PARAMETERS

AUTOMATIC EXCLUSION PARAMETERS

                      Automatic Exclusion by COS? y
                 Automatic Exclusion Coverage/Hold? y
             Automatic Exclusion with Whisper Page? y

                    Password to Change COR by FAC: 12344321
```

3. In the **Password to Change COR by FAC** field, type a password.

   This field determines if Communication Manager requires the user to enter a password when the user tries to change the COR, and what that password is.

4. Press **Enter** to save your changes.
5. Ensure that you notify all users of the assigned password.

End-user procedures for Class of Restriction

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for the Class of Restriction feature:

To temporarily change your COR from your telephone through a Feature Access Code (FAC):

1. Dial the Change COR Access Code FAC.
2. Dial the password to change your COR.
3. Change your COR.

Reports for Class of Restriction

The following reports provide information about the Class of Restriction feature:

- None

Interactions for Class of Restriction

This section provides information about how the Class of Restriction feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of the Class of Restriction in any feature configuration.

- Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS)

  Termination and miscellaneous restrictions do not apply to AAR or ARS calls. AAR or ARS access to a trunk group overrides miscellaneous trunk restrictions.

- AAR or ARS Partitioning

  Use a COR to assign partition group numbers.

- Abbreviated Dialing

  The system does not check direct calls that are made from group lists. These lists are inaccessible to a user whose telephone is fully restricted. However, once a user makes a call from the Abbreviated Dialing group list, the system checks all subsequent transfer and conference attempts.

- Abbreviated Dialing Privileged Group Number List

  A telephone user with authorization to access an Abbreviated Dialing Privileged Group Number List can place calls to any number on that list. The system does not check COR assignments.

- Bridged Call Appearance

  A COR that is assigned to a telephone also applies to calls that originate from a bridged call appearance of that telephone.

- Call Coverage

  Users who are restricted from calls can still receive calls that Call Coverage directs to these users. When a call goes to coverage, the system uses the restrictions of the called party, not of the covering party. When a call is redirected to coverage, the system does not check the COR of the covering party. If the COR of the covering party is fully restricted, the system cannot complete the call.

- Call Forwarding All Calls

  If a COR restricts a call between the forwarding extension and the forwarded-to extensions, Call Forwarding is denied. The system always checks when Call Forwarding is activated, but not when the system forwards a call.

- Call Vectoring

  When the system directs a call to a vector directory number (VDN), the system compares the COR of the caller and the VDN. This comparison determines if the caller can access the associated call vector.

- Centralized Attendant Service (CAS)

  Since COR information is not passed over release link trunks (RLT), fully restricted service allows all CAS calls. Therefore, CAS allows a public network call to be completed to a fully restricted telephone.

- Class of Restriction Display to the Attendant

  The attendant can display the COR for each telephone.

- Class of Service (COS)

  In some cases, the COS of a user can override a COR. For more information, see the **Trk-to-Trk Restriction Override** field in the "Class of Service" feature description.

- Controlled Restriction

  Restrictions that you assign through Controlled Restriction override any COR restrictions.

- Distributed Communications System (DCS)

  Fully restricted service allows all DCS calls. DCS can allow a public network call to be completed to a fully restricted telephone.

- Emergency Access to Attendant

  A COR does not restrict Emergency Access to Attendant calls.

- Fully Restricted Service

  Do not assign fully restricted service to a telephone that has these features or conditions:

  - Abbreviated Dialing
  - Bridged Call Appearance
  - Attendant telephones
  - Night Service telephones
  - Telephones that are Call Coverage or Send All Calls points
  - Telephones that are Call Forward destinations
  - Telephones that are Call Pickup points

- Hunt Groups

  The system checks the COR that is assigned to a hunt group on calls that are redirected by the Direct Department Calling (DDC) or Uniform Call Distribution (UCD) of the hunt group. If the COR of the hunt group does not have fully restricted service, extensions in the hunt group can receive calls from the public network.

- Night Service and Night Station Trunk Answer From Any Station

  Both the Night Service feature and the Night Station Trunk Answer From Any Station feature override:

  - Inward restrictions
  - Manual terminating line restrictions

  - Public restrictions

- Personal Central Office Line (PCOL)

  Do not assign fully restricted service to users who have a personal central office line. If you do, you are paying for a CO line that no one can use.

- Power Failure Transfer

  All authorization features are bypassed when the system is in emergency transfer mode.

- Privileged System Number List

  A telephone user with authorization to access a Privileged System Number List can place calls to any number on that list. The system does not check COR assignments.

- Remote Access

  If the user enters a barrier code during connection to remote access, the system uses the COR that is associated with that code for authorization checks. If remote access does not require a barrier code, the system uses the COR of the default barrier code. Remote access can require an authorization code instead of, or in addition to, the barrier code. If the system requires an authorization code, the COR of the authorization code overrides the COR of the barrier code.

- Tie trunk access

  The system can complete incoming dial-repeating tie trunk calls directly to an inward-restricted telephone or a public-restricted telephone. An attendant cannot extend incoming dial-repeating tie trunk calls to an inward-restricted telephone.

- Transfer

  When you administer a three-way conference, a user cannot transfer incoming trunk calls to an inward-restricted telephone. Transferred calls are subject to three-way COR Checking restrictions.

  A user can transfer incoming trunk calls from an unrestricted telephone to an inward-restricted telephone or a public-restricted telephone. However, you must override the three-way conference COR.

Class of Service

Use the Class of Service (COS) feature to allow or deny user access to some system features.

Detailed description of Class of Service

This section provides a detailed description of the Class of Service (COS) feature.

Use the COS feature to allow or deny user access to some system features, such as:

- Automatic Callback
- Call Forwarding
- Data Privacy
- Trunk-to-Trunk Transfer Override
- QSIG Call Offer Originations
- Contact Closure Activation
- Console Permission

Use the Class of Restriction (COR) feature, instead of COS, to define the restrictions that apply when a user places or receives a call. For more information, see the "Class of Restriction" feature.

COS does not apply to trunk groups, except for the Remote Access feature. For more information, see the "Remote Access" feature.

Administering Class of Service

The following steps are part of the administration process for the Class of Service feature (COS):

- Defining COS for your system
- Assigning a COS

This section describes:

- Any prerequisites for administering the Class of Service feature

- The screens that you use to administer the Class of Service feature
- Complete administration procedures for the Class of Service feature

Prerequisites for administering Class of Service

You must complete the following actions before you can administer the Class of Service feature:

- None

Screens for administering Class of Service

Screen name	Purpose	Fields
Attendant Console	Assign Class of Service (COS) for the attendant.	**COS**
Class of Service	Define COS for your system.	All
Console-Parameters	Assign COS for all the attendant consoles.	**COS**
Data Modules	Assign COS for a data module.	**COS**
Remote Access	Assign the COS associated with the barrier code of the Remote Access extension.	**COS**
Station	Assign COS for a user.	**COS**

Defining COS for your system

To define COS for your system:

1. Type **`change cos`**. Press **Enter**.

   The system displays the Class of Service screen (Figure 160: Class of Service screen on page 735).

Figure 160: Class of Service screen

```
change cos                                                    Page 1 of 1
                          CLASS OF SERVICE

                                  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

   Auto Callback                  n y y n y n y n y n  y  n  y  n  y  n
   Call Fwd-All Calls             n y n y y n n y y n  n  y  y  n  n  y
   Data Privacy                   n y n n n y y y y n  n  n  n  y  y  y
   Priority Calling               n y n n n n n n n y  y  y  y  y  y  y
   Console Permissions            n n n n n n n n n n  n  n  n  n  n  n
   Off-hook Alert                 n n n n n n n n n n  n  n  n  n  n  n
   Client Room                    n n n n n n n n n n  n  n  n  n  n  n
   Restrict Call Fwd-Off Net      n y y y y y y y y y  y  y  y  y  y  y
   Call Forward Busy/DA           n n n n n n n n n n  n  n  n  n  n  n
   Personal Station Access (PSA)  n n n n n n n n n n  n  n  n  n  n  n
   Extended Forwarding All        n n n n n n n n n n  n  n  n  n  n  n
   Extended Forwarding B/DA       n n n n n n n n n n  n  n  n  n  n  n
   Trk-to-Trk Restriction Override n n n n n n n n n n  n  n  n  n  n  n
   QSIG Call Offer Originations   n n n n n n n n n n  n  n  n  n  n  n
   Automatic Exclusion            n n n n n n n n n n  n  n  n  n  n  n
```

2. Perform one of the following actions for any, or all, of the COSs, which are numbered zero through 15:
   - If you want to activate the feature for the COS, type **y**.
   - If you do not want to activate the feature for the COS, type **n**.
3. Press **Enter** to save your changes.

Descriptions of the COS features

The system displays some features only if the associated feature is set to **y** on the Feature-Related System Parameters screen. The information on the Class of Service screen that you display can differ from the information shown in the Figure 160: Class of Service screen.

- **Automatic Callback**

  Allows a user to request Automatic Callback. For more information, see the "Automatic Callback" feature.

- **Automatic Exclusion**

  Allows a user to automatically activate Privacy Exclusion when the user goes off hook at a telephone that has an assigned Exclusion button.

  If you set this field to **n**, the user can use manual exclusion when the user presses the Exclusion button, either before the user dials a call or during a call.

  The system displays this field when the **Automatic Exclusion by COS** field on the Feature-Related System Parameters screen is set to **y.**

- **Call Forwarding All Calls**

  Allows a user to forward all calls to any extension. For more information, see the "Call Forwarding" feature.

- **Call Forwarding Busy/DA**

  Allows the system to forward calls when the user is active on a call, or does not answer a call. For more information, see the "Call Forwarding" feature.

- **Client Room**

  Allows users to access the Check-In, Check-Out, Room Change/Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message-waiting notification.

  You can administer a COS for Client Room only when you have Hospitality Services and a Property Management System (PMS) interface. See the *GuestWorks® and DEFINITY® Systems Technician Handbook for Hospitality Installations* for more information.

- **Console Permissions**

  Console Permissions allows a user who has a multiappearance telephone, to control the same features that the attendant controls. You might assign this permission to front-desk personnel in a hotel or a motel, or to a call center supervisor. With console permission, a user can:

  - Activate Automatic Wakeup for another extension
  - Activate and deactivate controlled restrictions for another extension, or group of extensions
  - Activate and deactivate Do Not Disturb for another extension, or group of extensions
  - Activate Call Forwarding for another extension
  - Add and remove agent skills
  - Record integrated announcements

- **Data Privacy**

  Allows a user to enter a Feature Access Code (FAC) to protect a data call from interruption by any of the system override or ringing features. For more information, see the Privacy feature.

- **Extended Forwarding All**

  Allows a user to use Call Forwarding All Calls from an off-site telephone.

  You can change a COS to **y,** only if the **Extended Cvg/Fwd Admin** field on the System Parameters Customer-Options screen is set to **y**. For more information, see the "Extended User Administration of Redirected Calls" feature.

- **Extended Forwarding B/DA**

  Allows a user to activate Call Forwarding from an off-site telephone.

  You can change a COS to **y** only if the **Extended Cvg/Fwd Admin** field on the System Parameters Customer-Options screen is set to **y**. For more information, see the "Extended User Administration of Redirected Calls" feature.

- **Off-Hook Alert**

  You can change a COS to **y**, only if either the **Hospitality (Basic)** field or the **Emergency Access to Attendant** field on the System Parameters Customer-Options screen is set to **y**. For more information, see the Emergency Access to Attendant feature.

- **Personal Station Access (PSA)**

  Allows a user to use a FAC to associate a telephone to the extension that is assigned to the user.

  You must set this field to **n** for virtual telephones.

  You can change this field to **y**, only if the **Personal Station Access (PSA)** field on the Optional Features screen is set to **y**. For more information, see the "Personal Station Access" feature.

- **Priority Calling**

  Allows a user to dial a FAC to originate a priority call. For more information, see the "Priority Calling" feature.

- **QSIG Call Offer Originations**

  Allows a user to invoke QSIG Call Offer services. For more information, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

- **Restrict Call Fwd-Off Net**

  If you set this field to **y**, a user cannot forward calls to the public network.

  For security reasons, type **y** in the **Restrict Call Fwd-Off Net** field for all COS, except those that you use for special circumstances. For more information, see the "Call Forwarding" feature.

- **Trk-to-Trk Restriction Override**

SECURITY ALERT:
You increase the risk of toll fraud if you allow users to perform trunk-to-trunk transfers.

Allows a user to override any system COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-trunk transfer operation for a user with this COS. For more information, see the Transfer feature.

From Communication Manager, Release 3.0, the Class of Service screen has a new page, and a new field **VIP Caller**. The **VIP Caller** field enables automatic priority calling to extensions when it is marked **y** on the Class of Service screen. The default for this field is **n**.

For more information on impact of this field on Priority Calling, see the feature description on Priority Calling.

Figure 161: Class of Service screen

```
change cos                                                    Page 2 of x
                          CLASS OF SERVICE

                                  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

   VIP Caller                     y y y y y y y y y y  y  y  y  y  y  y
```

Assigning a COS

To assign a COS:

1. Change the **COS** field on any of the following screens:
   - Attendant Console
   - Console-Parameters
   - Data Modules
   - Remote Access
   - Station
2. Press **Enter** to save your changes.

Considerations for Class of Service

This section provides information about how the Class of Service feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Class of Service under all conditions. The following considerations apply to Class of Service:

- Hunt Groups

  Many Hunt Groups have a COS of 1. Ensure that you do not cause unintended restrictions for Hunt Groups when you administer COS 1.

Interactions for Class of Service

This section provides information about how the Class of Service feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Class of Service in any feature configuration.

- Class of Service (COS) controls use of the following features and capabilities:
  - Automatic Callback
  - Automatic Exclusion
  - Call Forwarding
  - Call Forward Busy/Don’t Answer
  - Client room
  - Console permission
  - Data Privacy
  - Extended Forwarding All
  - Extended Forwarding Busy/Don’t Answer
  - Off-hook alert
  - Personal Station Access
  - Priority Calling
  - QSIG Call Offer Originations
  - Restrict Call Forwarding Off-Net
  - Trunk-to-Trunk Transfer Restriction Override

Conference

Use the Conference feature, with the associated Conf button, to create a conference without the assistance of an attendant.

Detailed description of Conference

This section provides a detailed description of the Conference feature.

Use the Conference feature, with the associated **conf** button, to create a conference without the assistance of an attendant.

A user with a multiple appearance telephone with a **conf** button can create a conference with as many as six participants.

A user with a single-line telephone can create a conference with as many as three participants. Each of these three participants can then add another participant. Thus, a user who has a single-line telephone can create a conference call with as many as six participants.

Conference and DCP, hybrid, IP, wireless, and ISDN-BRI telephones

A user with a Digital Communications Protocol (DCP), hybrid, IP, wireless, or ISDN-BRI telephones can use the Conference feature for a call on hold when:

- Only one call is on hold
- No call appearances are active
- An available call appearance exists for the conference call

If more than one call is on hold, the user must make a call active to start a conference. If the user presses the **conf** button when two or more calls are on hold, the system ignores the conference request from the user.

If the user has an active call, and also has calls on hold, the system includes the active call in the conference when the user presses the **conf** button.

Meet-me Conference

The Meet-me Conference feature allows users to set up a dial-in conference of up to six parties. The Meet-me Conference feature uses Call Vectoring to process the setup of the conference call. For more information, see the "Meet Me Conference" feature.

The Conference feature supports the following capabilities:

- Conference/Transfer Toggle/Swap
- No Dial Tone Conferencing
- No Hold Conference
- Select Line Appearance Conferencing
- Selective Conference Party Display, Drop, and Mute

Conference/Transfer Toggle/Swap

A user who sets up a conference call can use the Conference/Transfer Toggle/Swap capability to talk back and forth between two users before the user connects all the participants to the conference call. The display also toggles between the two parties.The Conference/Transfer Toggle/Swap capability is unavailable on attendant consoles.

The user uses an administered feature button, **togle-swap**, for the Conference/Transfer Toggle/Swap capability

No Dial Tone Conferencing

This capability eliminates the dial tone that the user usually hears while the user adds the participants to the conference call. A user uses the No Dial Tone Conferencing capability to add existing calls to a conference call. The user does not need to select a line appearance if there is someone on hold, or if the system is alerting a line appearance.

For example, a user places a call on hold, and talks to another party. When the user presses the **conf** button and then presses the button of the call on hold, the party on hold joins the conference without hearing a dial tone.

No Hold Conference

When a user who is active on a call creates a conference call, the user can use the No Hold Conference capability to add another participant to a conference call, while the user continues a conversation with the participant on the call that is currently active. When the user calls the new participant, the new participant automatically joins the conference when the new participant answers the call.

For example, a user presses the administered **no-hold-conf** feature button and then dials an extension. The party that answers the call automatically joins the conference.

If the called user does not answer the call within the time that you specify in the **No Hold Conference Timeout** field on the Feature-Related System Parameters screen, the system deactivates the No Hold Conference capability for the call.

Users with multiline digital telephones can use the No Hold Conference capability.

Select Line Appearance Conferencing

If a user is at a call on line B, and another line is on hold or an incoming call alerts at line A, the user can press the **conf** button to bridge the calls together. If the user uses the select line appearance capability, the user can press a line appearance button to complete a conference instead of pressing the **conf** button a second time.

Selective Conference Party Display, Drop, and Mute

A user who has a digital telephone with a display, or an attendant with an attendant console, can use the Selective Conference Party Display, Drop, and Mute capability to identify the participants on a call.

The conference prompts that the system displays are based on the user Class of Restriction (COR). The display prompts are based on the user COR, independent of the select line appearance conferencing and the No Dial Tone Conferencing capability. The display messages vary depending on the activation of the various Conference capabilities. The user COR controls the display of any additional information.

A user presses the administered conf-dsp feature button to scroll through the telephone numbers and names of the participants on the call. The telephone numbers of the participants are always available, although the names of the participants are sometimes unavailable. When the system displays the telephone number of a participant, the user can either press the administered fe-mute feature button to place the participant on mute, or the user can press the **drop** button to drop the participant from the call.

The ability to place a call participant on mute is useful when that participant has a noisy trunk line because of a cell phone, music-on-hold, or background noise. The Selective Conference Party Mute capability applies only to trunk lines, and a user can mute only one trunk line on a conference call.

Click to Conference

For the Click to Conference feature, make sure the **Enhanced Conferencing** field is set to y on the Optional Features screen.

Note:
For more information on how to administer the Click to Conference feature, see:
Installing, Administering, Maintaining, and Upgrading Avaya Aura™ SIP Enablement Services, 03-600768
SIP Softphone Release 2.1 Quick Setup Guide, 16-600974

Administering Conference

The following steps are part of the administration process for the Conference feature:

- Assigning the togle-mute feature button
- Assigning feature buttons

This section describes:

- Any prerequisites for administering the Conference feature
- The screens that you use to administer the Conference feature
- Complete administration procedures for the Conference feature

Prerequisites for administering the Conference feature

You must complete the following actions before you can administer the Conference feature:

Administer the Feature-Related System Parameters screen to support the Conference feature on your system.

To administer the Feature-Related System Parameters screen:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen

2. Click **Next** until you see the **Public Network Trunks on Conference Call** field (Figure 162: Feature-Related System Parameters screen on page 745).

Figure 162: Feature-Related System Parameters screen

```
change system-parameters features                              Page   5 of  13
                     FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5              Auto Start? n
    Conference Parties with Public Network Trunks: 6               Auto Hold? y
 Conference Parties without Public Network Trunks: 6          Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180          Bridging Tone? n
                  Short Interdigit Timer (seconds): 3         Conference Tone? y
               Unanswered DID Call Timer (seconds):             Intrusion Tone? n
               Line Intercept Tone Timer (seconds): 30      Special Dial Tone? n
                  Long Hold Recall Timer (seconds): 0     Mode Code Interface? n
                       Reset Shift Timer (seconds): 0
    Station Call Transfer Recall Timer (seconds): 0
                              DID Busy Treatment: tone
       Invalid Number Dialed Intercept Treatment: tone
              Allow AAR/ARS Access from DID/DIOD? n
                Allow ANI Restriction on AAR/ARS? n
     Use Trunk COR for Outgoing Trunk Disconnect? n
                  7405ND Numeric Terminal Display? y                  7434ND? n
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                       Attendant Originated Calls: external
```

3. In the **Public Network Trunks on Conference Call** field, type the maximum number of participants with public network trunks that you want to participate in a conference call. The valid entries for this field are **0** through **5**.

   Type **0** if you do not want any public network trunks to participant in a conference call. If you type **0** in this field, the **Conference Parties with Public Network Trunks** field does not appear on the Feature-Related System Parameters screen.

4. In the **Conference Parties without Public Network Trunks** field, type the maximum number of participants without public network trunks that you want to participate in a conference call. The valid entries for this field are **3** through **5**.

5. In the **Conference Tone** field, perform one of the following actions:

   - If you want the participants in a conference call to hear the conference tone if there are three or more participants on a conference call, type **y**.
   - If you do not want conference participants to hear the conference tone if there are three or more participants on a conference call, type **n**.

6. Click **Next** until you see the **No Dial Tone Conferencing** field (Figure 163: Feature-Related System Parameters screen).

Figure 163: Feature-Related System Parameters screen

```
change system-parameters features                              Page   6 of  13
                        FEATURE-RELATED SYSTEM PARAMETERS

CONFERENCE/TRANSFER

               Abort Transfer? n                 No Dial Tone Conferencing? n
       Transfer Upon Hang-Up? n       Select Line Appearance Conferencing? n
Abort Conference Upon Hang-Up? n                                   Unhold? n
   No Hold Conference Timeout: 60

ANALOG BUSY AUTO CALLBACK
               Without Flash? n



AUDIX ONE-STEP RECORDING
                            Recording Delay Timer (msec): 500
Apply Ready Indication Tone To Which Parties In The Call? all
  Interval For Applying Periodic Alerting Tone (seconds): 15
```

7. In the **No Dial Tone Conferencing** field, take one of the following actions:
   - If you want a user who is on hold to hear dial tone while the conference owner adds another conference participant, type **n**.
   - If you do not want a user who is on hold to hear dial tone while the conference owner adds another conference participant, type **y**.
8. In the **Select Line Appearance Conferencing** field, take one of the following actions
   - Type **y** to activate select line appearance conferencing.
   - Type **n** to deactivate select line appearance conferencing.
9. In the **Abort Conference on Hang-up** field, perform one of the following actions:
   - If you want the user to stop a conference call if the user hangs up the telephone before the conference call is complete, type **y**.
   - If you do not want the user to stop a conference call when the user hangs up the telephone before the conference call is complete, type **n**.
10. In the **No Hold Conference Timeout** field, type the number of seconds that you want the system to wait while a user uses the No Hold Conference capability to add a participant to a conference call. Note that you must set the **Answer Supervision** field on the Trunk Group screen to fewer seconds than the seconds in the **No Hold Conference Timeout** field.
11. Press **Enter** to save your changes.

Screens for administering Conference

Screen name	Purpose	Fields
Attendant Console	Assign **conf-dsp**, **fe-mute**, and **togle-swap** feature buttons to an attendant console.	Any available button field in the **Feature Button Assignments** area
Feature-Related System Parameters	Allow users of DCP, hybrid, IP, wireless, or ISDN-BRI telephones to "abort the conference operation when they hang up."	**Abort Conference Upon Hang-Up**
	Specify that the system generate a conference tone.	**Conference Tone**
	Specify the maximum number of participants in a conference call when any of the participants uses a public network trunk.	**Conference Parties With Public Network Trunks**
	Specify the maximum number of participants on a conference call when none of the participants uses a public network trunk.	**Conference Parties Without Public Network Trunks**
	Specify the number of seconds before the system deactivates the No Hold Conference capability for a call.	**No Hold Conference Timeout**
	Specify that a user who is on hold hears dial tone while the conference owner adds another conference participant.	**No Dial Tone Conferencing**
	Specify that the user can use the line appearance rather than the Conf button to include a call in a conference.	**Select Line Appearance Conferencing**
Station	Assign **conf-dsp**, **fe-mute**, **no-hold-conf**, and **togle-swap** feature buttons to a user telephone.	Any available button field in the **Button Assignments** area

Assigning the togle-mute feature button

To assign the **togle-mute** feature button to a user telephone:

1. Type **change station *n***, where ***n*** is the extension to which you want to assign the Conference/Transfer Toggle/Swap capability. Press **Enter**.

   The system displays the Station screen for the extension that you requested.

2. Click **Next** until you see the **Button Assignments** area (Figure 164: Station screen on page 748).

Figure 164: Station screen

```
change station 20001                                        Page   3 of 4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                        Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          5:togle-swap
 2: call-appr                          6:
 3: call-appr                          7:
 4:                                    8:
```

3. In the **Button Assignments** area, type **togle-swap** next to the button that you want the user to use for the Conference/Transfer Toggle/Swap capability.
4. Press **Enter** to save your changes.

Assigning feature buttons

Prerequisites

You must complete the following actions before you can assign the **conf-dsp**, **fe-mute**, and **no-hold-conf** feature buttons:

- On the Optional Features screen, verify that the **Enhanced Conferencing?** field is set to **y**, if you want to use the Selective Conference Party Display, Drop, and Mute capability and the No Hold Conference capability on your system. If the **Enhanced Conferencing?** field is set to **n**, your system is not enabled for the Selective Conference Party Display, Drop, and Mute capability. Contact your Avaya representative for assistance before you continue with this procedure.

  To view the Optional Features screen, type **display system-parameters customer-options**. Press **Enter**.

- Assign a COR for the Selective Conference Party Display, Drop, and Mute capability.

To Assign a COR for the Selective Conference Party Display, Drop, and Mute capability:

1. Type **change COR *n***, where ***n*** is the number of the COR to which you want to assign the Selective Conference Party Display, Drop, and Mute capability. Press **Enter**.

   The system displays the Class of Restriction screen.

2. Click **Next** until you see the **Block Enhanced Conference/Transfer Displays?** field (Figure 165: Class of Restriction screen on page 749).

Figure 165: Class of Restriction screen

```
change cor 10                                                Page 2 of 4
                          CLASS OF RESTRICTION

                     MF Incoming Call Trace? n
                Brazil Collect Call Blocking? n
                     Block Transfer Display? n
Block Enhanced Conference/Transfer Displays? y
                     Remote Logout of Agent? n

                              Station Lock COR: 10
  Outgoing Trunk Disconnect Timer (minutes):
```

3. In the **Block Enhanced Conference/Transfer Displays?** field, perform one of the following actions:

   - If you want the system to block all the enhanced conference/transfer display messages except "Transfer Completed" for a user or an attendant, type **y**.
   - If you do not want the system to block all the enhanced conference/transfer display messages except "Transfer Completed" for a user or an attendant, type **n**.

To assign the conf-dsp, fe-mute, and no-hold-conf feature buttons, you must complete the following procedures:

- Assign the conf-dsp, fe-mute, and no-hold-conf feature buttons to a user.
- Assign the conf-dsp and fe-mute feature buttons to an attendant.

Assigning feature buttons to a user

To assign the **conf-dsp**, **fe-mute**, and **no-hold-conf** feature buttons to a user telephone:

1. Type **change station *n***, where ***n*** is the telephone number of the extension to which you want to assign the following capabilities:
   - Conference Display
   - Selective Conference Party Display, Drop, and Mute
   - No-Hold Conference

   Press **Enter**.

   The system displays the Station screen for the extension that you requested.
2. Click **Next** until you see the **Button Assignments** area (Figure 166: Station screen on page 750).

Figure 166: Station screen

```
change station 20001                                        Page   3 of 4
                                    STATION
 SITE DATA
      Room:                                          Headset? n
      Jack:                                          Speaker? n
     Cable:                                         Mounting: d
     Floor:                                     Cord Length: 0
  Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          5:togle-swap
 2: call-appr                          6:conf-dsp
 3: call-appr                          7:fe-mute
 4:                                    8:no-hold-conf
```

3. In the **Button Assignments** area, perform the following actions:
   - Type **conf-dsp** next to the button that you want the user to use for the Conference Display capability.
   - Type **fe-mute** next to the button that you want the user to use for the Selective Conference Party Display, Drop, and Mute capability.
   - Type **no-hold-conf** next to the button that you want the user to use for the No-Hold Conference capability.

4. Press **Enter** to save your changes.

Assigning feature buttons to an attendant

To assign the **conf-dsp** and **fe-mute** feature buttons to an attendant console:

1. Type **change attendant *n***, where ***n*** is the number of the attendant console to which you want to assign the Conference Display capability, and the Selective Conference Party Display, Drop, and Mute capability. Press **Enter**.

   The system displays the Attendant Console screen for the attendant that you requested.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 167: Attendant Console screen on page 751).

Figure 167: Attendant Console screen

```
change attendant 1                                          Page   3 of 4
                              ATTENDANT CONSOLE

FEATURE BUTTON ASSIGNMENTS

 1: split                                13: conf-dsp
 2: dn-dst                               14: fe-mute
 3: split-swap                           15:
 4:                                      16:
 5:                                      17:
 6: hold                                 18:
 7: serial-cal                           19: forced-rel
 8: verify                               20:
 9: intrusion                            21:
10:                                      22:
11:                                      23: night-serv
12:                                      24: pos-busy
```

3. In the **Feature Button Assignments** area, perform the following actions:
   - Type **conf-dsp** next to the button that you want the attendant to use for the Conference Display capability.
   - Type **fe-mute** next to the button that you want the attendant to use for the Selective Conference Party Display, Drop, and Mute capability.
4. Press **Enter** to save your changes.

End-user procedures for Conference

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Conference:

- Displaying the participants on a conference call

Displaying the participants on a conference call

Users of a digital telephone and attendants at an attendant console can use the Selective Conference Party Display, Drop, and Mute capability to display information about the participants on a call. When the system displays the information about a participant on a call, a user can drop a participant from the conference call or place a participant on mute.

To display the participants on a conference call:

1. Press the conference display feature button to place the station or the console in the conference display mode.
2. Press the conference display feature button repeatedly to scroll through the telephone numbers and names of each participant on the call. The telephone number of a participant is always available. The name of a participant might be unavailable.
3. To drop the participant that the system displays, press the Drop button.

   This action is useful during a conference call when a user tries to add a participant that does not answer and the call goes to voice mail.
4. To place the participant that the system displays on mute, press the fe-mute button.

   The remaining participants on the conference call cannot hear the participant who is on mute. A user or attendant can use the fe-mute button to place only one participant on mute, and that participant must be on a trunk call.

   This ability to place a conference participant on hold is useful during conference calls when a participant puts the conference call on hold and the system plays music-on-hold to the remaining participants on the conference call.

CAUTION:
If a user quickly scrolls through the display information repeatedly, the system might take the telephone out of service. If the system takes the telephone out of service, the system resets the telephone, and drops the user from the call.

Considerations for Conference

This section provides information about how the Conference feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Conference under all conditions. The following considerations apply to Conference:

- Trunk-to-Trunk Connections

  If you do not allow trunk-to-trunk connections on your system, the system drops all conference participants when:

  — A user hangs up.

  — All the other participant connect to the conference through trunk lines.

- Loss Plan on Conference Calls

  The end-to-end total loss for multiparty conference calls that is administered on the Location Parameters screen is not always applied to a specific call. The loss applied to a three-party conference call, for example, is calculated by adding the fixed pairwise loss for each pair of ports to the value for two-party loss shown on the Location Parameters screen. If this total is less than the end-to-end total loss value configured for a three-party conference, calculate the difference, and divide the difference by 2. Add 1 to this figure, and the result is the amount of loss applied to the call.

Interactions for Conference

This section provides information about how the Conference feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Conference in any feature configuration.

- Bridged Call Appearance

  A user can use a bridged call appearance to make a conference call.

  A bridged appearance can bridge onto a conference call if that action does not cause the number of participants on the conference call to exceed six participants.

- Call Vectoring

  A call to a Vector Directory Number (VDN) can be included as a party in a conference call only after vector processing terminates for that call, for example, after a successful route-to command.

- Call Waiting

  When a user on an analog single-line telephone activates the Call Wait feature, and the user creates a conference call, the Call Wait feature does not function while the user is on the conference call.

- Class of Restriction (COR)

  If the **Restriction Override** field on the Class of Restriction screen is set to **all**, the system compares the COR of the participant who controls the conference call with the COR of a new conference participant. The system compares the COR of the participant who controls the conference call with the COR of a new conference participant before the system adds the participant to the conference call. The system does not compare the COR of the new participant with the CORs of the other conference participants.

  If the COR of the user who controls the conference call allows the override of inward call restrictions, the system compares the COR of the user who controls the conference call with the COR of a new conference participant. The system compares the COR of the user who controls the conference call with the COR of a new conference participant before the system adds the new participant to the conference call. The system does not compare the COR of the new participant with the CORs of the other conference participants.

- Emergency Access to an Attendant

  A user cannot make an Emergency-Access-to-an-Attendant call a participant in conference call.

- Trunk-to-Trunk Transfer

  The system does not recognize the Conference button or the Transfer button when a user dials enough digits for the system to route a call, and the system can route the call differently if the user dials more digits. The user must be a user of a multifunction telephone, for example a BRI telephone, a digital telephone, or a hybrid telephone.

  If the user wants the system to route the call based on the digits that the user has already dialed, the user must not dial any digits for three seconds, or the user must dial a pound sign (#). The system then recognizes the Conference button or the Transfer button and completes the call.

- VDN in a Coverage Path

  Calls in an established conference do not cover to a vector directory number (VDN).

  Once a call covers to a VDN, a conference cannot be established until the call is delivered to an extension and vector processing ends.

Co-resident DEFINITY LAN Gateway

Use the Co-resident DEFINITY LAN Gateway (DLG) feature to provide the functionality of the Adjunct/Switch Application Interface (ASAI), with the use of an Ethernet transport instead of the traditional Basic Rate Interface (BRI) transport.

Detailed description of Co-resident DEFINITY LAN Gateway

This section provides a detailed description of the Co-resident DEFINITY LAN Gateway (DLG) feature.

Co-resident DEFINITY LAN Gateway is a software application that is part of Avaya MultiVantage™ Communications Applications on the server that is running Communication Manager. In the S8300 Server with a G700 Media Gateway, Ethernet connectivity is provided through the processor.

The DEFINITY LAN Gateway software enables communications between TCP/IP clients and Communication Manager call processing. The DLG application software:

- Routes internetwork messages from one protocol to another, for example, ISDN to TCP/IP
- Bridges all Adjunct/Switch Application Interface (ASAI) message traffic by way of a TCP/IP tunnel protocol

In previous configurations, a DEFINITY LAN gateway (DLG) was connected externally on a separate TN801 MAPD circuit pack. The DLG application is now packaged internally, where the application co-resides with the Communication Manager software. The internally packaged DLG is referred to as the Co-resident DLG. Co-resident DLG is supported on all Communication Manager platforms 2.1 or later. However, it is not supported with the S8700 with G700 configuration.

Co-resident DLG provides the functionality of the Adjunct/Switch Application Interface (ASAI), with the use of an Ethernet transport instead of a Basic Rate Interface (BRI) transport.

How Co-resident DLG works

1. DLG listens for client connections over a well-known TCP port (5678) at a specified IP address.
2. The client connects to TCP port 5678 at the IP address to receive the services of the DLG.
3. The client exchanges TCP Tunnel Protocol messages with the DLG to request a connection to a specific Computer Telephony Integration (CTI) link.

4. DLG authenticates the client based on the administration of the client and then establishes or refuses the connection.
5. Once the connection is established, the actual ASAI layer 3 messages are passed transparently through the DLG. Each TCP connection to the DLG has a one-to-one correspondence with a CTI link.

Administering Co-resident DEFINITY LAN Gateway

This section describes:

- Any prerequisites for administering the Co-resident DEFINITY LAN Gateway feature
- The screens that you use to administer the Co-resident DEFINITY LAN Gateway feature

Prerequisites for administering Co-resident DEFINITY LAN Gateway

You must complete the following actions before you can administer the Co-resident DEFINITY LAN Gateway feature:

With the TN799 C-LAN circuit pack as the Ethernet Interface

- View the Optional Features screen. Ensure that the **ASAI Link Core Capabilities** field, the **Computer Telephony Adjunct Links** field, or both fields are set to **y**, and that the **Co-Res DEFINITY LAN Gateway** field is set to **y**. If these fields are set to **n**, your system is not enabled for the Co-resident DEFINITY LAN Gateway feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- View the IP Node Names screen. Ensure that a node name is associated with the C-LAN. If a node name is not associated with the C-LAN, add a node name.

  To view the IP Node Names screen, type **`display node-names ip`**. To add a node name, type **`change node-names ip`**. Press **Enter**.

- View the IP Interfaces screen. Ensure that a C-LAN is administered, and the Ethernet port for the C-LAN is enabled. If a C-LAN is not listed, add a C-LAN.

  To view the IP Interfaces screen, type **`display ip-interfaces`**. To add a C-LAN, type **`add ip-interface next`**. Press **Enter**.

- View the Data Modules screen. Ensure that the Ethernet port on the C-LAN is administered. If an Ethernet port on the C-LAN is administered, the **Service Type** field is set to **Ethernet**, and the **Port** field is set to port **17** on the TN799. If the Ethernet port is not listed, add an Ethernet port.

  To view the Data Modules screen, type **`list data-modules`**. To add an Ethernet port, type **`add data-module next`**. Press **Enter**.

With the TN2314 circuit pack as the Ethernet Interface

- View the Optional Features screen, and ensure that the **ASAI Link Core Capabilities** field, the **Computer Telephony Adjunct Links** field, or both fields, are set to **y**. Click **Next** until you see the **Processor Ethernet** field. Ensure that the **Processor Ethernet** field is set to **y**. If these fields are set to **n**, your system is not enabled for the Co-resident DEFINITY LAN Gateway feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- View the IP Interfaces screen, and ensure that the processor (PROCR) is administered and the Ethernet port for the processor is enabled. If the processor is administered, and the Ethernet port is enabled, **PROCR** appears in the **Type** field and the previously administered node name appears in the **Node Name** field. If the PROCR is not listed, add a processor.

  To view the IP Interfaces screen, type **`display ip-interfaces`**. To add a processor, type **`add ip-interface next`**. Press **Enter**.

Screens for administering Co-resident DEFINITY LAN Gateway

Screen name	Purpose	Fields
Optional Features	Ensure that the proper license fields are set to **y**.	• **ASAI Link Core Capabilities** (if required) • **Computer Telephony Adjunct Links** (if required) • **Co-Res DEFINITY LAN Gateway** • **Processor Ethernet**
IP Node Names	Ensure that a node name is associated with the C-LAN.	• **Name**

Screen name	Purpose	Fields
IP Interfaces	Ensure that the C-LAN is administered, and the Ethernet port for the C-LAN is enabled. If the C-LAN is administered and the Ethernet port is enabled, the **Type** field is set to **C-LAN**, and the previously administered node name appears in the **Node Name / Local Node** field.	• **Type** • **Node Name/Local Node**
Data Modules	Ensure that the Ethernet port on the C-LAN is administered. If the Ethernet port on the C-LAN is administered, the **Service Type** field is set to **Ethernet**, and the **Port** field is set to port **17** on the TN799.	• **Service Type** • **Port**
CTI Link	Add a CTI link.	All
IP Services	Set the IP service type to **DLG**.	**Service Type**
Administer DLG	When the **Service Type** field is set to **DLG**, this page is added to the IP Services screen.	All

Note:
For more information on DLG administration for the S8300 Server, see the Avaya CallVisor® ASAI Technical Reference.

Considerations for Co-resident DEFINITY LAN Gateway

This section provides information about how the Co-resident DEFINITY LAN Gateway feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Co-resident DEFINITY LAN Gateway under all conditions. The following considerations apply to Co-resident DEFINITY LAN Gateway:

- The Co-Resident DLG feature that is available in all configurations of Communication Manager software Release 2.0 and 2.1 has a problem that could potentially bring the CTI link down by triggering a link restart. The Communication Manager software error logs point to a lack of response to TCP Heartbeats from the adjunct side. However, the reason for the link restart is that a Communication Manager internal process stops processing messages from the adjunct.The messages not processed include the response to TCP Heartbeat. While this condition is experienced, messages from Communication Manager to the adjunct (for example, event reports) continue to flow.

  To avoid this problem, if your system is running Communication Manager Release 2.0 or 2.1, you must upgrade to Communication Manager Release 2.1.1, load 414 or later, or get patch Release 7381. Contact your Avaya representative for details.

Co-residency of Communication Manager and SIP Enablement Services

Use the Co-Residency of Communication Manager and SIP Enablement Services (SES) as a solution that helps reduce the cost of adding full, native support for SIP to your communications network by merging the hardware platforms of Release 5.0 of the Communication Manager software. The merged platform for co-residency is the Avaya S8300C Server, with compact flash replacing RAMDISK.

Detailed description of Co-residency of Communication Manager and SIP Enablement Services

The co-resident hardware platform for SES and Communication Manager enables the two to operate more efficiently (for example, without firewall issues or the need to encrypt links between the two), and to share some of the same server resources and capabilities. For example, some of the pages of the Maintenance web interface are shared and reused, including the Web pages for system backup and restore capabilities. The system logging, process status and role-based web access controls also are the same for both.

You can also install Avaya's Communication Manager Messaging voice mail with Communication Manager on S8300 Servers. Both the SES software and Communication Manager are installed, patched and configured in the usual way, with a separate license for each. This makes transitioning to the new co-resident implementation easier for existing administrators. A server reboot is required after enabling SES on the S8300C.

Communication Manager running in a co-resident implementation is supported as a main server only, and not as an ESS or LSP. SES running in a co-resident implementation supports 100 SIP users, or the capacity of the gateway being used with the S8300C, if smaller.

When SES is deployed co-resident with Communication Manager, the server must be configured as an SES Home server or combined Home/Edge server. Co-resident SES cannot be configured as a standalone Edge server, and therefore cannot be designated perform core routing in an Avaya 'Communication Manager Branch Edition' solution. A standalone SES Edge 5.0 (using an Avaya S8500 Server) is still required for these larger SIP implementations.

For more information, see *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server, 03-602508, Issue 1, November 2007*.

Data Call Setup

Use the Data Call Setup feature to set up a data call by any of following methods:

- Data-terminal or keyboard dialing
- Telephone dialing
- Hayes AT command dialing
- Permanent-switched connections
- Administered connections
- Automatic-calling unit interface (MPD and HSC)
- Hotline dialing

Detailed description of Data Call Setup

This section provides a detailed description of the Data Call Setup feature.

In addition to data-terminal and telephone dialing, the system accepts calls from other devices. For example, you can use a modular-processor data module (MPDM) that is equipped with an automatic-calling unit (ACU) interface module to dial from a host computer.

In addition to the numbers, the pound key (#), and the asterisk key (*) on a telephone. Table 74: Special characters on page 763 shows the special characters that a user can dial.

Table 74: Special characters

Character	Short description	Long description
SPACE or minus (-)	and	A space or a minus (-) improves legibility. The server ignores these characters during dialing.
plus (+)	wait	A plus (+) interrupts or suspends dialing until the user receives dial tone.
comma (,)	pause	A comma (,) inserts a 1.5-second delay.
		1 of 2

Table 74: Special characters (continued)

Character	Short description	Long description
percent (%)	mark	Use a percent (%) to indicate that the digits are for end-to-end signaling when you use a touchtone trunk. Use a percent (%) with a rotary trunk. The percent (%) is not required when you use a touchtone trunk.
UNDERLINE or BACKSPACE	-	Use an underline or a backspace to correct characters that you typed on the same line.
at (@)	-	Use an "at" sign (@) to delete the entire line and start again with a new DIAL prompt.
		2 of 2

Each line of information that a user dials can contain 42 characters. Note that the system counts the plus (+) and the percent (%) as two characters each.

You administer the asynchronous data module (ADM) as one endpoint of a connection. The server establishes the connection at the scheduled time, and maintains the connection for the specified duration. After the call is accepted, the data set enters into continuous mode for the specified duration. If the server reboots during the connection, or if the connection drops, the server starts the connection again.

The system handles all ISDN basic rate interface (BRI) bearer data-call requests that are presently defined. If the server does not support a capability, the system returns a proper cause value to the terminal.

The system sends a cause code, also called a reason code, to BRI terminals to identify the reason that the system clears a call. The BRI data module converts some cause values to text messages for the system to display. In a passive-bus multipoint configuration, the system supports two BRI endpoints per port, and thus doubles the capacity of the BRI circuit pack. When you change the configuration of a BRI endpoint from point-to-point configuration to a multipoint configuration, the original endpoint does not need to reinitialize. In a multipoint configuration, you can administer only endpoints that support service profile identifier (SPID) initialization.

Table 75: Call progress messages on page 765 shows the call progress messages and the call progress descriptions for digital communication protocol (DCP) and ISDN-BRI modules that the system provides.

Table 75: Call progress messages

Message Code	Module Type	Message Description
DIAL:	DCP	This message is the equivalent of a dial tone. Type the desired number or the Feature Access Code (FAC), and then Press **Enter**.
CMD	BRI	This message is the equivalent of a dial tone. Type the desired number or the FAC, and then Press **Enter**.
RINGING	DCP, BRI	This message is the equivalent of a ringing tone. The called terminal is ringing.
BUSY	DCP, BRI	This message is the equivalent of a busy tone. The called number is busy or out of service.
ANSWERED	DCP, BRI	The call is answered.
ANSWERED-NOT DATA	DCP	The call is answered, and the system does not detect a modem answer tone.
TRY AGAIN	DCP, BRI	This message is the equivalent of a reorder tone. The system facilities are unavailable.
DENIED	DCP, BRI	This message is the equivalent of an intercept tone. The system cannot place the call as dialed.
ABANDONED	DCP, BRI	The calling user abandoned the call.
NO TONE	DCP, BRI	The system does not detect a tone.
CHECK OPTIONS	DCP, BRI	The data-module options are incompatible.
XX IN QUEUE	DCP, BRI	XX represents the position of the call that is in the queue.
PROCESSING	DCP, BRI	The call is out of the queue. The facility is available.
TIMEOUT	DCP, BRI	The call exceeds the time that is allowed. The system terminates the call.
FORWARDED	DCP, BRI	This message is the equivalent of a redirection-notification signal. The called terminal activates Call Forwarding and receives a call, and the system then forwards the call.
		1 of 2

Table 75: Call progress messages (continued)

Message Code	Module Type	Message Description
INCOMING CALL	DCP, BRI	This message is the equivalent of ringing.
INVALID ADDRESS	DCP	The user entered a name that is not defined in the Alphanumeric Dialing feature.
WRONG ADDRESS	BRI	The user entered a name that is not defined in the Alphanumeric Dialing feature.
PLEASE ANS-	DCP, BRI	The originating telephone user used the One-Button Transfer to Data capability to transfer the call to a data module.
TRANSFER	DCP	Data Call Return-to-Voice is occurring.
CONFIRMED	DCP, BRI	This message is the equivalent of the confirmation tone. The system either accepts the feature request of the user, or the system sends the call to a local coverage point.
OTHER END	DCP, BRI	The endpoint terminates the call.
DISCONNECTED	DCP, BRI	The system disconnects the call.
WAIT	DCP, BRI	The normal process continues.
WAIT, XX IN QUEUE	DCP	The call is in a local hunt-group queue.
		2 of 2

The following data functions are unavailable on ISDN-BRI telephones:

- One-Button Transfer to Data
- Return-to-voice
- Data call preindication
- Voice-call transfer to data
- Data-call transfer to voice

Administering Data Call Setup

The following steps are part of the administration process for the Data Call Setup feature:

- Defining a data module
- Specifying the port location

- Assigning the data extension feature button

This section describes:

- Any prerequisites for administering the Data Call Setup feature
- The screens that you use to administer the Data Call Setup feature
- Complete administration procedures for the Data Call Setup feature

Prerequisites

You must complete the following actions before you can administer the Data Call Setup feature:

- Ensure that the Feature Access Code (FAC) for data origination is available on your system.

To ensure that the FAC for data origination is available on your system:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen.

2. Click **Next** until you see the **Data Origination Access Code** field (Figure 168: Feature Access Code (FAC) screen on page 767).

Figure 168: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page   2 of 7
                              FEATURE ACCESS CODE (FAC)
                  Data Origination Access Code:
                      Data Privacy Access Code:
              Directed Call Pickup Access Code:
    Emergency Access to Attendant Access Code:
                   Enhanced EC500 Activation: *45    Deactivation: *46
 Extended Call Fwd Activate Busy D/A      All:        Deactivation:
       Extended Group Call Pickup Access Code:
              Facility Test Calls Access Code:
                           Flash Access Code:
            Group Control Restrict Activation:        Deactivation:
                  Hunt Group Busy Activation:        Deactivation:
                             ISDN Access Code:
               Last Number Dialed Access Code: *03
   Leave Word Calling Message Retrieval Lock: *33
 Leave Word Calling Message Retrieval Unlock: *34
           Leave Word Calling Send A Message: *35
         Leave Word Calling Cancel A Message: *37
             Malicious Call Trace Activation:        Deactivation:
       Meet-me Conference Access Code Change:
```

3. In the **Data Origination Access Code** field, type the FAC for data origination access.

4. Press **Enter** to save your changes.

Screens for administering Data Call Setup

Table 76: Screens for data-terminal dialing

Screen name	Purpose	Fields
Data Module • PDM/TDM • 7500 • Data Line	Define the data module.	 • All • All • All
Modem Pool Group	Specify the port that is associated with the conversion resource on the integrated modem pool circuit pack.	**Circuit Pack Assignments**

Table 77: Screens for telephone dialing

Screen name	Purpose	Fields
Feature Access Codes	Assign the Feature Access Code (FAC) for data origination.	**Data Origination Access Code**
Station	Assign the **data-ext (Ext:)** feature button for data extension.	Any unassigned button field in the area
Data Module • PDM/TDM • Data Line	Define the data module.	 • All • All
Modem Pool Group	Specify the port that is associated with the conversion resource on the integrated modem pool circuit pack.	**Circuit Pack Assignments**

Defining a data module

To define a data module:

1. Type **`add data-module next`**. Press **Enter.**

   The system displays the Data Module screen.

   — For PDM/TDM data modules, Figure 169: Data Module screen - pdm data module on page 769.

- For 7500 data modules, Figure 170: Data Module screen - 7500 data module on page 770 and Figure 171: Data Module screen - 7500 data module on page 770.
- For Data Line data modules, Figure 172: Data Module screen - data-line data module on page 771 and Figure 173: Data Module screen - data-line data module on page 771.

Figure 169: Data Module screen - pdm data module

```
add data-module next                                          Page   1 of 1
                                DATA MODULE

  Data Extension: 502             Name:                              BCC: 2
            Type: pdm              COS: 1         Remote Loop-Around Test? n
            Port:                  COR: 1           Secondary data module? n
             ITC: restricted        TN: 1                    Connected To: dte


ABBREVIATED DIALING
  List1:

SPECIAL DIALING OPTION:



ASSIGNED MEMBER ( Station with a data extension button for this data module )

         Ext      Name (first 26 characters)
     1:
```

Figure 170: Data Module screen - 7500 data module

```
add data-module next                                          Page   1 of 2
                              DATA MODULE

  Data Extension: 502             Name:
            Type: 7500             COS: 1
            Port:                  COR: 1                  Multimedia? n
                                    TN: 1


ABBREVIATED DIALING
  List1: group    1

SPECIAL DIALING OPTION:



CIRCUIT SWITCHED DATA ATTRIBUTES
  Default Duplex: full     Default Mode: async    Default Speed: 1200

DATA MODULE CAPABILITIES
  Default ITC: restricted                  Default Data Application: M2_A
```

Figure 171: Data Module screen - 7500 data module

```
add data-module next                                          Page   2 of   2
                              DATA MODULE


BRI LINK/MAINTENANCE PARAMETERS

                   XID? y     Fixed TEI? n
           MIM Support? y    Endpt Init? y  SPID: 502         MIM Mtce/Mgt? y
```

Figure 172: Data Module screen - data-line data module

```
add data-module next                                          Page   1 of 2
                              DATA MODULE

  Data Extension: 502             Name:                              BCC: 2
            Type: data-line        COS: 1
            Port:                  COR: 1
             ITC: restricted        TN: 1                 Connected To: dte


ABBREVIATED DIALING
  List1: personal 1

SPECIAL DIALING OPTION:



ASSIGNED MEMBER ( Station with a data extension button for this data module )

         Ext      Name (first 26 characters)
      1:
```

Figure 173: Data Module screen - data-line data module

```
add data-module next                                          Page   2 of 2
                              DATA MODULE

CAPABILITIES
               KYBD Dialing? y                    Configuration? n
                   Busy Out? n
SPEEDS
      Low? y           1200? y           4800? y          19200? y
      300? y           2400? y           9600? y     Autoadjust? n

OPTIONS
            Permit Mismatch? n                     Dial Echoing? y
        Disconnect Sequence: two-breaks             Answer Text? y
                     Parity: even          Connected Indication? y
```

The system shows two display-only fields in the **Abbreviated Dialing** area. These display only-fields are **Ext** and **Name**. The fields contain the extension number and the name of the users who have associated data extension buttons, and who share this data module.

2. In the **BCC** field, perform one of the following actions:
   - If the speed is 56 kbps, type **1**.

- If the speed is 64 kbps, type either **2**, **3,** or **4** .

The system compares the speed setting that you assign here with the speed setting in an associated routing pattern. The system compares the two speed settings when calls that attempt to use the data module fail to complete.

The system displays the **BCC** field if the **ISDN-PRI** field or the **ISDN-PRI Trunk**s field on the Optional Features screen is set to **y**.

3. The **Capabilities** area contains three fields.
   - In the **Busy Out** field, perform one of the following actions:
     - To place the data line circuit (DLC) port in a busy-out state so that calls do not terminate at the data terminal equipment when the DTE control lead to the DLC drops, type **y**. Use this option for DTEs that are members of a hunt group.
     - To keep the DCL port out of a busy-out state when the DTE control lead to the DLC drops, type **n**.
   - The system displays the **Configuration** field only when the **KYBD Dialing** field is set to **y**.
     - If you want to view and change options from originating or receiving DTEs, such as non intelligent terminals, type **y**.
     - If you do not want view and change options from intelligent devices such as computers, type **n**.
   - In the **KYBD Dialing** field, perform one of the following actions:
     - If you want the users to dial calls from a keyboard, and to allow the data module endpoint to transmit and receive text during call origination or call termination, type **y**.

       If you type **y**, you must also type **n** in the **Low** field in the **Speeds** area of the **Data Module** screen.
     - If you do not want the users to dial calls from a keyboard, type an **n**. If you type **n**, the data module endpoint cannot transmit and receive text during call origination and call termination. If you type an **n**, data calls can be answered, but there is no text feedback.
4. The **Circuit Switched Data Attributes** area contains information that is used with 7500 data modules and World Class BRI data modules.

   Note that the fields in the **Circuit Switched Data Attributes** area contain default information. The default information is for modem pooling conversion resource insertion when the endpoint does not support the data query capability, and for when the endpoint does not support the administered connections. The information in the fields has no significance for data modules that provide data query, such as Avaya-supported ISDN-BRI data modules. Use the system default settings that the system provides for Avaya ISDN-BRI data modules or World Class ISDN-BRI data modules.
   - In the **Default Duplex** field, perform one of the following actions:

  - To allow simultaneous, two-way transmission, type **full**.

    This is duplex mode.

  - To allow only one transmission direction at a time, type **half.**

    This is half duplex mode.

- In the **Default Mode** field, perform one of the following actions:
  - For synchronous data mode, type **sync**.
  - For asynchronous data mode, type **async**.
- In the **Default Speed** field, type the data rate. The valid entries are:
  - **1200**
  - **2400**
  - **4800**
  - **9600**
  - **19200**
  - **56000** when the **Default Mode** field is set to **sync**
  - **64000** when the **Default Mode** field is set to **sync**

5. The system displays the **Connected To** field, when the **Type** field contains either **dpm** or **data-line**.

   In the **Connected To** field, perform one of the following actions:

   - If the Asynchronous Data Unit (ADU) is connected to DTE, type **dte**.
   - If the ADU is connected to an information systems network, type **dte**.

6. In the **COR** field, type the number of the class of restriction for this data module. Valid entries are **0** through **95**.
7. In the **COS** field, type the number of the class of service for this data module. Valid entries are **1** through **15**.
8. The **Data Module Capabilities** area contains three fields with information for the 7500 data modules and the World Class BRI (WCBRI) data modules.

   - The **Default Data Applications** field identifies the mode that the system uses to originate calls when the calling parameters do not specify the mode. The system also uses the mode to terminate trunk calls that do not have administered connections or for which the bearer capability is unspecified. See the "Uniform Dial Plan feature" for more information.
   - In the **Default Data Applications** field, perform one of the following actions:
     - Type M0 to specify mode 0. Use this option for a WCBRI endpoint that the system uses as an administered connection.
     - Type M1 to specify mode 1.

- Type M2_A to specify mode 2 asynchronous.
- Type M2_S to specify mode 2 synchronous.
- Type M3/2 to specify mode 3/2 adaptable.

- In the **Default ITC** field, perform one of the following actions:
  - Type **restricted** for a WCBRI endpoint that is an administered connection.
  - Type **unrestricted** for a WCBRI endpoint that is not an administered connection.
- The display-only **MM Complex Voice Ext** field contains the number of the associated telephone in the multimedia complex. The system displays the **MM Complex Voice Ext** field only when the **Multimedia** field is set to **y**.

  The field is blank until you type the data module extension in the **MM Complex Data Ext** field on the Station screen. When you type the data module extension in the **MM Complex Data Ext** field on the Station screen, the system associates the numbers in the **MM Complex Data Ext and the MM complex Voice Ext** fields as two parts of a one-number complex. The one-number complex is the extension of the telephone.

The system displays the data module extension in the display-only **Data Extension** field.

9. The system does not display the **ITC** field for voice-only stations or for BRI stations. The **ITC** field applies only when the **Comm Type** field on the Trunk Group screen, that the system uses for an outbound call, contains **avd** or **rbavd**. The **ITC** field specifies the type of transmission facilities that an ISDN call uses when a call originates from this data module endpoint.

   In the **ITC** field, perform one of the following actions:

   - If the data module can send bits at speeds less than or equal to 56 kbps, type **restricted**. If you type **restricted** in the **ITC** field, the system uses a trunk group for which the COMM Type field on the Trunk Group screen is set to **rbavd** or to **avd** to complete a call from this data module endpoint.

     A restricted transmission facility enforces ones density digital transmission. Ones density digital transmission is a sequence of eight digital zeroes that the firmware on the DS1 port board converts to a sequence of seven zeroes and a digital 1.
   - If the data module can send bits at a speed no greater than 64 kbps, type **restricted**. If you type **unrestricted** in the **ITC** field, the system uses a trunk group for which the **COMM Type** field on the Trunk Group screen is set to **avd** to complete a call from this data module endpoint. The value **avd** in the **Comm Type** field indicates that the trunk group provides both restricted and unrestricted transmission facilities.

     An unrestricted transmission facility does not enforce ones density digital transmission. The DS1 port board firmware does not convert the digital information.
10. In the **List1** field in the **ABBREVIATED DIALING** area, perform one of the following actions:

    - If you do not want the data module to have an abbreviated dialing list, leave the field blank.

- If you want the data module to have an enhanced abbreviated dialing list, type **e**.
- If you want the data module to have a group list, type **g**. If you type **g**, the system displays a field to the right of the **List1** field. If you type **g** in the **List1** field, you must also type a group list number in the field that the system displays.
- If you want the data module to have a personal list, type **p**. If you type **p**, the system displays a field to the right of the **List1** field. If you type **p** in the **List1** field, you must type a personal list number in the field that the system displays.
- If you want the data module to have a system abbreviated dialing list, type **s**.

11. In the **Name** field, perform one of the following actions:
    - Type the name of the user who is associated with the data module.
    - Leave the field blank.
12. The **OPTIONS** area contains six fields.
    - The system displays the **Answer Text** field only if the **KBDY Dialing** field is set to **y**.

      The **Answer Text** field applies to the following call messages:

      — Incoming

      — Answered

      — Disconnected

      — Disconnected other end

      In the **Answer Text** field, perform one of the following actions:

      — To allow text feedback to the DTE when a user answers a call or the system disconnects a call, type **y**. The text feedback includes both DLC-generated text and system-generated text.

      — To disable text feedback to the DTE when a user answers a call or the system disconnects a call, and when the DTE that answers a call is a computer or an intelligent device, type **n**. The system still generates the text, but the DLC does not allow the text to be delivered to the DTE.
    - The system displays the **Connected Indication** field only if the **KBDY Dialing** field is set to **y**. If the **Connected Indication** field is set to **n**, DLC provides the connection indication when the DLC activates the Electronics Industries Association (EIA) 232C control lead.

      In the **Connected Indication** field, perform one of the following actions:

      — If you want the system to generate a "connected" message to the DTE when the system establishes a connection, type **y**.

      — If you do not want the system to generate a "connected" message to the DTE when the system establishes a connection, type **n**.
    - The system displays the **Dial Echoing** field only if the **KBDY Dialing** field is set to **y**.

      In the **Dial Echoing** field, perform one of the following actions:

- If you want the system to echo characters back to the DTE, type **y**.
- If you do not want the system to echo characters back to the DTE and when an intelligent device provides keyboard dialing, type **n**.

- The system displays the **Disconnect Sequence** field only if the **KBDY Dialing** field is set to **y**.

  In the **Disconnect Sequence** field, perform one of the following actions:

  - If you want a break that is greater than 2 seconds, type **long-break**.
  - If you want a break that is less than 1 second, type **two-breaks**.

- The system displays the **Parity** field only if the **KBDY Dialing** field is set to **y**. The DLC generates the parities when the DLC sends call setup text to the DTE. The DLC does not check the parity when the DLC receives dial characters. Select the parity that matches the DTE that connects to the data module.

  In the **Parity** field, type one of the following types of parity:

  - **even**
  - **odd**
  - **mark**
  - **space**

- The **Permit Mismatch** field contains information that allows an EIA interface to operate at a rate that differs from the rate that is agreed upon during the data module handshake. The rate that is agreed upon during the data module handshake is always the highest compatible rate among the speeds that each data module reports.

  The information in the **Permit Mismatch** field eliminates the need to change the DTE or DLC speed whenever someone, or something, places a call to or from endpoints that operate at a different speed.

  When the **Permit Mismatch** field is set to **y**, the DLC reports the highest optional speed and all the lower speeds, or the previously selected autoadjust speed, during the handshake process.

  - If you want the DLC to operate at the highest selected speed, which is a higher rate than the far-end data module, type **y**.
  - If you do not want DLC to operate at the highest selected speed, type **n**.

13. In the **Port** field, type the appropriate values from Table 78: Port field values on page 777.

Table 78: Port field values

Characters	Description	Value
1-2	Cabinet Number	**01** through **44** (For DEFINITY R configurations) **01** through **03** (For DEFINITY SI configurations) **01** through **64** (For IP-PNC)
3	Carrier	**A** through **E**
4-5	Slot Number	**0** through **20**
6-7	Circuit Number	**01** through **04** (x.25 circuit pack) **01** through **31** (DEFINITY SI, IP-PNC (tdm, pdm) configurations) **01** through **16** (ppp for IP-PNC) **01** through **08** (system-port for IP-PNC) **17/33** (ethernet on IP-PNC)
x	Administration without Hardware	If the **Secondary data module?** field, contains an **n**, you can type **x** in the **Port** field. A **Port** field set to **x** indicates that no hardware is associated with the port assignment.

14. The **SPEEDS** area contains information about the operating speeds of the data module.
    - In the **Low** field, perform one of the following actions:
      - If you want the data line circuit to operate at a speed of 0 to 1800 bps, type **y**.
      - If the **KYBD Dialing** field in the **CAPABILITIES** area is set to **y,** type **n**.
    - In the **300**, **1200**, **2400**, **4800**, **9600**, and **19200** fields, perform one of the following actions:
      - If you want the DLC to operate at the speed, type **y**.

        You can choose any of the speeds for the DLC. The DLC matches the speed for the duration of the call.

        If you select multiple speeds, you must also set the **Autoadjust** field to **n** and select at least three speeds. The speed of the DTE must be the highest speed that you select. The DTE must have the highest speed because the system delivers feedback to the DTE at the highest selected speed.
      - If you do not want the DLC to operate at the speed, type **n**.

- The system displays the **Autoadjust** field when the **KYBD Dialing** field in the **CAPABILITIES** area is set to **y**. The **Autoadjust** field applies only to calls that a user originates from a keyboard.

  In the **Autoadjust** field, perform one of the following actions:

  — If you want the DLC port to automatically adjust to the operating speed and the parity of the DTE to which the DLC port connects, type **y**.

  — If you do not want the DLC port to automatically adjust to the operating speed and the parity of the DTE to which the DLC port connects, type **n**.

15. In the **Special Dialing Option** field, perform one of the following actions:

    - If you do not want the data module to have special dialing, leave the field blank.
    - If you want the data module to have hot-line dialing, type **hot-line**. If you type **hot-line**, the system displays the **Abbreviated Dialing Dial Code (from above list):** field. Type the **abbreviated dial code** in the **Abbreviated Dialing Dial Code (from above list):** field. Valid entries are **0** through **999**.
    - If you want the data module to have default dialing, type **default**. If you type **default**, the system displays the **Abbreviated Dialing Dial Code (from above list):** field. Type the **abbreviated dial code** in the **Abbreviated Dialing Dial Code (from above list):** field. Valid entries are **0** through **999**.

16. In the **TN** field, type the tenant partition number of the data module. Valid entries are **1** through **100**.

17. In the **Type** field, perform one of the following actions:

    - To assign a 7500 data module, type **7500**.

      The 7500 data module supports:

      — Automatic TEI

      — B-channel, maintenance and management messaging

      — **Service Profile Identifier (SPID)** initialization capabilities.

      BRI voice endpoints, BRI data endpoint, or both BRI voice and BRI data endpoints are assigned to either the **ISDN**-**BRI** - 4-wire S/T-NT Interface circuit pack **or the ISDN**-**BRI** - 2-wire U circuit pack. Each circuit pack can support up to 12 ports.

      You can administer more than one ISDN endpoint, either a voice endpoint or a data endpoint, on one port. You can administer more than one ISDN endpoint, because BRI provides a multipoint capability.

      For **BRI**, multipoint administration allows for telephones that have **SPID** initialization capabilities. Multipoint administration is allowed only if no endpoint that is administered on the same port is a fixed tie endpoint, and no station on the same port has B-channel data capability. The system restricts multipoint administration to two endpoints per port.

- To assign a data line data module, type **data-line**.

  Use the Data Line Data Module (DLDM) screen to assign ports on the Data Line (**DLC**) circuit pack that allow **EIA** 232C devices to connect to the system. The **DLC**, with a companion **ADU**, provides a less expensive data interface to the system than other asynchronous DCP data modules.

  The **DLC** supports asynchronous transmissions at speeds of Low and 300, 1200, 2400, 4800, 9600, and 19200 bps over 2-pair (full-duplex) lines. These lines can have different lengths, depending on the transmission speed and the wire gauge.

  The **DLC** has eight ports. The connection from the port to the **EIA** device is direct, which means that no multiplexing is involved. A single port of the **DLC** is equivalent in functionality to a data module and a digital line port. The **DLC** appears as a data module to the **DTE,** and as a digital line port to the server that runs Communication Manager.

  The **DLC** connects the following **EIA** 232C equipment to the system:

  - Printers
  - Non intelligent data terminals
  - Intelligent terminals, personal computers (**PC**s)
  - Host computers
  - Information Systems Network (**ISN**), **RS**-232C local area networks (**LAN**s), or other data switches

- To assigns a DCE interface for processor data modules or trunk data modules, type **pdm**.

  Use these screens assign Modular Processor Data Modules (MPDMs) and Modular Trunk Data Modules (MTDMs). Use one screen to assign MPDMs (700D), 7400B, 7400D or 8400B Data Module. Use another screen for MTDMs (700B, 700C, 700E, 7400A). You must complete one screen for each MPDM, 7400B, 7400D, 8400B or MTDM.

  The MPDM, 7400B, or 8400B Data Module provides a Data Communications Equipment (DCE) interface. Use the interface for a connection to equipment such as a data terminal, call detail recording (CDR) output device, on-premises administration terminal, Message Server, Property Management System (PMS), CM Messaging, and host computers. The MPDM, 7400B, or 8400B Data Module also provides a Digital Communications Protocol (DCP) interface to the digital switch.

  Note that DCE is the equipment on the network side of a communications link that provides all the functions that are required to make the binary serial data from the source or transmitter compatible with the communications channel.

  The MTDM provides an EIA DTE interface for connection to off-premises private line trunk facilities, or a switched telecommunications network and a DCP interface for connection to the digital switch.Note that DTE is the equipment that comprises the endpoints in a connection over a data circuit. For example, in a connection between a data terminal and a host computer, the terminal, the host, and their associated modems or data modules make up the DTE. The MTDM or the 7400A Data Module can also serve as part of a conversion resource for combined modem pooling.

18. Press **Enter** to save your changes.

Specifying the port location

To specify the port location:

1. Type **change modem-pool num** *n*, where *n* is the modem pool that you want to change. Press **Enter.**

   The system displays the Modem Pool Group screen (Figure 174: Modem Pool Group screen on page 781).

Figure 174: Modem Pool Group screen

```
change modem pool group                                          Page 1 of 1
                                  MODEM POOL GROUP

                      Group Number: 1                    Group Type: integrated
  Receiver Responds to Remote Loop? n               Hold Time (min): 5
            Send Space Disconnect? y     Receive Space Disconnect? y
                      CF-CB Common? y   Loss of Carrier Disconnect? y
             Speed: LOW/300/1200    Duplex: full    Synchronization: a/sync
         CIRCUIT PACK ASSIGNMENTS
                                Circuit Pack   Circuit Pack
                                Location       Location
                                1: ___          9: ___
                                2: ___         10: ___
                                3: ___         11: ___
                                4: ___         12: ___
                                5: ___         13: ___
                                6: ___         14: ___
                                7: ___         15: ___
                                8: ___         16: ___
```

2. In the **Circuit Pack Location** field, type the 7-character port number that is associated with the conversion resource on the integrated modem pool circuit pack.

   Information in the **Circuit Pack Location** field is optional for integrated conversion resources only.

3. Press **Enter** to save your changes.

Assigning the data extension feature button

To assign the data extension feature button:

1. Type **`change station n`**, where ***n*** is the telephone number of the user that you want to change. Press **Enter.**

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 175: Station screen on page 782).

Figure 175: Station screen

```
change station 32023                                        Page   3 of 3
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          4: data-ext    Ext: 22000
 2: call-appr                          5:
 3: call-appr                          6:
```

3. Type **data-ext** after any available button number.

   When you type **data-ext** in a field, the system displays an **Ext:** field.
4. Type the extension of the data module in the **Ext:** field.
5. Press **Enter** to save your changes.

End-user procedures for Data Call Setup

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Data Call Setup:

- Setting up and disconnecting data calls from a DCP data terminal
- Setting up data calls from a DCP telephone
- Setting up and disconnecting data calls from an ISDN-BRI data terminal
- Setting up data calls from an ISDN-BRI telephone

Setting up and disconnecting data calls from a DCP data terminal

To set up and disconnect data calls from a Digital Communications Protocol (DCP) data terminal.

1. At the Dial: prompt, type the data number.

   The system displays the RINGING message.

   If the call is in a queue, the system displays the WAIT, XX IN QUEUE message. The system displays the position of the call in the queue, represented by XX, as the system moves the call through the queue.

2. Press **Break** to originate or disconnect a call.
3. If the terminal does not generate a 2-second continuous break signal, press the **originate/ disconnect** button on the data module.
4. At the DIAL: prompt, type the digits.

Setting up data calls from a DCP telephone

When a data terminal is unavailable, you can originate and control data calls from a DCP telephone. Use any unrestricted telephone to set up the call, and then transfer the call to a data module endpoint.

Use a button on a multiappearance telephone data-extensions to make the data call. Assign any administrable feature button as a data-extension button. The data-extension button provides one-touch access to a data module.

Use any of the following options, either alone or in combination, to make a data call from a voice terminal.

- One-Button Transfer to Data

  Press the **data-extension** button after the endpoint answers, to transfer a call to the associated data module.

- Return-to-Voice

  Press the **data-extension** button that is associated with a busy data module to change a connection from a data connection to a voice connection. If you hang up, the system disconnects the call. If the system returns the data call to the telephone, the system either continues the call in voice mode, or the system transfers the data call to another endpoint.

- Data Call Preindication

  Press the data-extension button to reserve the associated data module before you dial a data endpoint. The system reserves the data module for the call and reserves a conversion resource for the call, if the call needs a conversion resource.

  Use the Data Call Preindication option before you use one-button transfer to data, for data calls that use toll-network facilities. Data Call Preindication is in effect until you press the associated **data-extension** button again for a one-button transfer. There is no timeout.

Setting up and disconnecting data calls from an ISDN-BRI data terminal

To set up and disconnect data calls from an ISDN-BRI data terminal:

1. Press **Enter** a few times until the system displays the **CMD**: prompt.
2. If the system does not display the **CMD**: prompt:
   a. Press **Break**, **A**, and **T** at the same time.
   b. Press **Enter**.
   c. Type three plus signs (**+++**).

      The system displays the CMD: prompt.
   d. Type **end**.
   e. Press **Enter**.

Setting up data calls from an ISDN-BRI telephone

To set up a data call from an ISDN-BRI telephone:

1. Press the data button on the telephone.
2. Type the number on the dial pad.
3. Press the data button again.

The following data functions are unavailable on ISDN-BRI voice terminals:

- One-button transfer to data
- Return-to-voice
- Data call preindication
- Voice call transfer to data, and data call transfer to voice

Considerations for Data Call Setup

This section provides information about how the Data Call Setup feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Data Call Setup under all conditions. The following considerations apply to Data Call Setup:

- ISDN basic rate interface (BRI) has a voice-to-data restriction. A telephone cannot call a data terminal, and a data terminal cannot call a telephone
- BRI telephones cannot have data-extension buttons. Digital Communications protocol (DCP) sets have data-extension buttons. However, DCP sets cannot have data-extension buttons for BRI.
- When a telephone user uses a modem to place a data call, the user dials the data-origination access code that is assigned in the system before the user dials the endpoint.
- The system does not limit the number of assigned data-extension buttons per telephone. Assign telephone buttons that access the data module.
- Telephone dialing is unavailable in ISDN-BRI applications because ISDN-BRI terminals supports neither voice-call transfer to data, nor data-call transfer to voice.

Interactions for Data Call Setup

This section provides information about how the Data Call Setup feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Data Call Setup in any feature configuration.

- Abbreviated Dialing

  You can use only 22 of the 24 digits in an abbreviated-dialing number when you dial at a keyboard. The remaining two digits must contain the wait indicator for tone detection.

- Alphanumerical Dialing

  When a data-terminal user uses the Alphanumeric Dialing feature to place a call, the user enters an alphanumeric name.

- Call Coverage

  You cannot assign a coverage path to a hunt group that consists of data endpoints.

- Call Detail Recording (CDR)

  CDR records the use of modem pools on trunk calls.

- Call Forwarding All Calls

  The system uses the Call Forwarding All Calls capability to redirect data calls to a user-designated extension. The attendant or a forwarding party dials a Feature Access Code (FAC) to activate the Call Forwarding All Calls capability.

  A user can use data-terminal dialing to activate Call Forwarding All Calls for calls to a data module. If the forwarded-to endpoint is an analog endpoint, and the caller is a digital endpoint, the system activates modem pooling automatically.

- Data Hotline

  Data Hotline is a security feature. The server terminates calls to a preadministered hotline. The system discards any address string and routes the call as if the users entered the hotline-destination address. This Data Hotline feature does not affect incoming calls. You cannot use the Data Hotline feature and the Default Dialing feature at the same time.

- Default Dialing

  If the Default Dialing feature is active, a data-terminal user can Press **Enter** to call a preadministered destination. The data-terminal user enters a complete address to call other destinations.

- Digit Dialing

  The system provides basic digit dialing through an asynchronous data module (ADM) or a 7500B data module. The user can enter digits from 0 to 9, an asterisk (*), and a pound sign (#) from a 7500 series telephone keypad or from an Electronics Industries Association (EIA) terminal interface.

- Internal Automatic Answer

  Data calls are not eligible for Internal Automatic Answer.

- Modem Pooling

  Modem Pooling is available on data calls. The system automatically inserts a modem if the data call needs a modem. You can use the Data Call Preindication option or the Data Origination option to indicate the need for a modem.

- Uniform Call Distribution (UCD)

  UCD provides a group of data modules, or analog modems, for answering calls to a connected facility. A computer port is an example of a connected facility.

- World-Class Tone Detection

  The system supports multiline data-terminal dialing, if you set the **tone-detection options** field on the Feature-Related System-Parameters screen to **precise**.

  The message that Data Call Setup sends to users depends on the tone-detection option that you administer.

Default Dialing

Use the Default Dialing feature to provide data-terminal users who often dial the same number a very simple method to dial that number. Normal data-terminal dialing and the alphanumeric dialing features are unaffected.

Detailed description of Default Dialing

This section provides a detailed description of the Default Dialing feature.

Data terminal users use the computer keyboard to dial. With Default Dialing, a data-terminal user can place a data call to a preadministered destination by doing either of the following:

- Press **Enter** at the DIAL: prompt (for data terminals using DCP data modules).

  The data-terminal user with a DCP data module can place calls to other destinations by entering the complete address after the DIAL: prompt (normal data terminal dialing or alphanumeric dialing).

- Type **d** and press **Enter** at the CMD: prompt. For data terminals that use ISDN-BRI data modules.

  To place calls to other destinations, the user calls types **d**, a space, the complete address, and press **Enter** after the CMD: prompt.

Note:
DU-type hunt groups that connect the system to a terminal server on a host computer have hunt-group extensions set to no keyboard dialing.

Administering Default Dialing

This section describes the screens that you use to administer the Default Dialing feature.

Screens for administering Default Dialing

Screen name	Purpose	Fields
Data Module	Set the default dialing options.	• **Special Dialing Option** • **Abbreviated Dialing List** • **AD Dial Code**

Demand Print

Use the Demand Print feature to print undelivered messages.

Detailed description of Demand Print

This section provides a detailed description of the Demand Print feature.

With Demand Print, a user can dial a Feature Access Code (FAC) or press a button to print undelivered messages.

Administering Demand Print

This section describes the screens that you use to administer the Demand Print feature.

Screens for administering Demand Print

Screen name	Purpose	Fields
Feature Access Code (FAC)	Specify the FAC for Demand Print.	**Print Messages Access Codes**
Station (multiappearance)	Assign a **print-msgs** feature button for a user.	Any available field in the **Feature Button Assignments** area
	Assign a Station Security Code (SSC) for a user.	**Security Code**

Dial Access to Attendant

Use the Dial Access to Attendant feature to dial an attendant access code and reach an attendant.

Detailed description of Dial Access to Attendant

With the Dial Access to Attendant feature, telephone users in your system can use an attendant access code to reach an attendant. Attendants can then extend the call to a trunk, or to another telephone.

Administering Dial Access to Attendant

The following steps are part of the administration process for the Dial Access to Attendant feature:

- Changing the attendant access code

This section describes:

- Any prerequisites for administering the Dial Access to Attendant feature
- The screens that you use to administer the Dial Access to Attendant feature
- Complete administration procedures for the Dial Access to Attendant feature

Prerequisites for administering Dial Access to Attendant

You must complete the following actions before you can administer the Dial Access to Attendant feature:

- None

Screens for administering Dial Access to Attendant

Screen name	Purpose	Fields
Dial Plan Analysis Table	Change the attendant access code from the default setting of **0**.	• **Dialed String** • **Total Length**

Changing the attendant access code

You can administer the length of the attendant access code. The attendant access code can be a 1-digit or 2-digit number. The default attendant access code is **0**.

Note:
If you have multiple locations, you can also change the attendant access code from the Locations screen. For more information, see the "Multi-Location Dial Plan" feature.

To change the attendant access code:

1. Type **`change dialplan analysis`**. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen (Figure 176: Dial Plan Analysis Table screen on page 793).

Figure 176: Dial Plan Analysis Table screen

```
change dialplan analysis                                      Page 1 of 12
                            DIAL PLAN ANALYSIS TABLE
                                                            Percent Full: 7

      Dialed  Total  Call        Dialed  Total  Call      Dialed  Total  Call
      String  Length Type        String  Length Type      String  Length Type
        00      2    attd
        1       3    dac
        2       4    ext
        3       4    ext
        3       1    aar
        4       1    ars
        4       5    ext
        5       5    ext
        5       7    ext
        6       5    ext
        7210    7    ext
        8       7    ext
        9       1    fac
        *       3    fac
        #       3    fac
```

2. To assign a digit other than **0**, find **attd** in the **Call Type** column. In that row:
   - Change the number in the **Dialed String** column to a unique 1-digit or a 2-digit number.
   - If you changed the number in the **Dialed String** column to a 2-digit number, change the number in the **Total Length** column to **2**.
3. Press **Enter** to save your changes.

Starting with Communication Manager Release 2.0, you can also enter a **fac** or **dac** entry on the Dial Plan Analysis Table screen to administer the attendant access code. You then enter the actual access code on the Feature Access Codes screen. You can administer location-specific attendant access codes on the Locations screen.

For more information, see the "Dial Plan" feature and the "Feature Access Code" feature.

Reports for Dial Access to Attendant

The following reports provide information about the Dial Access to Attendant feature:

- None

Interactions for Dial Access to Attendant

This section provides information about how the Dial Access to Attendant feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Dial Access to Attendant in any feature configuration.

- Class of Restriction

  If the Class of Restriction (COR) of a telephone restricts a user from originating calls, the user cannot call the attendant.

- Conference

  If a telephone user dials the attendant access code, the attendant cannot add that user to an existing conference call.

Dial Plan

Use the Dial Pan feature to interpret the digits that a user dials. The system needs this information to properly route the call. The Dial Plan feature supports intraserver dialing for extensions that are colocated with the server, and for extensions that are spread across several locations.

Detailed Description of Dial Plan

Use the Dial Pan feature to provide the information that the software uses to interpret the digits that a user dials. The software needs this information to properly route the call. The Dial Plan feature supports intraserver dialing for extensions that are colocated with the server, and for extensions that are spread across several locations.

If you need a dial plan that supports interserver dialing, see the "Uniform Dial Plan" feature.

Dial Plan enhancements for Communication Manager

Beginning with Communication Manager Release 4.0, the Dial Plan feature has been expanded to accommodate maximum extension lengths of 13 digits, and allow 18-digit extension dialing using the Uniform Dial Plan (see the Uniform Dial Plan feature). This expansion to 13 digits permits Communication Manager to support the Open Numbering plan that is offered by the Tenovis I55, as well as by other vendors.

This expansion to 13 digits also involves full support for short/long number dialing, flexible punctuation formats, and flexible extension lengths in call appearance and button labels. For US customers, the Dial Plan Expansion feature improves the Dial Plan. This feature allows Communication Manager to fit more easily into European networks with numbering plans of 8 or more digits (notably those that use Open Numbering).

Punctuation of long numbers, introduced in Communication Manager 1.3 for 6-digit and 7-digit extensions, is still supported for the new longer extensions. Communication Manager 4.0 extends this capability to administration forms as well. With punctuation, customers can more easily read extensions of eight or more digits.

The Multi-Location Dial Plan feature that was introduced in Communication Manager 2.0 has been extended for Communication Manager 4.0. This means that a customer can let their users dial short numbers within a location. For example, a user can dial 66180 instead of having to dial the full extension 1-908-456-6180. Beginning in Communication Manager 4.0, customers have the option to display the short number on station displays rather than the full extension.

Note:

The Dial Plan Expansion feature affects the information that is displayed on a display telephone. The display information changes based on the type of telephone. However, when extensions longer than 8 characters displays on a telephone, some display strings had to be modified to allow everything to fit. For example, on a normal station-to-station call, if the punctuated extension is longer than 8 digits, the last three letters of the 27-character name are truncated.

The expanded dial plan is intended to support the “flatten and consolidate” architecture that Avaya is offering to customers with large DCS and QSIG networks. It simplifies administration, since only a few Communication Manager servers need to be managed rather than dozens or even hundreds of small switches. Communication Manager Release 4.0 is making this consolidation easier by letting users keep seeing and dialing their shorter extensions even as their actual extensions grow larger.

Note:

Starting with Communication Manager Release 5.0, you can also use the Per-Location Dial Plan feature to allow different branches to have different short extensions, so that the extensions do not conflict across branches.

The Dial Plan Expansion feature is implemented on all Linux-based server platforms.

Some of the screens that are modified to accommodate the longer extensions, or have new fields added to them, are:

- Dial Plan Analysis screen
- Dial Plan Parameters screen
- Location Parameters screen
- Station screen
- Uniform Dial Plan Table screen

For more detailed information, see the *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Dial plan information

The system supports several types of calls. You must define dial plan information for each type of call.

- Attendant
- Automatic alternate routing (AAR)
- Automatic Route Selection (ARS)
- Dial access codes (DACs), which includes Feature Access Codes (FACs) and trunk access codes (TACs)
- Extensions

- FACs only
- Prefixed extensions

You must also define dial plan information for all calls, regardless of the type of call. You also can define information that controls the appearance of extensions up to 13 digits that the system displays for users and attendants.

If the users on your server are at several physical locations, you need to define additional dial plan information about the locations.

Multi-location dial plan

When a customer migrates from a multiple independent node network to a single distributed server whose gateways are distributed across a data network, it might appear that some dial plan functions are unavailable. For example, the multilocation dial plan preserves dial plan uniqueness for extensions and attendants that were provided in a multiple independent node network, but appear to be unavailable when customers migrate to a single distributed server.

Short dialing

Users in small locations might not like dialing 7 digits to reach the person across the hall. Also, customers want to set up their system, like retail stores, so that the same extension is used for the same department in each store, even if each store uses a gateway connected to a central Communication Manager server.

This is solved using a new special entry on the UDP screen that tells the system to “transfer” the leading digits of the calling party’s telephone number to the dialed number. For example, if extension 852-5581 dials 23529, the leading 85 is prepended and 852-3529 is called. However, the station displays all show the long number (852-xxxx), not the shorter dialed number (2xxxx). This is the default behavior. Starting from Communication Manager Release 4.0, you can use the **Intra-Location** formats on the Dial Plan Parameters screen to display the shorter, dialed numbers. For more information, see Other options for the dial plan on page 798.

Location prefix

The system adds the prefix assigned to the location of the user to the digits that the user dials. The server then analyzes the combined string and routes the call. The system uses several sources for the location information. The system uses the:

- Location number to which the non-IP telephones and trunks are attached for Non-IP telephones and trunks
- Information that you define for IP telephones
- Signaling group that is associated with the IP trunk or information that you define for IP trunks

Location prefix example

For example, in a department store with many locations, each location might have had its own switch with a multiple independent node network. The department store might use the same extension across all the stores for the same department. For example, the department store might always use 4567 for the luggage department. If the department store migrates to a single distributed server, a user can no longer dial 4567 to reach the luggage department in the store. The user must now dial the complete extension to connect to the luggage department, for example 123-4567.

With the multilocation dial plan the user can continue to dial 4567. The user can continue to dial 4567 because the software adds the location prefix to the digits that the user dials. The server analyzes the combined digits and routes the calls based on the dial plan that you define.

Other options for the dial plan

The Dial Plan Parameters screen works with the Dial Plan Analysis Table to define your system's dial plan. Communication Manager 4.0 supports the following changes to the **Dial Plan Parameters screen**:

- New fields are added, allowing customers to specify punctuation formats for 6-digit through 13-digit extensions.
- The punctuation field is divided into two columns, one for inter-location displays, and one for intra-location displays.
- Blank spaces are sometimes used in telephone extensions, especially outside of the US. Some SAT administration screens do not accept blanks. Dots (**.**) are now used on SAT screens in place of blanks. A new HELP screen warning reflects this change.
- The following table gives the maximum number of punctuation marks permitted for each extension length:

Note:

The number of punctuation marks that the system allows is determined by the number of "x"s in the format:

- If the format contains fewer than 6 x's, no punctuation marks can be entered.
- For 6 or more x's, the maximum number of punctuation marks is determined by the table included in this requirement.

Extension Length	Max Punctuation Marks	Max Total Length
6	2	8
7	1	8
8	3	11

Extension Length	Max Punctuation Marks	Max Total Length
9	3	12
10	3	13
11	2	13
12	1	13
13	0	13

- In the **Intra-Location** column only, customers can enter fewer x's than the number of extension digits. This indicates that they wish to see only the trailing "n" digits. At least 3 x's must be entered.

  Note:
  On upgrade from Communication Manager 3.1 or earlier, the 6- and 7-digit fields shall be populated with the 6- and 7-digit values from Communication Manager 3.1. On new installations, the 6- and 7-digit fields shall default as they do in Communication Manager 3.1.

- The default values for the 8-, 9-, 10-, 11-, 12-, and 13-digit fields are those shown in Figure 177.

  Note:
  The 13-digit entry in the **Inter-Location/SAT** column is read-only.

Figure 177: Dial Plan Parameters screen

```
display dialplan parameters                                    Page   1 of   1
                           DIAL PLAN PARAMETERS

                 Local Node Number:                      FIPN ISSLC:
                   ETA Node Number:
               ETA Routing Pattern:
        UDP Extension Search Order: udp-table-first
      AAR/ARS Internal Call Prefix:
AAR/ARS Internal Call Total Length:
Retry ARS Analysis If All-Location Entry Inaccessible? n

 EXTENSION DISPLAY FORMATS
                                  Inter-Location/SAT     Intra-Location
         6-Digit Extension:       xx.xx.xx               xx.xx.xx
         7-Digit Extension:       xxx-xxxx               xxx-xxxx
         8-Digit Extension:       xx.xx.xx.xx            xx.xx.xx.xx
         9-Digit Extension:       xxx-xxx-xxx            xxx-xxx-xxx
        10-Digit Extension:       xxx-xxx-xxxx           xxx-xxx-xxxx
        11-Digit Extension:       xxxx-xxx-xxxx          xxxx-xxx-xxxx
        12-Digit Extension:       xxxxxx-xxxxxx          xxxxxx-xxxxxx
        13-Digit Extension:       xxxxxxxxxxxxx          xxxxxxxxxxxxx
```

AAR/ARS Internal Call Prefix

The digits entered in this field are concatenated with the calling or called extension. Appears only if, on the System-Parameters Customer-Options screen, the **ARS/AAR Dialing Without FAC** field is **y**. (Contact your Avaya representative to discuss the ARS/AAR Dialing Without FAC feature before enabling it.)

Valid entries	Usage
0-**9** up to 13 digits**,** or **blank**	Enter a string from 1 to 13 digits long (not including * or #).

AAR/ARS Internal Call Total Length

The total length of the internal call digit string. Appears only if, on the System-Parameters Customer-Options screen, the **ARS/AAR Dialing Without FAC** field is **y**. (Contact your Avaya representative to discuss the ARS/AAR Dialing Without FAC feature before enabling it.)

Valid entries	Usage
6-10 or blank	Enter the total length of the internal call digit string, which includes the Internal Call Prefix and the calling or called extension.

Note:
If either the **AAR/ARS Internal Call Prefix** or the **AAR/ARS Internal Call Total Length** field is non-blank and valid, the other must also be non-blank and valid. In addition, the longest extension length on the Dial Plan Analysis screen, plus the length of the **ARS/AAR Internal Call Prefix**, must equal or be greater than, the **ARS/AAR Internal Call Total Length** value.

ETA Node Number

Enter the number of the destination server for Extended Trunk Access (ETA) calls. ETA calls are unrecognized numbers you can send to another switch for analysis and routing. Such numbers can be Facility Access Codes, Trunk Access Codes, or extensions that are not in the UDP table.

Valid entries	Usage
1 - **999** or blank	Enter the number of a destination server.

ETA Routing Pattern

Enter the number of the routing pattern to reach the destination server.

Valid entries	Usage
1 - **640** or blank	Avaya DEFINITY Server R, CSI, or SI.
1-**999** or blank	Avaya S8300 Server, IP-PNC, S8700 or S8710 Multi-Connect.

Local Node Number

Enter a number to identify a specific node in a server network. This entry must match the DCS switch node number and the CDR node number if they are specified.

Valid entries	Usage
1-**63**	Enter the number of a specific node in a network.
blank	The field may be left blank if automatic restoration, DCS, and CDR are not used.

UDP Extension Search Order

Important:
If the **Call Type** on the **Dial Plan Analysis Table screen** is set to **udp**, then the system bypasses the **UDP Extension Search Order** field. For more information, see the **udp** **Call Type** description.

Appears if the **Uniform Dialing Plan** field is **y** on the System-Parameters Customer-Options screen. Specifies the first table to search to match a dialed extension. If the dialed extension is not found in the specified place, it then is searched for in the "other" place.

Valid entries	Usage
local-extensions-first	Searches the local server first to match a dialed extension; if not found, then uses the UDP tables to route the call.
udp-table-first	Searches the UDP tables for an off-switch conversion; if not found, then searches the local server for the dialed extension.

Retry ARS Analysis if All-Location Entry Inaccessible (ESS/LSP)?

This field appears on the Dial Plan Parameters screen in Communication Manager Release 4.0.x or later.
If this field is set to **no**, the system does not retry ARS analysis.
If this field is set to **yes**, the system finds and uses the best possible entry in the per-location ARS table, if the all-location table points to a trunk group that cannot be accessed because the network has fragmented.

This section describes the following topics:

- Dial Plan Analysis Table
- Dial Plan Parameters

- Multi-Location Dial Plan

All Feature Access Codes (FACs), extensions, and trunk access codes (TACs) that you assign must be consistent with the dial plan.

Dial Plan Analysis Table

The Dial Plan Analysis Table is the guide that the software uses to translate the digits dialed by users. This screen enables you to determine the beginning digits and total length for each type of call that Communication Manager needs to interpret.

Figure 178: Dial Plan Analysis Table screen on page 803 shows an example of a simple dial plan.

Figure 178: Dial Plan Analysis Table screen

```
display dialplan analysis                                    Page   1 of  12
                           DIAL PLAN ANALYSIS TABLE
                                 Location:  all           Percent Full:    2

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
    0            1    attd   9           5    ext
    0            4    dac    *0          3    fac
    1            3    dac    *1          3    fac
    2            4    ext    *2          3    fac
    2            5    ext    *3          3    fac
    3            4    ext    *4          3    fac
    3            5    ext    *5          3    fac
    4            3    dac    *6          3    fac
    4            4    ext    *7          3    fac
    4            5    ext    *8          3    fac
    5            5    ext    *9          2    fac
    6            5    ext    #           3    dac
    63           3    dac
    7            5    ext
    8            1    dac
```

Use the Dial Plan Analysis Table screen to define the dial plan for your system.

- **Call Type** - Indicates what the system does when a user dials the digit or digits indicated in the **Dialed String** column. The Dial Plan Analysis Table screen contains the following call types:
  - Attendant (attd) - Defines how users call an attendant. Attendant access numbers can be any number from 0 to 9 and contain 1 or 2 digits.

- Dial access code (dac) - Allows you to use trunk access codes (TAC) and Feature Access Codes (FACs) in the same range. For example, you could define the group 100 -199, which would allow both FAC and TAC in that range. Dial access codes can start with any number from 1 to 9, * and #, and contain up to 4 digits.

Note:
The Dial Plan Analysis Table screen does not allow you to enter a range specifically for trunk access codes. However, the Trunk Group screen still allows you to assign a TAC to a trunk group. The TAC you enter on the Trunk Group screen must match the format you have administered for a DAC on the Dial Plan Analysis Table screen.

- Extensions (ext) - Defines extension ranges that can be used on your system.
- Feature access codes (fac) - FAC can be any number from 1 to 9 and contain up to 4 digits. You can use * or #, but only as a first digit.
- Uniform Dial Plan (udp) - The udp call type works identically with the ext call type, with this exception:
  - If dialed digits match the call type of udp, Communication Manager automatically checks the UDP Table first to see if there is a match, regardless of the value in the **UDP Extension Search Order** field on the **Dial Plan Parameters screen**. If there is no match, Communication Manager then checks the local server.
  - If dialed digits match the call type of ext, Communication Manager checks the value in the **UDP Extension Search Order** field on the **Dial Plan Parameters screen**.
    - If the value in the **UDP Extension Search Order** field on the **Dial Plan Parameters screen** is **udp-table-first**, Communication Manager checks the UDP Table first to see if there is a match. If there is no match, Communication Manager then checks the local server.
    - If the value in the **UDP Extension Search Order** field on the **Dial Plan Parameters screen** is **local-extensions-first**, Communication Manager checks the local server first to see if there is a match. If there is no match, Communication Manager then checks the UDP Table.

    The udp call type allows Communication Manager to recognize strings of 14 and 15 digits, which are longer than the maximum extension length of 18 digits. However, the udp call type can be used with any length in case this provides a useful new capability to customers.

Note:
If you are administering a Per-Location Dial Plan, you must use the Uniform Dial Plan feature.

- **Total Length** - Indicates how long the dialed string will be for each type of call.

Dial Plan Parameters

The Dial Plan Parameters screen works with the Dial Plan Analysis Table to fully define the dial plan of your system. The Dial Plan Parameters screen allows you to set system-wide parameters for your dial plan. The Dial Plan Parameters screen also controls the appearance of 8-digit and 13-digit extensions on station displays. You can select a system-wide format to display all 8-digit extensions, and a format to display all 13-digit extensions.

The following figure shows a simple Dial Plan Parameters screen (Figure 179: Dial Plan Parameters screen on page 805).

Figure 179: Dial Plan Parameters screen

```
change dialplan parameters                                    Page   1 of   1
                            DIAL PLAN PARAMETERS

                 Local Node Number:                      FIPN ISSLC:
                   ETA Node Number:
               ETA Routing Pattern:
        UDP Extension Search Order: udp-table-first
      AAR/ARS Internal Call Prefix:
AAR/ARS Internal Call Total Length:
Retry ARS Analysis If All-Location Entry Inaccessible? n

 EXTENSION DISPLAY FORMATS
                                  Inter-Location/SAT     Intra-Location
         6-Digit Extension:       xx.xx.xx               xx.xx.xx
         7-Digit Extension:       xxx-xxxx               xxx-xxxx
         8-Digit Extension:       xx.xx.xx.xx            xx.xx.xx.xx
         9-Digit Extension:       xxx-xxx-xxx            xxx-xxx-xxx
        10-Digit Extension:       xxx-xxx-xxxx           xxx-xxx-xxxx
        11-Digit Extension:       xxxx-xxx-xxxx          xxxx-xxx-xxxx
        12-Digit Extension:       xxxxxx-xxxxxx          xxxxxx-xxxxxx
        13-Digit Extension:       xxxxxxxxxxxxx          xxxxxxxxxxxxx
```

For more information on fields in the Dial Plan Parameters screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Multi-Location Dial Plan

When a customer migrates from a multiple independent node network to a single distributed server whose gateways are distributed across a data network, it may initially appear as if some dial plan functions are no longer available.

The multi-location dial plan feature preserves dial plan uniqueness for extensions and attendants that were provided in a multiple independent node network, but appear to be unavailable when customers migrate to a single distributed server.

For example, in a department store with many locations, each location might have had its own switch with a multiple independent node network. The same extension could be used to represent a unique department in all stores (extension 4567 might be the luggage department). If the customer migrates to a single distributed server, a user could no longer dial 4567 to get the luggage department in their store. The user would have to dial the complete extension to connect to the proper department.

Instead of having to dial a complete extension, the multi-location dial plan feature allows a user to dial a shorter version of the extension. For example, a customer can continue to dial 4567 instead of having to dial 123-4567.

Communication Manager takes the location prefix and adds those digits to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters screen.

Other options for Dial Plan

You can establish a dial plan so that users only need to dial one digit to reach another extension. You can also establish a dial plan that allows users to dial, for example, three digits to reach one extension, and four digits to reach another. This is particularly useful in the hospitality industry, where you want users to be able to simply dial a room number to reach another guest.

Administering Dial Plan

The following steps are part of the administration process for the Dial Plan feature:

- Defining your dial plan
- Adding extension ranges
- Defining a multi-location dial plan

This section describes:

- Any prerequisites for administering the Dial Plan feature
- The screens that you use to administer the Dial Plan feature
- Complete administration procedures for the Dial Plan feature

Prerequisites for administering Dial Plan

You must complete the following actions before you can administer the Dial Plan feature:

- None

Screens for administering Dial Plan

Screen name	Purpose	Fields
Dial Plan Analysis Table	Specify the dial plan information for each type of call.	All
Dial Plan Parameters	Specify system-wide parameters for your dial plan.	All
Locations	If you have multiple locations, provide the information about the locations.	• **ARS FAC** • **ARS Prefix 1 Required for 10-Digit NANP Calls?** • **Attd FAC** • **Loc Number** • **Loc. Parms.** • **Name** • **NPA** • **Prefix**
Optional Features	If you have multiple locations, ensure that your system is enabled to support them.	**Multiple Locations**

Defining your dial plan

To display your dial plan:

1. Type **`change dialplan analysis`**. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen (Figure 180: Dial Plan Analysis Table screen on page 808).

Figure 180: Dial Plan Analysis Table screen

```
display dialplan analysis                                    Page   1 of  12
                          DIAL PLAN ANALYSIS TABLE
                                Location:  all          Percent Full:    2

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
    0            1    attd   9           5    ext
    0            4    dac    *0          3    fac
    1            3    dac    *1          3    fac
    2            4    ext    *2          3    fac
    2            5    ext    *3          3    fac
    3            4    ext    *4          3    fac
    3            5    ext    *5          3    fac
    4            3    dac    *6          3    fac
    4            4    ext    *7          3    fac
    4            5    ext    *8          3    fac
    5            5    ext    *9          2    fac
    6            5    ext    #           3    dac
    63           3    dac
    7            5    ext
    8            1    dac
```

2. Move the cursor to an empty row.
3. In the **Dialed String** field, type the initial digits that a user might dial.

   The dialed string contains the digits that Communication Manager analyzes to determine how to process the call.

Valid entries	Usage
0-**9**, ***** and **#**	Enter any combination of 1 to 10 digits. the following restrictions apply: ● The digits ***** and **#** may only be used as first digits, and only for the Call Types **fac** and **dac**. ● For Call Type **attd**, if the Total Length is 2, the Dialed String must be 2 digits long. ● Two Dial Plan entries can use the same Dialed String only if the Dialed String is 1 digit long. Longer Dialed Strings must all be unique. ● A new entry cannot be administered if it causes an existing extension, Feature Access Code, or trunk access code to become inaccessible.

4. In the **Total Length** field, type the total number of digits that a user might dial for this dialed string.

Valid entries	Usage
1-2 for attd **1-4 for dac** **1-4 for fac** **1-13 for ext** **2-6 for pext** **1-18 for udp**	Enter the number of digits for this call type. The allowed length varies by call type. This must be greater than or equal to the number of digits in the Dialed String.

Note:
If you are administering a Per-Location Dial Plan, you must use the Uniform Dial Plan feature.

5. In the **Call Type** field, type the name of the call type for this dialed string.

Valid entries	Usage
aar	Automatic Alternate Routing. The system uses this call type to route calls within your company over your own private network. In order to use this code in your dial plan, the ARS/AAR Dialing without FAC feature must be enabled on the System Parameters Customer Options screen. (Contact your Avaya representative to discuss the ARS/AAR Dialing Without FAC feature before enabling it.) When dialing digits of Call Type aar, as soon as the dialed digits have reached the administered length, the digits are treated as if an AAR Feature Access Code (FAC) was dialed. Control is transferred and the digits are routed according to the AAR Analysis and Digit Conversion forms. In the example shown on the Dial Plan Analysis Table on page 803, extensions of 3xxx cannot be dialed directly. Whenever a user dials the first digit of 3, the system immediately interprets the dialed string as an AAR string and transfers control to AAR. Extensions of 3xxx can only be accessed using AAR Digit Conversion. That is, you must dial a longer AAR number from which AAR Digit Conversion deletes leading digits to form a number of the form 3xxx.

Valid entries	Usage
ars	Automatic Route Selection. The system uses this call type to route calls that go outside your company over public networks. ARS is also used to route calls to remote company locations if you do not have a private network. In order to use this code in your dial plan, the ARS/AAR Dialing without FAC feature must be enabled on the System Parameters Customer Options screen. (Contact your Avaya representative to discuss the ARS/AAR Dialing Without FAC feature before enabling it.) When dialing digits of Call Type ars, as soon as the dialed digits have reached the administered length, the digits are treated as if an ARS Feature Access Code (FAC) was dialed. Control is transferred and the digits are routed according to the ARS Analysis and Digit Conversion forms. In the example shown on the Dial Plan Analysis Table on page 803, extensions of 4xxxx cannot be dialed directly. Whenever a user dials the first digit of 4, the system immediately interprets the dialed string as an ARS string and transfers control to ARS. Extensions of 4xxxx can only be accessed using ARS Digit Conversion. That is, you must dial a longer ARS number from which ARS Digit Conversion deletes leading digits to form a number of the form 4xxxx.
attd	Attendant. The system uses this call type to define how users call an attendant. Attendant access numbers can start with any number from 0 - 9 and contain 1 or 2 digits. If a telephone's COR restricts the user from originating calls, this user cannot access the attendant using this code. You can also administer the attendant access code by entering an appropriate **fac** or **dac** entry on the Dial Plan Analysis screen, and then entering the actual access code on the Feature Access Codes screen. Location-specific attendant access codes can be administered on the Locations screen.
dac	Dial Access Code. The system uses this call type to allow you to use both trunk access codes (TAC) and Feature Access Codes (FACs) in the same range. Dial access codes can start with any number from 0-9, * or # and can contain up to 4 digits. If an extension entry and a DAC entry have the same Dialed String, the extension entry can be longer than the DAC entry only if all of the trunk groups covered by that DAC entry have Dial Access on the Trunk Group screen set to "no." You can use the DAC to activate or deactivate a Communication Manager feature or to seize a trunk from a trunk group, or both. In the first case, the DAC functions as a FAC, in the second as a TAC. For example, you can define the group 300-399 for dial access codes, and allow both FAC and TAC in that range. You can use 4-digit DACs for ordinary trunk access, but they do not work for attendant control of trunk groups, trunk-ID buttons, or DCS, and only the last 3 digits of the codes can be recorded in CDR records. See also the description below for **fac**.

Valid entries	Usage
ext	Primary extension. The system uses this call type to define extension ranges that can be used on your system. Extension can have a first digit of 0 through 9 and can be 1 - 13 digits in length. Extension cannot have the same first digit as a 1-digit ARS or AAR Feature Access Code (FAC). When a dial plan has mixed station numbering, extensions of various lengths (all with the same first digit) are mapped on the Dial Plan Analysis table. The system then employs an inter-digit time-out to ensure that all dialed digits are collected. You can have multiple entries of call type ext with the same dialed string, but you must have different valid lengths.
fac	Feature access code. The system uses this call type to define Feature Access Codes only. A FAC can be any number from 1-9 and contain up to 4 digits. You can also use * or #, but only as a first digit. Avaya recommends that a FAC have the longest total length for a given dialed string when using mixed numbering. Otherwise, problems may occur when, for example, 3-digit FACs and 4-digit extensions begin with the same first digit and the FAC is an abbreviated dialing list access code. However, if the entry in the dial plan that defines the FAC is used to define the AAR or ARS access code, then it *must* have the longest total length in the dial plan.
pext	Prefixed extension. The system uses this call type to define prefixed extensions. A prefixed extension is made up of a prefix (first digit) that can be a **0**-**9** (* and # not allowed), and an extension number of up to 5 digits in length. The maximum length of a prefix and extension combination is 6 digits. You cannot administer a dial access code with the same first digit as a prefixed extension. The purpose of the prefix is to identify the call type as an extension. After digit collection, the prefix digit is removed from the string of dialed digits. The remaining digits (extension number) are then processed. A prefixed extension allows the use of extensions numbers with any dialed string (the extension length must be specified on the table). The "prefixed extension" cannot have the same dialed string as the ARS or AAR facility access code (FAC).

Valid entries	Usage
udp	Uniform Dial Plan. This call type works identically with the ext call type, with this exception: • If dialed digits match the call type of udp, Communication Manager automatically checks the UDP Table first to see if there is a match, regardless of the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen. If there is no match, Communication Manager then checks the local server. • If dialed digits match the call type of ext, Communication Manager checks the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen. – If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **udp-table-first**, Communication Manager checks the UDP Table first to see if there is a match. If there is no match, Communication Manager then checks the local server. – If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **local-extensions-first**, Communication Manager checks the local server first to see if there is a match. If there is no match, Communication Manager then checks the UDP Table. The udp call type allows Communication Manager to recognize strings of 14 and 15 digits, which are longer than the maximum extension length of 18 digits. However, the udp call type can be used with any length in case this provides a useful new capability to customers.

Note:
The **Percent Full** field displays the percentage (0 to 100) of the system's memory resources that have been allocated for the dial plan that are currently being used.

6. Press **Enter** to save your changes.

Adding extension ranges

Before you assign a telephone to an extension, the extension must belong to a range that is defined in the dial plan. In this example, you are adding a new set of extensions that start with 3, and are 4 digits long (3000-3999).

To add this set of extensions to the dial plan:

1. Type **change dialplan analysis**. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen Figure 180: Dial Plan Analysis Table screen on page 808.
2. Move the cursor to an empty row.
3. In the **Dialed String** column, type **3**. Press **Tab** to move to the next field.
4. In the **Total Length** column, type **4**. Press **Tab** to move to the next field.
5. In the **Call Type** column, type **ext**.
6. Press **Enter** to save your changes.

Defining a multi-location dial plan

Prerequisites

- On the Optional Features screen, ensure that the **Multiple Locations** field is set to **y**. If this field is not set to **y**, you cannot administer the Multi-Location Dial Plan feature. Contact your Avaya representative for assistance.

  To view the Optional Features screen, type **display system-parameters customer-options**. Press **Enter**.

Considerations for Dial Plan

This section provides information about how the Dial Plan feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Dial Plan feature under all conditions:

- You cannot assign prefixed extensions longer than five digits (including prefix) to intercom lists.
- Although extensions with the same first digit can have different lengths, data-channel extensions must have the maximum number of digits to avoid timeout problems for data calls that Communication Manager automatically sets up, for example, the **CDR** link.
- An extension and a FAC can share the same first digit only if the extension is longer as long as they are not used for **AAR**/**ARS** faxes. These extensions work only within Communication Manager; they do not work as remote **UDP** extensions.

- When you design your dial plan or add new information to your dial plan, be careful if you assign the same first digit to more than one FAC. Your system may need to distinguish between FACs with the same first digit by using the **Short Interdigit Timer** field on the Feature Related System Parameters screen.

Interactions for Dial Plan

This section provides information about how the Dial Plan feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the Dial Plan feature in any feature configuration.

- Attendant Display and Telephone (Voice Terminal) Display

  Prefixed extensions display without the prefix. The return call button causes the prefix to dial, even though it does not display.

- Integrated Services Digital Network-Basic Rate Interface (ISDN-BRI)

  When an ISDN-BRI station dials sufficient digits to route a call, but the call could route differently if additional digits were dialed, the station does not recognize the Conference or Transfer buttons. The user must delay dialing for 3 seconds or dial # to indicate that the call can be routed based on the digits already dialed. The Conference or Transfer buttons then are recognized and Communication Manager completes the operation.

- Multifrequency (MF) Signaling

  Flexible numbering is supported in countries using R2-MFC trunk signaling without Group II tones. Different-length extensions can exist as long as the extensions have different first digits.

- Property Management System (PMS)

  PMS products accept only extensions of 5 digits or shorter. Therefore, a customer using PMS cannot use 6/7-digit extensions.

  If any of the following is administered on the Hospitality System Parameters (HSP) screen, you cannot administer an **ext** entry on the Dial Plan Analysis screen with a length greater than 7, even if Special Application SA8662 is enabled:

  — PMS Log Endpoint

  — Journal/Schedule Endpoint

  Likewise, you cannot enter a value in either of the above HSP fields if the Dial Plan Analysis screen has any ext entries longer than 7 digits.

  You can administer **PMS**, **PMS_JOURNAL**, and **PMS_LOG** fields on the IP Services screen, but these fields cannot be entered on the Hospitality System Parameters screen.

- Uniform Dial Plan

- The following limitations apply to a **DCS** environment:
  - Extensions that differ in length from the **UDP** do not distribute to other servers or switches.
  - You can use only a single length in your UDP.
- Single-Digit Dialing
  - A prefixed extension is still made up of a prefix and an extension of up to five digits.
  - Mixed station numbering extensions can have 1 - 13 digits.

The following are the interactions for Multi-location Dial Plan.

- Attendant

  This feature provides a way to administer multiple attendant codes. This does not provide a way to administer multiple attendant groups. Only one attendant group is allowed per switch, unless you have attendant partitioning. This feature does provide a way to support multiple local centralized answering points. The LCAPs do not utilize attendant groups to support this.

- Attendant Vectoring

  If attendant vectoring is enabled, it will take precedence over any local attendant codes administered. This is how attendant vectoring currently works. Attendant seeking or "dial 0" calls (local attendant codes, attendant code on the dial plan screen or attendant access code on the Feature Access Code (FAC) screen) are processed using call vectors and not using the normal attendant console call routing.

- Automatic Circuit Assurance

  The field **ACA Referral Destination** on page 1 of the System Features Parameters screen requires either the **attd** administration on the Dial Plan Analysis Table screen, or administration of the attendant access code on the Feature Access Code (FAC) screen. This field requires that an attendant group exists.

- Automatic Wakeup

  If a station has automatic wakeup requests pending when the **change extension-station** command is run, the wakeup requests are canceled.

- Call Forwarding

  Any call forwarding information stored with an extension is lost when using the **change extension-station** command. If the station that is changed with the **change extension-station** command is a forwarded-to station, the extension using that forwarded-to extension must be manually updated. If not, calls are not forward correctly.

- Call Park

  This feature does not support common shared extensions on the console parameter to park calls. Since common shared extensions are not assigned to physical stations, the range of common shared extensions should be able to be shared in all locations.

- Crisis Alert

  The **Originating Extension** on the Crisis Alert System Parameters screen is not updated by the **change extension-station** command. It must be manually updated if the originating extension field was changed.

- Leave Word Calling (LWC)

  The field **Stations with System-wide Retrieval Permission for the Leave Word Calling Parameters** on page 2 of the System Features Parameters screen require either the **attd** administration on The Dial Plan Analysis Table screen, or administration of the **Attendant Access Code** on the Feature Access Code (FAC) screen. This field requires that an attendant group exists.

- LSP

  If the **change extension-station** command is run on the controller, but the translations are not also saved to the Local Survivable Processor (LSP), the two system translations might not be synchronized.

- Night Service

  Location-based Night Service is not supported. A customer may want to restrict attendant-seeking calls to attendants who are local to the calling party. The reason is the local attendant would most likely speak the same language as the caller. Those customers would want an attendant to be able to put one location only into Night Service, without putting the entire switch into Night Service.

  One way to accomplish this is to use hunt groups as attendant queues. Each hunt group can be put into Night Service separately, and have its own Night Service destination. In addition, the Night Service destination can be administered by tenant, by trunk group, and by trunk group number.

- Station Hunting

  Changing a station extension with the **change extension-station** command maintains the station hunting chain.

- Survivable Remote EPN/WAN Spare Processor

  If an administrator runs the **change extension-station** command in a configuration where a survivable remote processor exists, and the command is not run on the survivable processor, when the remote processor takes control, the extensions that were changed on the server will not exist on the survivable remote.

- Uniform dial plan (UDP)

  If an administrator runs the **change extension-station** command, extensions that were typed into the UDP screen are not updated. The change to the UPD table is handled by external system management tools that Avaya supports, but it is not changed by this command.

The following Communication Manager features, operations, and systems require a user to dial an extension after dialing a Feature Access Code (FAC) or pressing a button. These features support the dial plan expansion to 13 digits:

- Add/Remove Agent Skill
- Agent Login/Logout
- Attendant Call Forwarding
- Call Park
- Call Pickup, including Directed Pickup
- Code Calling/Deluxe Paging
- Controlled Restrictions
- EC500 (Extension to Cellular)
- Enhanced Call Forwarding
- Enterprise Mobility User (EMU) – EMU relies on the Uniform Dial Plan for passing numbers through the network. Therefore, all systems in a QSIG network must be upgraded to Communication Manager 4.0 if an EMU user with an extension longer than 7 digits wishes to visit another site in the network. If not all systems are upgraded to Communication Manager 4.0 and extensions on the upgraded systems are expanded beyond 7 digits, EMU features will not work properly.
- Intercom Calling
- Leave Word Calling
- Malicious Call Trace
- Personal Station Access (PSA)
- Posted Messages
- Priority Calling
- Refresh Terminal Parameters
- Remote Access
- Service Observing
- Station Busy Verify
- Terminal Translation Initialization
- Whisper Paging

The following features, operations, and systems also support the dial plan expansion to 13 digits:

- Abbreviated Dialing (AD) – An extension that is stored in an AD button will not be converted automatically when the station with that extension is changed. So if you use the **`change extension-station`** command to convert a short extension to a longer extension, any AD button that is programmed with an extension must be reprogrammed.
- Application Enablement Services (AES)
- ASAI and CTI API.

Note:
Device, Media, and Call Control (DMCC) does not support the expansion to 13 digits at this time.

- Attendant Direct Extension Selection (DXS) with Busy Lamp
- Attendant Display
- Attendant Vectoring
- Automatic Call Distribution (ACD)
  - With no reporting
  - With reporting by Basic Call Management System (BCMS)
  - With reporting by the next generation of Call Management System (CMS)

Note:
Reporting is not supported by Release 14 of CMS.

- Automatic Customer Telephone Rearrangement (ACTR)
- Basic Call Management System (BCMS) – Non-EAS agent BCMS/VuStats Login IDs also support the expansion to 13 digits. This maximum length is a function of the **ACD Login Identification Length** field on the Feature-Related System Parameters screen, and login IDs entered on the BCMS/VuStats Login ID screen, and not a function of any **ext** entry in the Dial Plan.

Note:
The BCMS/VuStats login IDs are optional when Expert Agent Selection (EAS) is not active. However, if EAS is active, login IDs are required.

Important:
On EAS-enabled systems, login IDs can only be nine digits long. If you want to upgrade to the EAS system at a future date, you must limit the login ID length to nine or fewer digits.

- Best Service Routing (BSR) – The **Status Poll** and **Interface VDN** fields in the BSR application tables already support 16-digit strings.
- Call Vectoring
- Direct Inward Dialing (DID)
- E911
- Expert Agent Selection (EAS): Logical Agents
- Extension Number Portability (ENP)
- External Reporting Adjunct interface – The external reporting interface messaging protocol Switch Processor Interface (SPI) is enhanced to support the expanded dial plan. However, the existing reporting adjunct CMS is not enhanced to support the expanded dial plan. See Call Management System (CMS), CMS Supervisor, and Operation Analyst (OS) in the next section.

- IP Agent, Release 7
- Multi-Level Precedence and Preemption (MLPP) – The MLPP feature works with short-extension dialing in CM4.0. For a user to be able to dial an MLPP access code followed by a short extension, the **Conv** field on the Precedence Routing Digit Conversion screen must be set to **y**. This lets the UDP Table do the required short-extension-to-long-extension conversion.
- QSIG Message Waiting Indication (MWI) – The DCS/messaging feature is unable to light the Message Waiting lamps of remote stations with extensions longer than 7 digits.
- Session Initiation Protocol (SIP)
- SIP Enablement Services (SES)
- Standard Local Survivability (SLS) on G250 and G350 Media Gateways, and the TGM 550 gateway module
- Meet-Me Conferencing
- VuStats – VuStats displays support longer agent, split, and VDN extensions. If you have Communication Manager Release 3.1 using VuStats Display Formats that contain 7-digit extensions, you must update these formats to accommodate the longer extensions. The system does not update the formats automatically when the extension size for a particular first digit is increased.

  Note:
  When longer extensions are used, the fixed 40-character station display cannot accommodate as much other data.

  Also see Basic Call Management System (BCMS) earlier in this section concerning BCMS/VuStats Login IDs.

The following Communication Manager features and operations do not support the dial plan expansion to 13 digits:

- Administrable Attendant Access Code – This feature is only one or two digits long.
- Announcements – Recording for the Announcements feature is not updated to 13-digit dialing, and remains at the maximum of 7-digits.
- Call Management System (CMS), CMS Supervisor, and Operation Analyst (OS) – Release 14 CMS/ CMS Supervisor, and OA are not enhanced to support greater than 7 digits for any extension data it receives. If CMS is administered as a reporting adjunct, administration of dial plans greater than 7 digits is not allowed.

  Note:
  Once any extension is set to more than 7 digits without CMS administered, you cannot later add CMS to the system.
- Basic Communication Management Reporting - Desktop (BCMR-D) – This product interfaces with Basic Call Management System (BCMS).

- Distributed Communications System (DCS and DCS+) – DCS is restricted to 4-digit and 5-digit dialing. DCS customers must migrate to QSIG to maintain feature transparency with a longer dial plan.
- Hospitality features, except:
  - Automatic Wakeup – A station with Console Permissions can enter an Automatic Wakeup request for an extension up to 13 digits long. However, the related station displays only show the trailing 7 digits.

Note:
No adjustment is made to the formats that the system sends to the Wakeup Printer. Extensions longer than 7 digits cannot be administered if a Wakeup Printer is administered.

  - Do Not Disturb – A station with Console Permissions can enter a Do Not Disturb request for an extension up to 13 digits long. However, the related station displays only show the trailing 7 digits.

ISDN-BRI data endpoints – When a BRI data endpoint is added, the **Service Profile Identifier** (SPID) field continues to default to the new extension, up to 10 digits. If the endpoint does not support SPIDs, the administrator must disable **Endpoint Initialization**.

Dial Plan Transparency

The Dial Plan Transparency feature preserves users' dialing patterns when a media gateway registers with a local survivable processor (LSP), or when a Port Network requests service from an Enterprise Survivable Server (ESS).

Note:
This document uses the term "LSP" in contexts where both LSP and ESS scenarios apply. Please keep in mind that LSPs accept registrations from Media Gateways, while ESSes provide service to Port Networks.

Detailed Description of Dial Plan Transparency

When a media gateway registers with a local survivable processor (LSP), or when a Port Network requests service from an Enterprise Survivable Server (ESS), the Dial Plan Transparency feature routes calls over the public network when they cannot be routed over the IP network. Note that this feature does not provide alternate routing for calls between port networks connected through networks other than IP (for example, ATM or DS1C) and that request service from different ESS servers during a network outage.

Administering Dial Plan Transparency

The following steps are part of the administration process for the Dial Plan Transparency feature:

- Setting up Dial Plan Transparency

This section describes:

- Any prerequisites for administering the Dial Plan feature
- The screens that you use to administer the Dial Plan feature
- Complete administration procedures for the Dial Plan feature

Prerequisites for administering Dial Plan Transparency

You must complete the following actions before you can administer the Dial Plan Transparency feature:

- None

Screens for administering Dial Plan Transparency

Screen name	Purpose	Fields
Feature-Related System Parameters	• Enable the DPT feature for your system. • Indicate the Class of Restriction to use for the Dial Plan Transparency feature.	• **Enable Dial Plan Transparency in Survivable Mode?** • **COR to use for DPT**
IP Network Region	Administer the DPT feature for Network Regions.	• **Incoming LDN Extension** • **Dial Plan Transparency in Survivable Mode?**
System Parameters-ESS	Enter the community assignments for each Port Network.	Community

Setting up Dial Plan Transparency

Administration of Dial Plan Transparency (DPT) is similar to setting up Inter-Gateway Alternate Routing (IGAR). You must first enable the DPT feature, then set up Network Regions and trunk resources for handling the DPT calls. For ESS servers, you must also assign Port Networks to communities.

To set up Dial Plan Transparency:

1. Type **`change system-parameters features`**, and press **Enter**.

   The system displays the Feature-Related System Parameters screen. Page down until you see the SYSTEM-WIDE PARAMETERS fields (Figure 181: Feature-Related System Parameters screen on page 823).

Figure 181: Feature-Related System Parameters screen

```
change system-parameters features                                  page 5 of x
                          FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint: ____           Lines Per Page: 60       EIA Device Bit Rate:


SYSTEM-WIDE PARAMETERS
                                    Switch Name: _________________
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                              COR to Use for DPT:

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n  MCT Voice Recorder Trunk Group: ___
      Delay Sending Release (seconds)?
SEND ALL CALLS OPTIONS
           Send All Calls Applies to: station
      Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? n
                                              UCID Network Node ID: ___
```

2. In the **Enable Dial Plan Transparency in Survivable Mode** field, enter **y**.
3. In the **COR to Use for DPT** field, enter the Class of Restriction to use for Dial Plan Transparency. The default is **station**, where the FRL of the calling station determines whether that station is permitted to make a trunk call and if so, which trunk(s) it is able to access.
4. Type **`change ip-network region n`**, where ***n*** is the number of the Network Region to change. Press **Enter**.

   The system displays the IP Network Region screen. Page down until you see the INTER-GATEWAY ALTERNATE ROUTING/DIAL PLAN TRANSPARENCY fields (Figure 182: IP Network Region screen on page 824).

Figure 182: IP Network Region screen

```
 change ip-network-region n                                    Page 2 of x

                                  IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING/DIAL PLAN TRANSPARENCY
Incoming LDN Extension:
Conversion to Full Public Number - Delete: ___Insert: ___
 Maximum Number of Trunks to Use for IGAR:
Dial Plan Transparency in Survivable Mode? n


BACKUP SERVERS IN PRIORITY ORDER            H.323 SECURITY PROCEDURES
1                                           1
2                                           2
3                                           3
4                                           4
5
6                                          Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? y
                        Near End TCP Port Min: 61440
                        Near End TCP Port Max: 61444
```

5. In the **Incoming LDN Extension** field, If not already done for IGAR, allocate one incoming DID/LDN extension for incoming DPT calls. This extension can be shared by IGAR and DPT – the system will distinguish incoming IGAR calls from incoming DPT calls.
6. In the **Dial Plan Transparency in Survivable Mode** field, enter **y**.
7. Ensure that each IGAR/DPT-enabled Network Region has sufficient trunks for the expected number of outgoing and incoming DPT calls. There is no need to set the maximum number of trunks for DPT.
8. Use existing routing techniques to ensure an outgoing DPT call from a given Network Region will have access to an outgoing trunk. Unlike IGAR, the outgoing trunk need not be in the same Network Region as the calling endpoint, as long as the endpoint and trunk Network Regions are interconnected.
9. If you are setting up DTP for an ESS, type **`change system-parameters ess`**. Press **Enter**.

   The system displays the System Parameters-ESS screen. Page down to page 6. (Figure 183: System Parameters - ESS screen - page 6 on page 825).

Figure 183: System Parameters - ESS screen - page 6

```
change system-parameters ess                                    Page 6 of x

            COMMUNITY ASSIGNMENTS FOR PORT NETWORKS
PN Community PN Community PN Community PN Community PN Community
------------ ------------ ------------ ------------ ------------
 1: 1         14: 1        27: 1        40: 1        53: 1
 2: 1         15: 1        28: 1        41: 1        54: 1
 3: 1         16: 1        29: 1        42: 1        55: 1
 4: 1         17: 1        30: 1        43: 1        56: 1
 5: 1         18: 1        31: 1        44: 1        57: 1
 6: 1         19: 1        32: 1        45: 1        58: 1
 7: 1         20: 1        33: 1        46: 1        59: 1
 8: 1         21: 1        34: 1        47: 1        60: 1
 9: 1         22: 1        35: 1        48: 1        61: 1
10: 1         23: 1        36: 1        49: 1        62: 1
11: 1         24: 1        37: 1        50: 1        63: 1
12: 1         25: 1        38: 1        51: 1        64: 1
13: 1         26: 1        39: 1        52: 1

Enter number between 1 and 64
```

10. In the **Community** field, enter the community assignments for each Port Network. Assigning an ESS server to a community associates the ESS server with the IPSI(s) (IP Interface Server) in the Port Network(s) for that community. The association effects how the ESS server is prioritized for the IPSI in that community, if the ESS server is administered with a Local Preferred or Local Only preference.

Note:
For more information on Enterprise Survivable Servers, see *Using Avaya Enterprise Survivable Servers (ESS)*, 03-300428.

Maintenance for Dial Plan Transparency

Alarms

Alarms should already exist when an LSP or ESS becomes active. No new alarms are introduced when a media gateway goes into LSP mode.

Audits/Logging

As with IGAR and most other features, CM logs Denial Events to help debug cases when a DPT trunk call cannot be launched.

Debugging/Diagnostic Tools

For calls that are launched but do not terminate properly, tools such as List Trace, List ARS Route-Chosen, Call Detail Recording, and Message Sequence Tracer can help diagnose the problem. List Trace shows the outgoing trunk call placed on behalf of the user when DPT is invoked.

Considerations for Dial Plan Transparency

This section provides information about how the Dial Plan Transparency (DPT) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Dial Plan Transparency under all conditions. The following considerations apply to Dial Plan Transparency:

- DPT only handles WAN connectivity failures between Network Regions. It does not cover the following cases:
  - Two Gateways in the same Network Region, registered to the same server (main or LSP or ESS), cannot reach each other due to LAN congestion or failure. Note that this case cannot be handled by IGAR either.
  - A Gateway becomes disconnected from the main server and cannot register with an LSP or ESS at all. In such a case the gateway will enter Standard Local Survivability mode, which provides basic call processing functionality during the outage.
- Failover strategies for Gateways and Port Networks, and alternate gatekeeper lists for IP stations must be in harmony. DPT will not cover cases such as the following:
  - Two Gateways or Port Networks in the same Network Region register to different LSP or ESS servers during a network outage.
  - Two IP endpoints in the same Network Region register to different servers during a network outage.
- Because DPT calls are trunk calls, most station features cannot be supported. DCS and QSIG features are not supported, even if the trunk carrying the DPT call supports DCS or QSIG. CM displays a new reason code to alert users about the reduced functionality.

- The biggest known limitation for DPT in CM 4.0 is that DPT is not triggered on redirected calls. Broadening the range of calls that trigger DPT is an important part of a DPT Phase 2.

Fiber PNC with Remote PNs

Fiber PNC refers to a Center-Stage Switch, ATM-PNC, DS1C-PN. Please note the following:

- Customers wanting DPT for ESS-controlled Port Networks (PNs) must migrate those PNs from Fiber-PNC to IP-PNC. Fiber-connected cabinets must be in Network Region 1.
- Fiber-PNC users can reach disconnected users in other Network Regions through DPT.
- IP-PNC/GW can only initiate DPT calls to the fiber-PNC fragment that contains the trunks associated with the IGAR LDN.
- Users connected through Fiber-PNC cannot use DPT if another fiber PN fails over to different ESS server. This is because DPT is not triggered within same Network Region.

Interactions for Dial Plan Transparency

This section provides information about how the Dial Plan Transparency (DPT) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Dial Plan Transparency in any feature configuration.

Overview

Because DPT calls are trunk calls, many CM features cannot be supported. DCS and QSIG features are not supported, even if the trunk carrying the DPT call supports DCS or QSIG (including SBS), because the call is not being originated in the normal way.

When you set up a multi-gateway server, it is unlikely that they will set up and maintain a DCS or QSIG net-work in parallel to support feature transparency in case of network fragmentation. Therefore, the only ways to get additional features to work are (1) in-band signaling over the DPT trunk before ringing the called party, or (2) out-of-band signaling using Q.931 messages; however, In-band signaling delays call setup, and Out-of-band signaling is generally not possible over normal public network ISDN connections.

AAR/ARS partitioning

ARS partitioning is used when routing the DPT trunk call, if the station COR is used to route the call. If not, then ARS Partition 1 is used.

Abbreviated Dialing

DPT is invoked whether the caller dials using the keypad or by pressing an Abbreviated Dialing button.

Alternate facilities restriction levels

If the calling station has invoked its Alternate facilities restriction level (FRL) and the station COR is used to route the call, the Alternate FRL is used.

Announcements

External announcements are not supported if the adjunct does not have access to the LSP.

Attendants

Calls to or from an attendant invoke DPT.

Authorization Codes

If the station COR is used to route DPT calls, and a caller's FRL is not high enough to access a Route Pattern Preference, and authorization codes are enabled, then the caller is prompted to enter an authorization code. This might be a surprise to some callers, but those with displays will recognize the reason for the prompting. If the unrestricted COR is used to route DPT calls, the call routes without prompting the caller.

Automatic Callback

Automatic callback (ACB) is not supported when the initial call has routed through DPT, even if the DPT call routes over a DCS or QSIG trunk group with TSCs enabled.

ANI

If an incoming ISDN call is routed using DPT, and the outgoing DPT call also travels through ISDN, the Calling Party Number IE received on the incoming call is passed on with the DPT call, and that number is displayed to the called user. It is under investigation to what extent this works with other trunks that provide Caller ID such as MFC trunks.

ARS

ARS is used to route DPT calls. The user must administer the ARS analysis forms to support Dial Plan Transparency for LSP and ESS fragments.

Bridging

Bridged appearances within an LSP fragment will function properly. However, bridging is not supported across LSP fragments, so DPT cannot be invoked by means of a user pressing a bridged appearance button.

If a server becomes active in LSP mode and bridged appearances exist across LSP fragments, bridging is not supported. For calls that originate from a call appearance with a bridged extension not local to the LSP, the bridged extension does not show/have access to the call. Calls cannot originate on a bridged extension if the principal extension is not local to the LSP server. For incoming calls to an extension on an LSP, the bridged extension does not alert if it is not local to the LSP server.

Busy Indicator

The busy indicator button is not supported across disconnected network fragments.

Call Detail Recording

CDR records are stored in a buffer while in LSP mode. Since the CDR adjunct is administered on the main server, no data can be sent to the adjunct from the LSP. Therefore, if the CDR buffer hits its capacity, CDR records are overwritten and data is lost.

Call Forwarding

Several scenarios must be considered. Assume the parties involved are A, B, and C, where A calls B, and B is forwarded to C.

- A and B are in the same Network Region; C is in a Network Region accessible only through DPT. This is not a principal termination and so DPT is not invoked – instead, the call either follows B's coverage path, or busy tone is played back to A.
- B and C are in the same Network Region; A can access B only through DPT. The initial call from A to B is a principal termination, and therefore works fine, and C sees a forwarding indication on its display. However, A does not see a forwarding indication, since no indication is passed back to A over the DPT trunk.
- If A, B, and C are all in LSP fragments, the result is a combination of the above two cases, and the first one overrides – the call is not forwarded from B to C, but either follows B's coverage path, or busy tone is played back to A.

Call Park

Call parking is not supported between disconnected network fragments.

Call Pickup

Call pickup is not supported across disconnected network fragments.

Conference

Conferencing is supported while in LSP mode, but the count of conference parties is different. That is, if two parties on a conference are in the LSP and two are on the main server, each station sees CONFERENCE 2, meaning each side is only aware of three parties on the conference: the two stations and the DPT trunk.

Note also that the system does not optimize trunk connections (as happens with IGAR), nor are the DCS or QSIG Path Optimization features available. Therefore, a conference call could use up many more trunks than are actually necessary; users would have to recognize the LSP condition (perhaps because of the reason code on their display) and would have to optimize trunk usage “manually” (for example, by conferencing together parties in the same LSP fragment).

Coverage

Call coverage is not a principal termination, so CM 4.0 does invoke DPT, even if the call is covering to a voice mail adjunct. That is, if A calls B, and B normally covers to C, there are two cases:

- If C is accessible to B, coverage takes place and C rings. “Accessible” means that the server controlling B’s gateway also controls C’s gateway.
- If C is not accessible to B, then the call rings forever at B. To get the call to cover to C in this case, the customer must use the Remote Coverage solution.

In the latter case, if A and B are not controlled by the same server, Remote Coverage through a trunk is initiated by B’s server, not A’s server.

Crisis Alert

The Crisis Alert feature causes CM to alert an attendant when an emergency call is placed. As described elsewhere, DPT does not alert members of an attendant group in a disconnected gateway. However, attendants accessible to the caller are alerted.

E911

Calls to an emergency number such as 911 in North America work normally, since those calls generally travel out over trunks local to the caller’s home gateway. We do not expect DPT to be invoked.

EC500

An incoming DPT call can invoke EC500 – that is, it can generate a trunk call to a cell phone or other re mote endpoint – assuming outgoing trunks are available on the server controlling the called party.

Enterprise Mobility User

In CM 4.0, Dial Plan Transparency will not support Enterprise Mobility User (EMU). There are two cases, depending on when EMU is activated.

If User A on a disconnected gateway calls User B, and if User B had EMU active *before* User A's gateway became disconnected, then the DPT call will not be launched to User B. Instead, the call will proceed, if possible, to the next coverage point.

If User A on a disconnected gateway calls User B, and if User B activated EMU *after* User A's gateway became disconnected, then the DPT call *will* be launched to User B, and the remote EMU "visiting" phone will be alerted, as per normal EMU operation.

Group Paging

Group Paging is not supported across LSP fragments.

Hunt Groups

Calls to hunt groups are not supported between LSP fragments. The problem with supporting hunt groups is the unknown state of the members in the hunt group. For example, you may know that the station is OOS because you are in LSP mode, but you don’t know if that station is on another call since you no longer have control of it.

The ports in a Voice Mail hunt group seldom span gateways. The Remote Coverage solution described elsewhere addresses calls that are placed directly to, or that cover to, a Voice Mail hunt group whose ports are in a disconnected gateway (typically on the main server).

Intercom

Intercom calls are not support between LSP fragments.

IP Endpoints

Because an IP endpoint does not have a physical port, CM software cannot be as sure as with digital or analog endpoints what Network Region it belongs to.

With an IP Softphone, the problem is even more acute. A Telecommuter or Road Warrior using an IP Softphone may log in and out several times during a WAN outage and register with different servers (the main or an LSP or ESS). Thus, an IP Softphone's Last Network Region may be out of date, causing CM software to route DPT calls to that Softphone using the LDN of the wrong Network Region. If that wrong Network Region is disconnected from the actual Network Region of the Softphone, the call will fail. (By contrast, if the wrong Network Region happens to be connected to the actual Network Region, the call will succeed.)

In such a case, the Telecommuter or Road Warrior may need to give an alternate PSTN number at which they can be reached. Outgoing calls from an IP Softphone registered to an LSP or ESS trigger DPT and work properly.

Last Number Dialed

DPT is invoked whether the caller dials using the keypad or by pressing a Last Number Dialed button.

Leave Word Calling

Leave Word Calling (LWC) is not supported when the initial call has routed through DPT, even if the DPT call routes over an SDN/DCS+ trunk group. To get LWC to work over an SDN/DCS+ trunk group, the customer would have to be using 4-digit or 5-digit UDP dialing and have TSCs enabled. But such a customer does not really need DPT, because they get better feature transparency among their gateways without it.

Note that LWC is used primarily by Voice Mail systems that use Digital Set Emulation (that is, they simulate a DCP endpoint). They use the LWC Store and LWC Cancel Feature Access Codes to light and turn off message waiting lamps.

Loudspeaker paging

Loudspeaker paging is not supported between LSP fragments.

Malicious Call Trace

If the recipient of a DPT call invokes Malicious Call Trace (MCT), the results visible to the MCT Controller and on the MCT History log are the same as for an incoming trunk call. The identity of the calling station is not displayed.

Meet-me Conference

Each LSP or ESS has its own "copy" of a Meet-Me Conference VDN and vector when a system breaks up due to a WAN outage. Thus, callers in disconnected gateways may dial into the "same" Meet-me Conference (MMC), but these are separate conferences. Since an MMC does not have a physical port or Network Region, DPT is not triggered to merge these conferences together.

Message Retrieval

Retrieval of Leave Word Calling messages is not supported while in LSP/ESS mode if the messages are stored in a remote Voice Mail server (typically CM Messaging).

Multi-Level Precedence and Preemption

The caller's precedence level is not transmitted when DPT launches a trunk call. Therefore, a high-ranking caller that invokes DPT will not preempt an existing trunk call, nor will a high-ranking caller placing a precedence call preempt a trunk call launched by DPT.

No-Hold Conferencing

A call initiated by the No-Hold Conferencing (NHC) feature triggers DPT. As soon as the DPT signaling has completed, the trunk is conference into the call and the parties hear the normal conference tones (if applicable).

Personal Station Access

During network fragmentation, an LSP or ESS is not notified about users on remote gateways associating their stations using PSA. Thus, DPT is not triggered on a call to a station that was associated through PSA during the outage.

Priority Calling

A Priority Call can invoke DPT, but the called party does not ring with the Priority (typically 3-burst) ring pattern, even if the DPT call routes over a DCS or QSIG trunk group.

Service Observing

A user cannot use Service Observing to monitor a user served by a disconnected LSP or ESS. Remote Service Observing works, but the observer must be notified that the network has fragmented before knowing to invoke Remote Service Observing.

Station Lock

Locking a station changes its COR. Thus, if the Station Lock COR blocks outgoing trunk calls, and the **COR to Use for DPT** system parameter is set to **station**, then the locked station cannot make DPT calls, while the unlocked station can do so.

TTI

During network fragmentation, an LSP or ESS is not notified about users on remote gateways associating their stations using TTI. Thus, DPT will not be triggered on a call to a station that was associated through TTI during the outage.

Transfer

A call initiated as part of a transfer operation can trigger Dial Plan Transparency. This includes all types of transfer (station & attendant, normal & pull transfer, and so on)

Transfer into/out of Voice Mail

A call initiated as part of a Transfer out of Voice Mail operation can trigger DPT – it looks like a normal call placed by a QSIG trunk or hunt group member.

Transfer into Voice Mail sets up a call to the Voice Mail Hunt Group, all of whose members are out of service during network fragmentation. It can be made to work by assigning a Coverage Path to the Hunt Group – see the subsection on Voice Messaging.

Voice Messaging

Covering to Voice Mail

Normal coverage scenarios are described in Coverage on page 830. The Remote Coverage solution allows calls covering to voice mail to get the proper greeting during network fragmentation.

This can come into play in two ways:

- The called party and the VM server are in the same Network Region (or in Network Regions that are still connected). In this case, normal coverage routes the call to the VM server and the correct greeting is played.
- The called party and the VM server are in disconnected Network Regions. In this case, a special Remote Coverage point in the called party's coverage path gets the call to the Voice Mail server and ensures that the correct greeting is played.

In both cases, the calling party information stored with the VM message is taken from the incoming trunk. If the trunk is ISDN, the full calling party number may be received; if so, the VM server will store it (for example, 732-852-1234 rather than the extension 21234).

You can use this calling number with the Off-PBX Station Mapping screen to make the trunk call from the disconnected Network Region look even more like a local call from a connected Network Region.

Retrieving Voice Messages

A user may dial the internal extension of the Voice Mail Hunt Group to access/retrieve voice messages on a QSIG-connected VM server or a CM Messaging server. Without any special changes, doing so will result in busy tone, because the hunt group or QSIG trunk group members are out of service from the point of view of the LSP or ESS. Thus, users must have a way of automatically dialing “out” through the PSTN to the VM server while their Media Gateway is served by an LSP or ESS.

This can be done by assigning a Coverage Path to the Voice Mail Hunt Group itself, with a special Remote Coverage point that is only active when the caller is on a Gateway in LSP or ESS mode.

Message Waiting Lamps

Note that whenever the Media Gateway is disconnected from the VM server, Message Waiting lamps are stuck in the on or off state until the Media Gateway reregisters, and the VM server updates the lamps.

Whisper Paging

A call initiated as part of a Whisper Paging operation can trigger DPT.

Distinctive Ringing

Use the Distinctive Ringing feature to distinguish between incoming call types based on the ringing pattern of the call.

Detailed description of Distinctive Ringing

This section provides a detailed description of the Distinctive Ringing feature.

For multiappearance telephones, you can administer the system-wide distinctive-ringing cycles. You cannot administer system-wide distinctive-ringing cycles for single-line analog telephones. For single-line analog telephones, you must administer the ringing cycle for the user on a Station screen. For more information, see the "Personalized Ringing" feature.

Most installations use a one-burst ring for internal calls, a two-burst ring for external calls, and a three-burst ring for priority calls.

The system controls the ringing cycles for the following types of calls. You can administer ringing for:

- Automatic and Dial Intercom calls
- Manual Signaling calls
- Redirect Notification calls

If the user of an internal telephone transfers an external call, the call usually rings as an internal call. You can administer the system so that the transferred call rings as an external call.

Administering Distinctive Ringing

The following steps are part of the administration process for the Distinctive Ringing feature:

- Defining Distinctive Ringing

This section describes:

- Any prerequisites for administering the Distinctive Ringing feature
- The screens that you use to administer the Distinctive Ringing feature
- Complete administration procedures for the Distinctive Ringing feature

Prerequisites for administering Distinctive Ringing

You must complete the following actions before you can administer the Distinctive Ringing feature:

- None

Screens for administering Distinctive Ringing

Screen name	Purpose	Fields
Feature-Related System Parameters	Assign the number of rings for a priority call.	**Distinctive Audible Alerting - internal, external**
	Change the ringing pattern for an internal call to the ringing pattern of an external call, when a user or an attendant transfers the internal call.	**Update Transferred Ring Pattern?**
Station	Assign the Distinctive Alerting feature to the station.	**Distinctive Audible Alert**

Defining Distinctive Ringing

To define Distinctive Ringing:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Distinctive Audible Alerting** area (Figure 184: Feature-Related System Parameters screen on page 839).

Figure 184: Feature-Related System Parameters screen

```
display system-parameters features                              Page   5 of  14
                        FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5              Auto Start? n
   Conference Parties with Public Network Trunks: 6               Auto Hold? y
 Conference Parties without Public Network Trunks: 6           Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180          Bridging Tone? n
                  Short Interdigit Timer (seconds): 3         Conference Tone? n
               Unanswered DID Call Timer (seconds):             Intrusion Tone? n
               Line Intercept Tone Timer (seconds): 30      Special Dial Tone? n
                  Long Hold Recall Timer (seconds): 0     Mode Code Interface? y
                       Reset Shift Timer (seconds): 0
    Station Call Transfer Recall Timer (seconds): 0
                               DID Busy Treatment: tone
       Invalid Number Dialed Intercept Treatment: tone
              Allow AAR/ARS Access from DID/DIOD? n
                Allow ANI Restriction on AAR/ARS? n
     Use Trunk COR for Outgoing Trunk Disconnect? n
                  7405ND Numeric Terminal Display? n                  7434ND? y
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                         Attendant Originated Calls: external
   DTMF Tone Feedback Signal to VRU - Connection:          Disconnection:
```

3. In the **Distinctive Audible Alerting** area, perform the following actions:
   - Type **internal** next to the number of rings that you want the system to use for an internal call.
   - Type **external** next to the number of rings that you want the system to use for an external call.
4. Click **Next** until you see the **Update Transferred Ring Pattern?** field (Figure 185: Feature-Related System Parameters screen on page 840).

Figure 185: Feature-Related System Parameters screen

```
change system-parameters features                                    page 9
                        FEATURE-RELATED SYSTEM PARAMETERS

                 Pull Transfer: n            Update Transferred Ring Pattern? n
         Outpulse Without Tone? y              Wait Answer Supervision Timer? n
         Misoperation Alerting? n               Repetitive Call Waiting Tone? y
    Allow Conference via Flash? y     Repetitive Call Waiting Interval (sec): _
 Vector Disconnect Timer (min): __    Network Feedback During Tone Detection? y
   Hear Zip Tone Following VOA? y    System Updates Time On Station Displays? n
       Intercept Treatment On Failed Trunk Transfers? n
                     Station Tone Forward Disconnect: silence
                              Level Of Tone Detection: precise
          Charge Display Update Frequency (seconds): 30
         Date Format on 607/2420/4600/6400 Terminals: mm/dd/yy
On-hook Dialing on 607/2420/4600/6400/8400 Terminals? n

ITALIAN DCS PROTOCOL
  Italian Protocol Enabled? y
   Apply Intercept Locally? _      Enforce PNT-to-PNT Restrictions? _
```

5. In the **Update Transferred Ring Pattern?** field, perform one of the following actions:
   - If you want the system to change the ringing pattern for an internal call to the ringing pattern of an external call, when a user or an attendant transfers the call, type **y**.

     If most of your calls go through an attendant, you might want to set this field to **y** so that your users can identify an external call.
   - If you do not want the system to change the ringing pattern for an internal call to the ringing pattern of an external call, when a user or an attendant transfers the call, type **n.**
6. Press **Enter** to save your changes.

Reports for Distinctive Ringing

The following reports provide information about the Distinctive Ringing feature:

- None

Considerations for Distinctive Ringing

This section provides information about how the Distinctive Ringing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Distinctive Ringing under all conditions. The following considerations apply to Distinctive Ringing:

- If Distinctive Ringing is disabled, the system generates a one-burst repetitive tone for all incoming calls. The one-burst repetitive tone is useful for equipment that is interfaced by analog lines, especially if you use an off-premises telephone. A single distinctive ring cycle is used for each new incoming call to an off-hook telephone or headset. The system alerts a Callmaster® terminal with a single ring cycle whenever either the headset or the handset is plugged into the headset jack.

Interactions for Distinctive Ringing

This section provides information about how the Distinctive Ringing feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Distinctive Ringing in any feature configuration.

- Personalized Ringing

  The called party hears the user-selected ringing pattern for the distinctive ring cycles.

Enhanced 911

Use the Enhanced 911 (E911) feature to quickly access your local public safety agency. The public safety agency can dispatch the appropriate response team in cases of a:

- Fire
- Accident
- Crime
- Medical emergency

Detailed description of Enhanced 911

This section provides a detailed description of the Enhanced 911 (E911) feature.

A caller who needs emergency assistance dials one of the following Universal Emergency Numbers (UENs):

- 911 in the United States
- 000 in Australia
- 112 in the European community

The system routes the call through a local central office (CO), through an emergency tandem office, to the appropriate public safety answer point (PSAP). The PSAP answers the call.

A tandem office can route the call to a PSAP in surrounding areas. In the United States, a tandem office can route the call to nearby area codes. If the PSAP that receives the call is not the correct PSAP to handle the emergency, the PSAP transfers the call to the correct PSAP. Transfers can only occur between geographically adjacent or nearby PSAPs.

Each PSAP usually covers one city, or one rural county or community. At the PSAP, emergency operators determine the nature of the emergency, and contact the appropriate response agency. In the United States, a PSAP is usually responsible for an area that covers several independent police and fire departments.

With E911, the system sends the call and the Calling Party Number (CPN) over Centralized Automatic Message Accounting (CAMA) trunks. The system can also send the call and the CPN through the calling number information element (IE) over Integrated Services Digital Network (ISDN) trunks.

To learn how CAMA and ISDN trunks translate an extension to the PSAP, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

The public emergency system maintains a database that stores location and background information to help public safety agencies respond quickly with the appropriate assistance. The PSAP uses the CPN or the Caller Emergency Service Identification (CESID) number to look up the street address of the caller. The PSAP uses an Automatic Location Information (ALI) database. The ALI database is usually owned and managed by local exchange carriers (LEC). Instead of a LEC, customers can also contract with a third party to update the ALI database for them.

The E911 feature does not provide PSAP with the location of the person who placed the emergency call if the call came from a telephone that is on:

- A system that is not equipped with CAMA or ISDN trunks
- An adjunct computer system that is associated with CAMA or ISDN trunks

Instead, the E911 system identifies only the location of the trunk termination.

To solve this problem, you can report the emergency location extension as the CPN. After someone moves a telephone, you can manually correlate the CPN with the new telephone location. You can also purchase an adjunct that performs this correlation and update for you. You do not have to update the ALI database for the public switched telephone network (PSTN) after each telephone move.

The E911 feature transmits the extension of a direct inward dialing (DID) telephone that is associated with the calling party. The E911 feature transmits either:

- CESID over CAMA trunks
- CPN over ISDN trunks

The calling party might be at or near a telephone on a remote port network. The calling party might also be at a remote location that is served by an off-premises telephone.

Important:
If you use the digit **9** on the Dialplan Analysis Table screen as the ARS access code, also administer the dial string **11** as either an **emer** or **alrt** number. That way, when a user dials **911**, the digit **9** provides an outside line, and the digits **11** indicate an emergency or crisis alert call.

For Avaya IP Softphone, if the **Remote Softphone Emergency Calls** field on the Station screen is set to **as-on-local**, the system processes information based on certain criteria. For more information on what the system does when the **Remote Softphone Emergency Calls** field is set to **as-on-local**, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Enhanced 911 supports the following capabilities:

- Configurations with media gateways in different locations
- Location Specific Routing
- E911 for wired IP telephones
- Crisis Alert

Configurations with media gateways in different locations

Media gateways in different locations might have a different PSAP than the PSAP of the main server. You must ensure that the system correctly routes emergency calls that are made from telephones that are registered to each gateway to the correct PSAP.

To ensure that a media gateway in a separate location can route emergency calls properly, the system requires a CO trunk, a CAMA trunk, or a Primary Rate Interface (PRI) trunk from the gateway to the LEC. You must administer each media gateway that is in a different PSAP jurisdiction than the main server in a separate location. This separate administration ensures that the system can route emergency calls from that location. If a media gateway is in the same PSAP jurisdiction as the main server, you do not need to administer the media gateway in a separate location.

Location Specific Routing

In a configuration with one location, the system routes all outgoing calls to the PSTN according to the Automatic Route Selection (ARS) table for location 1. If media gateways are in different locations, you must administer Location Specific Routing for each location.

If a media gateway is in a separate location from the main server, you can administer the media gateway in locations for Linux and Avaya DEFINITY servers. For more information, see the *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

The command for Location Specific Routing is **change ars analysis location *X 0***, where ***X*** is the chosen location (2 to 64 or 2 to 44), and *0* is the first placeholder in the analysis table. Once the system displays the table, enter the routing information:

- Chosen dialed string (for example, 911)
- Minimum and maximum number of digits
- Route pattern
- Call type

You must also set up the required route pattern information. When you complete this administration, the system routes emergency calls from the location over a CO trunk, a CAMA trunk, or a PRI trunk to the LEC.

1. If a media gateway is connected to the LEC over a CO trunk, the extension of the CO trunk identifies the gateway service address. The service address is the physical location that the PSAP sees. Calls from any telephone that is registered to the gateway display the CO trunk extension to the PSAP. The PSAP then sends the emergency response to the service address.

   Use the CO trunk to send and receive emergency calls only. You must verify with the LEC that the extension of the CO trunk is in the PSAP database so that all emergency help is sent to the correct location.

2. If a media gateway is connected to the LEC over a PRI trunk, the system sends an extension to the PSAP based upon how Communication Manager is administered. You must verify with the LEC that all the extensions are in the PSAP database. For more information, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
3. If you use DID numbers from the main server to administer the extensions at the gateway, the numbers that are used at the media gateway must be moved to the CO where the 911 calls terminate. If the numbers are not moved, emergency help is sent to the main server location and not to the media gateway location.

If the main server and the media gateway are in different LEC jurisdictions:

- If you use a CO trunk from the gateway to the central office, follow the procedure as previously described in Step 1. Ensure that the correct extension is in the PSAP database for the CO trunk. All calls that are made from the gateway use this extension. Also ensure that the correct street address is in the PSAP database for the CO trunk. All calls that are made from the gateway use this street address.
- If you use a PRI trunk, you can purchase a block of DID extensions from the LEC for your gateway telephones. You can shorten the gateway extensions for private calls within your system. For example, you can shorten extension 765-4321 to 4321.

  When the system calls the PSTN, you must use the complete extension so that the number is recognized at the PSAP. For example, the system must send extension 765-4321 to the PSAP. The PSAP does not recognize extension 4321. Some PSAPs require a 10-digit number.

These two scenarios apply to each media gateway that is in a separate location. You must repeat each applicable procedure for each media gateway that is connected to a server with a unique PSAP. You must also repeat this procedure for each media gateway that is in its own location.

You can use the same Location Specific Routing tables and trunks for:

- Media gateways that are in the same location as the main system
- Multiple media gateways that are in the same location

Contact your Avaya representative if you have questions about these procedures or scenarios.

E911 for wired IP telephones

Important:
When someone dials an emergency number from an Avaya IP telephone, the emergency call reaches the local emergency service in the PSAP only when the telephone system has local trunks. If someone dials an emergency number from a remote location that does not have local trunks, an Avaya IP telephone cannot dial to and connect with local emergency services.

To avoid possible delays in getting emergency aid, *do not use an Avaya IP telephone to dial emergency numbers from a remote location*. Avaya is not responsible or liable for any damages that might result from misplaced emergency calls that someone makes from an Avaya IP telephone.

Your use of Communication Manager indicates that you have read this advisory. You further agree to use an alternative telephone to dial all emergency calls from remote locations. Contact your Avaya representative if you have questions about emergency calls from an IP telephone.

When someone dials an emergency number from a wired IP telephone, the system assigns an Emergency Location Information Number (ELIN) through an IP subnetwork. The system then sends the ELIN over either CAMA or ISDN PRI trunks to the emergency services network. To use this capability, you must have subnetworks that correspond to geographical areas.

The E911 for wired IP telephones capability works with two types of IP protocols:

- H.323
- SIP

If someone dials an emergency number from a wired IP telephone, the system at the PSAP uses the CPN to look up the physical location of the caller. However, the CPN might not always correspond to the physical location of the caller, because users with:

- H.323 IP telephones can move the telephones without notifying the system administrator
- SIP IP telephones can use the same extension simultaneously at several different telephones

Without the E911 for wired IP telephones capability, the emergency response personnel might go to the wrong physical location. With the E911 for wired IP telephones capability, the system properly identifies the location of the caller. The emergency response personnel can go to the correct physical location, even if an emergency call comes from a bridged call appearance.

When someone uses an IP telephone to dial an emergency number, the software compares the following two values for that IP telephone:

- The **Emergency Location Extension** field on the IP Address Mapping screen
- The **Emergency Location Ext** field on the Station screen

- If the two values are the same, the telephone most likely did not move. If the telephone did move, the telephone moved within the same subnetwork. In this scenario, Communication Manager sends the station's own extension as the Calling Party Number (CPN) .
- If the two values are different, and if the **Emergency Location Extension** on the IP Address Mapping screen is not blank, the telephone moved from one subnetwork to another. In this scenario, Communication Manager sends the CPN that is on the IP Address Mapping screen.
- If the **Emergency Location Extension** on the IP Address Mapping screen is blank, the administrator expects the caller to be located outside the LAN. This situation is true for a softphone. In this scenario, the CPN sent by Communication Manager is the **Emergency Location Extension** on the Station screen.

Whenever you add an extension as an **Emergency Location Extension** to the IP Address Mapping screen, check all Station screens for telephones in that IP address range.

- If the telephone is a DID number, ensure that the **Emergency Location Extension** is the same on both the Station screen and the IP Address Mapping screen.
- If the telephone is not a DID number, ensure that the **Emergency Location Extension** on the Station screen is different from the **Emergency Location Extension** on the IP Address Mapping screen.

Emergency Extension Forwarding

If an emergency call is dropped, the public safety personnel immediately attempt to call back. If the ELIN that was sent is not equivalent to the extension number of the caller, the return call rings at a different telephone. To overcome this situation, you can, for an administered period of time, automatically forward all calls to the telephone that placed the emergency call.

Use the **Emergency Extension Forwarding (min)** field on the Feature-Related System Parameters screen to set the Emergency Extension Forwarding timer for all incoming trunk calls if an emergency call is dropped.

This Emergency Extension Forwarding applies only if the **Emergency Location Extension** is an extension on the same system as the extension from which 911 was dialed. Customers who have several systems in a campus should assign several emergency location extensions.

Call Forwarding of dropped emergency calls

In this scenario, an IP telephone and a nearby media gateway that provides a connection to the PSTN are both registered to a primary server. The media gateway is backed up by an LSP, and the IP telephone has some LSPs in its alternate gatekeeper list. The IP telephone dials 911, and then the LAN crashes and partially recovers.

If both the IP telephone and the media gateway can reregister to the primary server, no problem exists. Also, if both the IP telephone and the media gateway are forced to register with the same LSP, no problem exists.

However, if the IP telephone or the media gateway re-registers to an LSP and the other re-registers to the primary server, or if the IP telephone and the media gateway re-register to different LSPs, a minor problem exists.

When the emergency response personnel call back, the server that the media gateway is registered with determines that the IP telephone is unregistered. The server cannot forward the return call to the IP telephone. Instead, the server attempts to forward the call to a telephone that is equivalent to the sent ELIN.

Even with automatic Emergency Return Call Forwarding, select the **Emergency Location Extension** that is administered in the ip-network-map screen as follows:

- On media gateways that have incoming PSTN trunks
- On the same media gateway as the telephones that the media gateway covers, assuming that the media gateway has incoming PSTN trunks

Crisis Alert

The Crisis Alert capability notifies the attendant, up to 10 other designated users, or a digital pager when someone dials an emergency number. Designated users might include:

- Security guards
- Receptionists
- Secretaries
- Front office personnel
- Human resources personnel

If a person dials an emergency number, the attendant or other designated users might want to know who made the call so that they can direct the emergency personnel to the right place.

When a user dials an emergency number, the system sends both an audible alert and a visual alert to the attendant console and the telephone of the designated user.

- The audible alert is a siren alarm.
- The visual alert is a flashing **crss-alert** button. The system also displays the name and the extension of the caller.

  If a user, John Doe at extension 3041, dialed an emergency number, the following information appears on the display of attendant consoles and digital telephones that have a **crss-alert** button:

  EM=JOHN DOE 3041 EM

Cancelling an alert

To cancel the alert, you can administer the system so that only one notified user must acknowledge the alert, or all notified users must acknowledge the alert.

To cancel an emergency alert, an attendant must press the **crss-alert** button on the attendant console three times:

- The first press turns off the siren alarm.
- The second press stops the **crss-alert** lamp from flashing.
- The third press clears the display.

Digital telephone users must press the **crss-alert** button on the telephone to cancel the emergency alert.

- If only one user must acknowledge the alarm, the siren alarm stops at all telephones.
- If all administered users must acknowledge the alarm, the alarm continues at each telephone until the user of that telephone presses the **crss-alert** button. Once all administered users acknowledge the alarm, the siren alarm stops.
- The name and the extension of the person who dialed the emergency number remains on the telephone display. To completely cancel an alert and clear the display, each administered user must press the **normal** button.

If someone makes an emergency call while another crisis alert is still active, the second emergency call is placed in a queue. If you administer the system so that:

- All users must acknowledge the alert, all users must acknowledge all emergency calls. The calls might not appear in the queue in the order that the calls were made.
- Only one user must acknowledge the alert, the first alert remains active at the telephone from where the alert was acknowledged. Any subsequent calls are queued to the next available telephone, in the order that the calls were made.

Once you administer the Crisis Alert capability, the system continues to record each emergency call.The system also sends a record to the system printer, if a system printer is available. If a system printer is not available, you can type **`list emergency`** to view the Emergency Access Calls report.

Administering Enhanced 911

In this example, you administer your system to notify the attendant, plus the security guard at three entrances. All three guards and the attendant must acknowledge the alarm to stop the alarm.

The following steps are part of the administration process for the Enhanced 911 feature:

- Setting up Crisis Alert to an attendant or a display telephone

- Setting up Crisis Alert to notify a digital pager
- Setting up emergency extension forwarding
- Setting up CAMA numbering

This section describes:

- Any prerequisites for administering the Enhanced 911 feature
- The screens that you use to administer the Enhanced 911 feature
- Complete administration procedures for the Enhanced 911 feature

Prerequisites for administering Enhanced 911

You must complete the following actions before you can administer the Enhanced 911 feature:

- Set up calling party restrictions on the Class of Restriction screen. For information on how to set up a Class of Restriction (COR), see the "Class of Restriction" feature.
- Set up ARS access codes on the Feature Access Code (FAC) screen. For information on how to set up a FAC, see the "Feature Access Code" feature.
- Set up all telephone route patterns on the Route Pattern screen. For information on how to set up a route pattern, see the "Uniform Dial Plan" feature.

Screens for administering Enhanced 911

Screen name	Purpose	Fields
ARS Digit Analysis Table	Set up an emergency number that users dial to access emergency services.	All
Attendant Console	Notify the attendant when someone dials the emergency number.	Any available button field in the **Feature Button Assignments** area.
CAMA Numbering - E911 Format	Format CAMA trunks for dialing.	All
Class of Restriction	Ensure that calling party restrictions are set up on your system.	**Calling Party Restriction**

Screen name	Purpose	Fields
Crisis Alert System Parameters	Force all users who have a **crss-alert** button on the telephone to acknowledge a crisis alert.	**Every User Responds**
	Administer the Crisis Alert capability to send an alert to a digital pager.	All fields in the **Alert Pager** area
Feature Access Code (FAC)	Ensure that FACs for ARS access codes are set up on your system.	• **ARS Access Code 1** • **ARS Access Code 2**
Feature-Related System Parameters	Set the timer to forward all incoming trunk calls in an emergency.	**Emergency Extension Forwarding (min)**
Optional Features	Ensure that your system is set up to handle Automatic Route Selection (ARS) routing and digit analysis.	**ARS**
Route Pattern	Ensure that you have set up route patterns on your system.	All
Station	Notify another user when someone dials the emergency number.	Any available button field in the **Button Assignments** area.
	Determine when to use the extension as E911 CPN.	• **Remote Softphone Emergency Calls** • **Emergency Location Ext** • Always Use

Setting up Crisis Alert to an attendant or a display telephone

To activate the Crisis Alert feature, you must complete the following procedures:

- Setting up the emergency number
- Setting up the attendant console to receive emergency notification
- Setting up digital telephones to receive emergency notification
- Setting which users must acknowledge the emergency alert

Setting up the emergency number

Prerequisites

You must complete the following actions before you can set up the emergency number:

- On the Optional Features screen, ensure that the **ARS** field is set to **y**. If this field is set to **n**, your system is not set up for the Enhanced 911 feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **display system-parameters customer-options**. Press **Enter**.

To set up the emergency number:

1. Type **change ars analysis *n***, where ***n*** is the number of the ARS table that you want to change. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen (Figure 186: ARS Digit Analysis Table screen on page 853).

Figure 186: ARS Digit Analysis Table screen

```
change ars analysis 5                                          Page 1 of 2

                      ARS DIGIT ANALYSIS TABLE
                            Location: all          Percent Full:  6

          Dialed          Total    Route     Call   Node  ANI
          String         Min Max   Pattern   Type   Num   Reqd
    911                   3   3     1         alrt   ___   n
    11 _______________    2_  2_    1____     alrt   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
    ____________________  __  __    _____     ____   ___   n
```

2. In the **Dialed String** field, type the number that users dial to reach emergency services.

   In this example, type **911**.

3. In the **Total Min** and **Total Max** fields, type the number of digits that you typed in the **Dialed String** field.

   In this example, type **3**. The user must dial all 3 digits in the **Dialed String** field for the system to treat the call as an emergency call.

4. In the **Route Pattern** field, type the number of the route pattern for local calls.

   In this example, type **1**.

5. In the **Call Type** field, type **emer** or **alrt**.
   - **emer** identifies the number in the **Dialed String** field as an emergency call.
   - **alrt** ensures that the number in the **Dialed String** field activates emergency alert notification.

6. Press **Enter** to save your changes.

Setting up the attendant console to receive emergency notification

When Crisis Alerting is active at the attendant console, the console is in position-busy mode. No other incoming calls interfere with the emergency call, but the console can still originate calls. The attendant must press the **position-busy** button to unbusy the console. The attendant must then press the **crss-alert** button to deactivate the audible and the visual alerts.

To set up the attendant console to receive emergency notification:

1. Type **`change attendant`** ***`n`***, where ***`n`*** is the number of the attendant console. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 187: Attendant Console screen on page 855).

Figure 187: Attendant Console screen

```
change attendant 1                                              Page 3 of 4

                              ATTENDANT CONSOLE

FEATURE BUTTON ASSIGNMENTS

 1: split                                13:
 2: dont-split                           14:
 3:                                      15: whisp-act
 4:                                      16:
 5:                                      17:
 6: hold                                 18:
 7:                                      19: forced-rel
 8:                                      20:
 9:                                      21: crss-alert
10:                                      22:
11:                                      23: night-serv
12:                                      24: pos-busy
```

3. In the **Feature Button Assignments** area, assign **crss-alert** to a button.

   In this example, we assign **crss-alert** to button 21.

4. Press **Enter** to save your changes.

Setting up digital telephones to receive emergency notification

Prerequisites

You must complete the following actions before you can set up digital telephones to receive emergency notification:

- On the Station screen for each telephone that you want to receive emergency notification:
  - Ensure that the extension is a digital display telephone.
  - In the **Type** field, ensure that the telephone is not a virtual extension.

  To view the Station screen, type **`change station n`**, where ***n*** is the extension. Press **Enter**.
- You must also have one of the following circuit packs: Call Classifier or Tone-Clock with Call Classification and Tone Detection. A Call Classifier pack is needed only if the outgoing trunk to the pager does not provide answer supervision.

To set up the digital telephone of each security guard to receive emergency notification:

1. Type **`change station n`**, where ***n*** is the extension of the security guard. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 188: Station screen on page 856).

Figure 188: Station screen

```
change station 32023                                        Page   3 of 3
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          4: data-ext    Ext: 22000
 2: call-appr                          5: crss-alert
 3: call-appr                          6:
```

3. In the **Button Assignments** area, assign **crss-alert** to an available button.

   In this example, we assign **crss-alert** to button 5. You cannot assign this button to a softkey.

4. Press **Enter** to save your changes.
5. Repeat this process for the telephone of each security guard.

Setting which users must acknowledge the emergency alert

To force all security guards and the attendant to acknowledge and cancel an alert:

1. Type **`change system-parameters crisis-alert`**. Press **Enter**.

   The system displays the Crisis Alert System Parameters screen (Figure 189: Crisis Alert System Parameters screen on page 857).

Figure 189: Crisis Alert System Parameters screen

```
change system-parameters crisis-alert                          Page 1 of 1

                          CRISIS ALERT SYSTEM PARAMETERS

ALERT STATION
    Every User Responds? y

ALERT PAGER
            Alert Pager? n
```

2. In the **Every User Responds** field, type **y**.

   If you set the **Every User Responds** field to **n**, any one of the designated users can cancel an alert.

3. Press **Enter** to save your changes.

Setting up Crisis Alert to notify a digital pager

You also have the option to have the Crisis Alert capability notify a digital pager. When someone dials an emergency number, the system sends the extension and the location of the caller to the administered pager.

This feature sends a message containing the extension number to the administered pager. You can also administer a main number so that the pager displays the location from where the emergency call originated.

To receive a crisis alert message, you must administer at least one attendant console or one digital telephone with a **crss-alert** button.

The crisis alert call to a digital pager uses two to four trunks. The system uses:

- One trunk for the actual call
- One to three trunks to notify one to three pagers, depending on how many pagers you administer.

Prerequisites

You must complete the following actions before a user can receive notification to a digital pager in an emergency:

- In the ARS Digit Analysis Table screen, you must have emergency numbers in the **Call Type** column set to **alrt**. For more information, see Setting up the emergency number on page 853.

- You must administer a **crss-alert** button on at least one of the following telephones:
  - Attendant console. For more information, see Setting up the attendant console to receive emergency notification on page 854.
  - Digital telephone. For more information, see Setting up digital telephones to receive emergency notification on page 855.
- You must also have at least one digital numeric pager, and one of the following circuit packs:
  - Call Classifier
  - Tone-Clock with Call Classification and Tone Detection

To set up Crisis Alert to notify a digital pager:

1. Type **change system-parameters crisis-alert**. Press **Enter**.

   The system displays the Crisis Alert System Parameters screen (Figure 190: Crisis Alert System Parameters screen on page 858).

Figure 190: Crisis Alert System Parameters screen

```
change system-parameters crisis-alert                          Page 1 of 1

                          CRISIS ALERT SYSTEM PARAMETERS

ALERT STATION
    Every User Responds? y

ALERT PAGER
            Alert Pager? y
  Originating Extension: 7768
      Crisis Alert Code: 911
                Retries: 5
   Retry Interval (sec): 15
            Main Number: 3035550800

                         Pager Number          Pin Number
                     1: 3035559001         1: pp77614567890
                     2:                    2:
                     3:                    3:

                DTMF Duration - Tone (msec): 100  Pause (msec): 100
```

2. In the **Alert Pager** field, type **y**.

   The system displays additional Crisis Alert administration fields.

3. In the **Originating Extension** field, type a valid unused extension to send the Crisis Alert message.

   In this example, that extension is **7768**.

4. In the **Crisis Alert Code** field, type the number that a user dials to call for emergency assistance.

   In this example, that number is **911**.

5. In the **Retries** field, type the number of additional times that you want the system to try to send the alert message in case of an unsuccessful first attempt.

   In this example, that number is **5**.

6. In the **Retry Interval (sec)** field, type the number of seconds between retries.

   In this example, that number is **15**.

7. In the **Main Number** field, type the number that you want the system to display at the end of the pager message.

   In this example, that number is **3035550800**.

8. In the **Pager Number** field, type the telephone number for the pager.

   In this example, that number is **3035559001**.

9. In the **Pin Number** field, type the personal identification number (PIN), if required, for the pager. Insert pause digits (**pp**) as needed to pause for announcements from the pager service to complete before sending the PIN.

   In this example, that number is **pp77614567890**.

10. In the **DTMF Duration - Tone (msec)** field, type the the number of milliseconds that the dual-tone multifrequency (DTMF) tone plays for each digit.

    In this example, that number is **100**.

11. In the **Pause (msec)** field, type the number of milliseconds between DTMF tones for each digit.

    In this example, that number is **100**.

12. Press **Enter** to save your changes.

Setting up emergency extension forwarding

If an emergency call gets disconnected, the public safety person immediately attempts to call the caller back. If the ELIN that the PSAP receives is not equivalent to the extension of the caller, the return call might ring at a different telephone. To solve this problem, you can automatically forward all incoming trunk calls, for an administered period of time, to the telephone that placed the emergency call.

Note:

You must administer time limits on the system first. If time limits are not administered, the system will not forward all incoming trunk calls because the system cannot determine what incoming trunk call is from the PSAP.

To set up emergency extension forwarding:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Emergency Extension Forwarding (min)** field (Figure 191: Feature-Related System Parameters screen on page 860).

Figure 191: Feature-Related System Parameters screen

```
change system-parameters features                                Page 5 of 14

                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PARAMETER PRINTERS
                System Printer Endpoint:                  Lines Per Page: 60


 Emergency Extension Forwarding (min): 10

SYSTEM-WIDE PARAMETERS
                          Switch Name: Norbert


MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? y   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds)? 0
SEND ALL CALLS OPTIONS
     Send All Calls applies to: station    Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? n    UCID Network Node ID:
```

3. In the **Emergency Extension Forwarding (min)** field, type the number of minutes for which you want the system to forward all incoming trunk calls to the emergency extension. In this example, the number is **10**.

   The timer starts once an emergency call gets disconnected. This timer applies only if the Emergency Location Extension is an extension on the same system as the extension from which 911 was dialed. Customers with several systems in a location must assign multiple Emergency Location Extensions.

4. Press **Enter** to save your changes.

Setting up CAMA numbering

Use the CAMA Numbering - E911 Format screen to administer Centralized Automatic Message Accounting (CAMA) trunks. Also use this screen to provide Caller Emergency Service Identification (CESID) information to your local emergency system through the local tandem office.

This screen provides the CESID format by extension or number blocks. This flexibility allows for multiple CESID formats to be sent over multiple CAMA trunk groups, and mixed telephone numbering plans. This flexibility also allows some limited conversion from non-DID to DID numbers that the Private Switch/Automatic Location Interface (PS/ALI) database usually requires.

The **System CESID Default** field defines the CESID for all extensions that are not defined in the **Ext Code** fields. The first page of this screen contains the default CESID, plus extension fields for CESID entries. Each remaining page contains additional extension fields for CESID entries.

Note:
The following procedure assumes that a CAMA trunk group is already set up. For information on how to set up trunk groups, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

To set up CAMA numbering:

1. Type **`change cama-numbering`**. Press **Enter**.

   The system displays the CAMA Numbering - E911 Format screen (Figure 192: CAMA Numbering - E911 Format screen on page 862).

Figure 192: CAMA Numbering - E911 Format screen

```
change cama-numbering                                          Page 1 of 15
                          CAMA NUMBERING - E911 FORMAT

System CESID Default: _____________

Ext   Ext                     Total         Ext   Ext                     Total
Len   Code       CESID        Length        Len   Code       CESID        Length
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
 _   _______ ________________   __          _   _______ ________________   __
```

2. In the **System CESID Default** field, type the CESID that the system sends over the CAMA trunk if you do not define the **Ext Code** fields.

   Type a number that consists of 1 to 16 digits. The default value is blank.

3. In the **Ext Len** field, type the number of digits in the extension.

   Type a number from 1 to 5. The default value is blank.

4. In the **Ext Code** field, type the leading digits or all of the digits in the extension for the specified CESID.

   If the value in the **Ext Len** field is greater than the number of digits in the **Ext Code** field, the system interprets the **Ext Code** as a block of digits. For example, if the value in the **Ext Len** field is 4 and the value in the **Ext Code** field is 11, the CESID serves extensions 1100 through 1199. The **Ext Code** [11] is for a DID block. **Ext Code** [126] might point a non-DID block to a nearby DID extension 5241666.

   Enter a number that consists of 1 to 5 digits. The default value is blank.

5. In the **CESID** field, type the number that identifies the calling terminal within an emergency service system. This field can represent a prefix to an extension, or the entire CESID.

   Enter a number that consists of 1 to 16 digits. The default value is blank.

6. In the **Total Length** field, type the total number of digits to send.

   Enter a number that consists of 1 to 16 digits. The default value is blank.

7. Press **Enter** to save your changes.

Reports for Enhanced 911

The following reports provide information about the Enhanced 911 feature:

- The Emergency Access Calls report shows the following information for each emergency call:
  - Extension
  - Event
  - Type of call
  - Time

For detailed information on this report and the associated commands, see *Avaya Aura™ Communication Manager Reports*, 555-233-505.

Considerations for Enhanced 911

This section provides information about how the Enhanced 911 feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Enhanced 911 under all conditions.

The following considerations apply to Enhanced 911:

- The Enhanced E911 feature only applies to emergency calls that go over CAMA and ISDN trunks.
- You must provide several call appearances on the last telephone in both the coverage path and the telephone hunting path of the Emergency Location Extension.
- Do not include voice mail, automated attendant, or announcement extensions for Emergency Location Extensions.

The following two consideration scenarios apply to a Local Survivable Processor (LSP), and to backup S8700 servers. These considerations apply if the spare processor is an asynchronous transfer mode wide area network (ATM WAN), or is on a survivable remote expansion port network (EPN).

- Sending the correct ELIN to the PSAP

  Once each day, the LSP copies administration translations from its primary server. The system never copies translations from the LSP to the primary server. IP telephones can stay under the control of an LSP for 6 days, 10 days, or indefinitely. The length of time depends on what version of software you are running.

  If someone notifies you that an IP extension moved, update the ALI database with the physical location of the IP extension. Also change the **Emergency Location Extension** field on the IP Address Mapping screen to match the new subnetwork of the IP extension. You can also purchase an adjunct that performs this correlation and update for you.

  If the telephone registers with the LSP before the system copies the translations from the main server, the **Emergency Location Extension** field is still set to the old value. If the user dials 911, emergency response personnel might go to a different location for the caller instead of to the exact location.

  Never update translations directly on the LSP.

The following considerations apply to the Crisis Alert capability:

- The Automatic Number Identification (ANI) that the system sends to the CO might not be the same extension as the telephone that the person used to dial the emergency. If the call is disconnected and the public service person call back, the public service person calls the ANI. The public service person might not reach the caller.

  If a telephone has a **crss-alert** button assigned, the return call is answered by someone who was notified of the extension that made the emergency call. That person can then forward the return call from the public service person to the extension from which the emergency call was placed.
- Only one **crss-alert** button can appear on an attendant console or a digital telephone.
- Attendant consoles or digital telephones without a **crss-alert** button do not receive emergency notification.

Interactions for Enhanced 911

This section provides information about how the Enhanced E911 feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of E911 in any feature configuration.

- Bridged Call Appearances

  Emergency 911 calls from a bridged extension report the extension of the physical telephone, not the bridged call appearance.
- Class of Restriction (COR), Tenant Partitioning, and Facilities Restriction Level (FRL)

  COR, Tenant Partitioning, and FRL restrictions apply to CAMA trunks and 911 calls.

- Expert Agent Selection (EAS)

  When an EAS agent dials 911, the number is the number of the physical telephone, and not of the logical agent.

- Network Address Translation (NAT) devices

  If a telephone operates behind a NAT device, the ELIN is based upon the translated IP address of the telephone, and not the native IP address. If you use a NAT device, the NAT device must preserve IP subnetworks. To require a change in IP address, the E911 for wired IP telephones capability expects a move from one geographic area to another.

  For example, you have two subnetworks, 1.1.1.* and 2.2.2.*, that are mapped to two different ELINs in the ip-network-map screen. Both of these subnetworks operate behind a NAT device. If the NAT device maps both subnetworks of 1.1.1.* and 2.2.2.* into addresses in the range 3.3.3.*, Communication Manager can not detect if someone moves a telephone from 1.1.1.* to 2.2.2.*.

- Non-ARS calls

  The E911 feature uses Automatic Route Selection (ARS) digit analysis to classify an outgoing call as an emergency or crisis alert call. If a user does not use ARS to dial an emergency call, the E911 feature only applies if the trunk types are CO or FX. Examples of calls that do not use ARS are:

  - Calls that use a trunk access code
  - Personal CO line button calls
  - Facility test calls
  - AAR access code calls, if AAR digit analysis does not overflow to ARS

The following interactions apply to the Crisis Alert capability:

- Centralized Attendant Service (CAS)

  If CAS is enabled, the emergency alert still goes to the local attendant.

- Multiple Locations

  A crisis alert call to a digital pager is treated by the system as if the call is from Location 1. This means that the pager number digits are analyzed using the Location 1 dial plan and the Location 1 ARS Analysis Table. Note that the system does not use the location of the station that dialed the emergency call.

- Outgoing Trunk Queuing

  If a user attempts to make an emergency call when all trunks are busy, the call does not generate an alert. If the Outgoing Trunk Queuing feature is enabled for a trunk group, the call is placed in a queue, but does not generate an alert.

- Tenant Partitioning

  If Tenant Partitioning is active, stations and attendants with crisis alert buttons will receive emergency notification from only those callers who are within the tenant partition. If no stations or attendants with crisis alert buttons are assigned to a partition from which an emergency call originates, the system still sends a record of the call to the system printer, and to the Emergency Access Calls report.

- Terminal Self-Administration

  Users who can administer their own telephones cannot disable a **crss-alert** button.

Emergency Calls from Unnamed IP Endpoints

Use the Emergency Calls from Unnamed IP Endpoints feature to register an IP telephone without an extension number. The Emergency Calls from Unnamed IP Endpoints feature places the IP telephone into Terminal Translation Initialization (TTI) service. Users can dial a Feature Access Code (FAC) to either associate an extension number with a telephone, or to dissociate an extension number from a telephone.

A person can use an IP telephone that is in TTI service to make emergency calls if Communication Manager is appropriately administered.

Note:
Check with your Avaya sales representative or your Avaya Authorized Business Partner for availability of this feature.

Detailed description of Emergency Calls from Unnamed IP Endpoints

This section provides a detailed description of the Emergency Calls from Unnamed IP Endpoints feature.

Without the Emergency Calls from Unnamed IP Endpoints feature, if a user of an IP telephone registers the extension to another telephone or softphone, the IP telephone changes to an unregistered state. The IP telephone cannot reregister until the user releases the extension number from the other telephone or softphone. A user cannot use an IP telephone that is in an unregistered state to make emergency calls.

However, if a user has a DCP telephone and registers the extension to another telephone or softphone, the DCP telephone goes into a dissociated state. In this state, a user can still use the DCP telephone to make emergency calls if Communication Manager is appropriately administered.

The Emergency Calls from Unnamed IP Endpoints feature makes IP telephones work like DCP telephones when users make emergency calls from telephones that do not have extension numbers.

When an IP telephone is plugged in, power cycled, or after a user logs off, the system displays a prompt on the telephone display. The prompt asks the user for an extension number and a password. If a user does not dial at least one digit within 60 seconds from when the prompt first appears, the system registers the telephone into TTI service.

If a user wants to make an unnamed IP telephone reregister with an extension, the user must either:

- Press the Login prompt on the telephone softkey, and then enter an extension and a password
- Use the Feature Access Code (FAC) for the Personal Station Access (PSA) Associate feature

  A user can dial the FAC for the PSA Associate feature from an IP telephone that is in TTI service only if one of the following conditions is true:

  — the **Receive Unencrypted from IP Endpoints** field on the Security-Related System Parameters screen is set to **y**

  — The telephone encrypts signaling

  If a user dials the FAC for the PSA Disassociate feature, the system immediately places the IP telephone into TTI service.

The Emergency Calls from Unnamed IP Endpoints feature does not work with the following IP telephones:

- Non-AVAYA H.323 IP telephones
- IP Softphone release 5 or earlier
- IP telephones with 2.1 firmware or earlier
- IP telephones with 2.5 firmware

The Emergency Calls from Unnamed IP Endpoints feature supports the following capabilities:

- If a person makes a call from an IP telephone that is in TTI service, the called party sees the IP port of the calling party and the words “TTI port” on their display telephone. For example, a called party might see **S00001 TTI port** on their display telephone. This display allows the called party to identify the source of the call.
- If the Malicious Call Trace (MCT) feature traces an IP telephone that is in TTI service, the IP port appears on the display of the MCT controller. The administrator can use the **`display port n`** command to convert the port into an IP address. The administrator can then learn the original extension of the IP telephone, and where the telephone is located.

These two capabilities are especially helpful to trace calls.

The system can register an IP telephone to TTI service only if that IP telephone has an IP address that is administered on the IP Address Mapping screen. To view the IP Address Mapping screen, type the **`display ip-address-map`** command.

Changed screens

The following screens were changed for the Emergency Calls from Unnamed IP Endpoints feature:

- Feature-Related System Parameters screen
- Port Information screen
- System Capacity screen

Feature-Related System Parameters screen

On the Feature-Related System Parameters screen, the **COR for PSA Dissociated Sets** field is renamed **Default COR for Dissociated Sets**. The **CPN, ANI for PSA Dissociated Sets** field is renamed **CPN, ANI for Dissociated Sets**. The function of these two fields did not change.

To view the Feature-Related System Parameters screen:

1. Type **`display system-parameters features`** and press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Press **Next** until you see the **Default COR for Dissociated Sets** and **CPN, ANI for Dissociated Sets** fields (Figure 193: Feature-Related System Parameters screen on page 869).

Figure 193: Feature-Related System Parameters screen

```
display system-parameters features                              Page 3 of x


TTI/PSA PARAMETERS

  WARNING!  SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE

        Terminal Translation Initialization (TTI) Enabled? y
                TTI State: voice        TTI Security Code: 1234


                        Default COR for Dissociated Sets:

          Unnamed Registrations and PSA for IP Telephones? n
               Customer Telephone Activation(CTA) Enabled? n
 Don't Answer Criteria For Logged Off IP/PSA/TTI Stations? n
                     Hot Desking Enhancement Station Lock? n

EMU PARAMETERS
           EMU Inactivity Interval for Deactivation(hours):

CALL PROCESSING OVERLOAD MITIGATION
           Restrict Calls: stations-first
```

Port Information screen

The system displays the IP address of an IP telephone that is in TTI service in the **Identification** field on the Port Information screen.

To view the Port Information screen:

1. Type **display port *n***, where ***n*** is the port address. Press **Enter**.

   The system displays the Port Information screen (Figure 194: Port Information screen on page 870).

Figure 194: Port Information screen

```
display port s00001
                                PORT INFORMATION

                                   Port: S00001
                           Equipment Type: TTI port
                           Identification: 172.22.22.122
```

System Capacity screen

A new field, **IP Stations in TTI State**, is added to the System Capacity screen.

To view the System Capacity screen:

1. Type **display capacity** and press **Enter**.

   The system displays the System Capacity screen.

2. Press **Next** until you see the **IP Stations in TTI State** field (Figure 195: System Capacity screen on page 870).

Figure 195: System Capacity screen

```
display capacity                                              Page 10 of 12
                                SYSTEM CAPACITY

       CONCURRENT REGISTRATION COUNTS
                                            Currently              System
                                            Registered  Available  Limit
                                            ----------------------------
                                IP Stations:    1009       4091      5100
                  IP Stations in TTI State:       0          -         -
                     IP Attendant Consoles:       0          1         1
                    Remote Office Stations:       3        997      1000
```

Changed commands

The following commands were changed for the Emergency Calls from Unnamed IP Endpoints feature:

- reset ip-stations command

reset ip-stations command

reset ip-stations

The **reset ip-stations** command has a new option, **tti**. The complete command is now:

reset ip-stations [ip-phones | all | tti] [network-region(1-250) | all-regions].

The system administrator can use the **reset ip-stations tti** command to unregister IP telephones that are in TTI service without unregistering other IP telephones.

Administering Emergency Calls from Unnamed IP Endpoints

The following steps are part of the administration process for the Emergency Calls from Unnamed IP Endpoints feature:

- None

This section describes:

- Any prerequisites for administering the Emergency Calls from Unnamed IP Endpoints feature
- The screens that you use to administer the Emergency Calls from Unnamed IP Endpoints feature
- Complete administration procedures for the Emergency Calls from Unnamed IP Endpoints feature

Prerequisites for administering Emergency Calls from Unnamed IP Endpoints

- On the Optional Features screen, ensure that the **G3 Version** field is set to **V13** or later. **V13** is the version for Communication Manager Release 3.0. If this field is not set to **V13** or later, your system is not enabled for the Feature Description and Implementation feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- The Emergency Calls from Unnamed IP Endpoints feature requires that the TTI for voice terminals option be turned on. Your license file sets this field. If the TTI for voice terminals option is turned off for your system, IP telephones that are in the TTI state are unregistered.

  To verify if the TTI for voice terminals option is turned on:

  1. Type **`display system-parameters features`**. Press **Enter**.

     The system displays the Feature-Related System Parameters screen.

  2. Press **Next** until you see the **TTI/PSA Parameters** section (Figure 196: Feature-Related System Parameters screen on page 873).

Figure 196: Feature-Related System Parameters **screen**

```
display system-parameters features                                Page 3 of x


TTI/PSA PARAMETERS

  WARNING!  SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE

       Terminal Translation Initialization (TTI) Enabled? y
               TTI State: voice        TTI Security Code: 1234


                        Default COR for Dissociated Sets:

         Unnamed Registrations and PSA for IP Telephones? n
              Customer Telephone Activation(CTA) Enabled? n
 Don't Answer Criteria For Logged Off IP/PSA/TTI Stations? n
                     Hot Desking Enhancement Station Lock? n

EMU PARAMETERS
           EMU Inactivity Interval for Deactivation(hours):

CALL PROCESSING OVERLOAD MITIGATION
           Restrict Calls: stations-first
```

1. Ensure that the **Terminal Translation Initialization (TTI) Enabled?** field is set to **y**.
2. Ensure that the **TTI State** field is set to **voice**.
3. Press **Enter**.

Important:
Administrators or technicians might often turn off TTI during software upgrades. Remember that you must turn TTI back on when the upgrade is complete.

SECURITY ALERT:
You might choose to leave TTI turned off for security reasons. If you want to use the Feature Description and Implementation feature but not use TTI, set the **TTI FAC** field on the Feature Access Code (FAC) screen to blank.

Screens for administering Emergency Calls from Unnamed IP Endpoints

Screen name	Purpose	Fields
Feature-Related System Parameters	Ensure that the Emergency Calls from Unnamed IP Endpoints feature is enabled on your system.	• **Terminal Translation Initialization (TTI) Enabled?** • **TTI State**
Port Information	Identify the IP address of an IP telephone that is in TTI service.	**Identification**
System Capacity	Define the system limit of IP telephones in TTI status.	**IP Stations in TTI State**

Reports for Emergency Calls from Unnamed IP Endpoints

The following reports provide information about the Emergency Calls from Unnamed IP Endpoints capability:

- *Call Detail Recording (CDR)*

  If an IP telephone that is in TTI service makes an outgoing call, CDR records contain the port as the calling party. An example of a port is S00001.

- *History Log*

  If the **Record IP Registrations in History Log?** field on the System-Parameters Features screen is set to **y**, the system records registrations to TTI service and unregistrations from TTI service in the History Log. The History Log displays the:

  – IP address for registrations and unregistrations

– Telephone extension for Personal Station Access (PSA) associations and PSA disassociations

The same information is available from the Tracelog file. The **Qualifier** column shows the IP address. The system also records state changes to and from TTI service from **LoginInfoUpdate** messages, end user PSA, or similar actions.

- The List Usage Report lists IP telephones that are in TTI service (Figure 197: List Usage Report screen on page 875). To see the List Usage Report report, type the **`list usage ip-address n`**, where ***n*** is the IP address of the telephone.

Figure 197: List Usage Report screen

```
list usage ip-address 135.9.159.130

                              LIST USAGE REPORT
Used By
TTI Station             Port Number  S00074               Station IP Addr
```

- *Tracelog*

  Registrations to, and unregistrations from, TTI service get an entry in the tracelog file, if the Linux Registries has turned on each system for the appropriate platforms. Extensions that move from one telephone to another also get an entry in the tracelog file.

- The TTI Service IP Stations report lists IP telephones that are in TTI service (Figure 198: TTI Service IP Stations screen on page 875). To see the TTI Service IP Stations report, type the **`list tti-ip-stations`** command.

Figure 198: TTI Service IP Stations screen

```
list tti-ip-stations                                                    Page 1
                            TTI SERVICE IP STATIONS

Station          Product    Prod     Net     Gatekeeper
IP Address       ID         Rel      Rgn     IP Address     Port
135.9.159.130    IP_Phone   2.200    1       135.9.159.128  S00074
```

Field descriptions

All fields are display only. The system sorts the information on the screen by the **Station IP Address** field.

For more information on these reports and the associated commands, see *Avaya Aura™ Communication Manager Reports, 555-233-505*.

Interactions for Emergency Calls from Unnamed IP Endpoints

This section provides information about how the Emergency Calls from Unnamed IP Endpoints feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Emergency Calls from Unnamed IP Endpoints in any feature configuration.

- E911 layer 2 adjunct

  If you use the Cielo E-911 Manager from RedSky Technologies, Inc., contact RedSky for information about how that product interacts with this feature. The Web site for RedSky Technologies, Inc. is http://www.redskytech.com.

- E911 restricted telephones

  You might have telephones from which you do not want users to make or receive external calls. You can put such telephones into TTI service. However, a better method is to give the telephone an extension number, and then use a Class of Restriction (COR) to restrict the permissions.

  For example, if someone dialed 911 from such a telephone and the call accidentally dropped, the public safety officer will call back to the calling party number that the public safety office received during the 911 call. If the telephone that dialed 911 has an extension number, the telephone receives the return call. If the telephone that dialed 911 was in TTI service, the return call rings someone else who might not know about the emergency.

- Selective Conference Party

  With the Selective Conference Party feature, a member of a conference call can view the number and the name of the other parties on the call. The member can also drop or mute the other parties. A telephone that is in TTI service cannot use the Selective Conference Party feature because the feature requires the use of a button. However, a telephone that is in TTI service can be displayed, dropped, or muted.

Enterprise Mobility User

Use the Enterprise Mobility User (EMU) feature to associate the features of a user's primary telephone to a telephone of the same type anywhere within your enterprise.

Note:
Any telephone that is not the primary telephone is referred to as the visited telephone, and any server that is not the home server of the primary telephone is referred to as the visited server.

Detailed description of Enterprise Mobility User

This section provides a detailed description of the Enterprise Mobility User (EMU) feature.

- EMU Enhancements for Communication Manager 4.0 on page 877
- System requirements for EMU
- EMU use and activation
- EMU supported telephone buttons
- EMU call processing
- EMU and the station lock feature
- Traffic considerations
- Message waiting indication

EMU Enhancements for Communication Manager 4.0

Starting with Communication Manager Release 4.0, the EMU feature has the following enhancements:

- Extension to Cellular Availability with EMU on page 878
- A home station of a visitor can be visited on page 878
- Detailed description of Enterprise Mobility User on page 877

Extension to Cellular Availability with EMU

Starting with Communication Manager Release 4.0, mobile users can use the Extension to Cellular feature to access a station that is being visited by a user of the EMU feature.

Important:
This enhancement does not include the XMOBILE EC500.

A home station of a visitor can be visited

The home station of a user that is registered as an EMU visitor elsewhere in the enterprise network, can be visited by another EMU user. In the case where either user places an emergency call, both EMU registrations will be unregistered.

The EMU timer

The EMU timer can be administered on the Features-Related System Parameters screen. The EMU timer applies to the to the visited server only. You can administer the timer for each server in the system. The amount of time a visitor can remain registered during a period of inactivity is entered in the **EMU Inactivity Interval for Deactivation (hours)** field. Valid entries are one to 24 hours. If the entry is left blank, the EMU timer will not be used and the visited station will remain registered until it becomes unregistered by other means.

Figure 199: Feature-Related System Parameters screen for EMU

```
change system-parameters features Page   3 of  17
                     FEATURE-RELATED SYSTEM PARAMETERS
TTI/PSA PARAMETERS

  WARNING!  SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE

        Terminal Translation Initialization (TTI) Enabled? y
                 TTI State: voice        TTI Security Code: 12345


                         Default COR for Dissociated Sets: 1
                            CPN, ANI for Dissociated Sets: 33333
          Unnamed Registrations and PSA for IP Telephones? n
               Customer Telephone Activation(CTA) Enabled? n
 Don't Answer Criteria For Logged Off IP/PSA/TTI Stations? n

EMU PARAMETERS
           EMU Inactivity Interval for Deactivation(hours):

CALL PROCESSING OVERLOAD MITIGATION
           Restrict Calls: stations-first
```

System requirements for EMU

The following is a list of requirements for the EMU feature:

- QSIG must be the private networking protocol in the network of Communication Manager systems. This requirement also includes QSIG MWI.
- EMU phase 1: Communication Manager Release 3.1 and later software must be running on the home server and all visited servers.
- EMU phase 2: Communication Manager Release 4.0 and later software must be running on the home server and all visited servers. EMU phase 2 is not backward compatible with Communication Manager 3.1.
- All servers must be on a Linux platform. EMU is not supported on DEFINITY servers.
- The visited telephone must be the same model type as the primary telephone to enable a optimal transfer of the image of the primary telephone. If the visited telephone is not the same model type, only the call appearance (call-appr) buttons and the message waiting light are transferred.
- All endpoints must be self-designating terminals.
- Uniform Dial Plan (UDP).

Note:

All systems in a QSIG network must be upgraded to Communication Manager 4.0 or later in order for the Enterprise Mobility User feature to function properly. If only some systems are upgraded, and their extensions expanded, the EMU feature might not work with the systems that have not been upgraded. See your Avaya technical representative for more information.

EMU use and activation

To activate the EMU feature, a user enters the EMU activation feature-access-code (FAC), the extension number of their primary telephone, and a security code on the dial pad of a visited telephone. The visited server sends the extension number, the security code, and the set type of the visited telephone to the home server. When the home server receives the information it:

- Checks the class of service (COS) for the primary telephone to see if it has PSA permission.
- Compares the security code with the security code on the station form for the primary telephone.

- Compares the station type of the visited telephone to the station type of the primary telephone. If both the visited telephone and the primary telephone are of the same type, the home server sends the applicable button appearances to the visited server. If a previous registration exists on the primary telephone, the new registration is accepted and the old registration is deactivated.

If the registration is successful the visited telephone assumes the primary telephone's extension number and some specific administered button types. The display on the primary telephone shows Visited Registration Active: <Extension>. The extension number that displays is the extension number of the visited telephone.

Note:
The speed dialing list that is stored on the primary telephone and the station logs are not downloaded to the visited telephone.

EMU supported telephone buttons

The following list shows the buttons that are supported by EMU:

- Abbreviated dialing (abrv-dial)
- Automatic message waiting (aut-msg-wt)
- Automatic callback (auto-cback)
- Automatic intercom (auto-icom)
- Automatic dialing (autodial)
- Bridged appearance (bridg-appr)
- Bridged Appearance of an analog telephone (abrdg-appr (Extension))
- Busy indicator (busy-ind)
- Call appearance (call-appr)
- Call forwarding (call-fwd)
- Call forwarding busy don't answer (cfwd-bsyda)
- Dial intercom (dial-icom)
- ec500
- Exclusion
- Personal central office line (per-COline)
- Send all calls (send-calls)

Up to 24 of the supported button types can be downloaded to the visited server for mapping to a visited telephone. The 24 button limitation applies to all telephones supported by EMU.

The home server sends the button state of the visited telephone. The supported states are idle, alerting with ringing or alerting without ringing, and in-use. The busy state is shown as a steady light and will not blink on the visited telephone.

EMU call processing

Calls made from a visited telephone can be processed by either the home server or the visited server. Which server processes the call depends on how the user originates the call. The home server processes any calls that are a result of a user depressing one of the buttons that were downloaded to the visited telephone. The visited server processes any calls that are placed on the visited telephone using the dial pad.

All emergency numbers must originate from the dial pad of the visited telephone to ensure that the locally applicable emergency number entered on the key pad is sent to the emergency call receipt agency. A visited telephone will be deactivated when an emergency number is dialed. The visited server determines if the call is an emergency through the Automatic Routing Selection (ARS) analysis table category of the called number. Deactivating the visited telephone gives the emergency call receipt agency the ability to make a call back to the telephone if necessary. After a visitor makes emergency call of the type **emer** or **alrt**, the EMU feature does not allow use of EMU FAC for registration for an amount of time that can be administered.

EMU and the station lock feature

If the primary telephone is locked, the visited telephone cannot place outgoing calls using the Abbreviated Dial buttons or the Bridged Appearance buttons. Calls from the Abbreviated Dial buttons or the Bridged Appearance buttons are processed by the home server. The home server blocks any outgoing calls from a locked telephone.

A visited telephone can make outgoing calls if the dial pad is used. Calls from the dial pad of a visited telephone are processed from the visited server. The visited server does not know about the lock on the primary telephone.

Traffic considerations

The EMU feature is used by people who travel to various locations within a company’s enterprise. The number of visited telephones activated to use EMU and the subsequent traffic the EMU users generate, must be taken into consideration when designing for EMU. EMU can affect both the signaling links used for transporting the QSIG messages and the bearer network used for voice traffic. Additional trunking between the Avaya servers in the network may be required to accommodate the additional traffic. The number of additional trunks can be determined by looking at the busy hour call rate for the roaming users and the blocking rate that is allowed or desired.

Message waiting indication

When a visited telephone registers with a home server, the home server sends the current message waiting lamp status. The home server continues to send message waiting lamp updates to the visited server until the visited telephone is no longer registered with the home server.

Administering Enterprise Mobility User

The following steps are part of the administration process for the Enterprise Mobility User (EMU) feature:

- Configuring your system for Enterprise Mobility User
- Setting EMU options for stations
- Defining options for calling party identification

This section describes:

- Any prerequisites for administering the Enterprise Mobility User feature
- The screens that you use to administer the Enterprise Mobility User feature
- Complete administration procedures for the Enterprise Mobility User feature

Prerequisites for administering Enterprise Mobility User

You must complete the following actions before you can administer the Enterprise Mobility User feature:

To use the EMU feature, you must have Communication Manager Enterprise Edition Release 3.1 running on Linux Media Servers.

The EMU feature does not require any other right-to-use agreements, that is, it does not have to be turned on in the license file for your system.

For other system requirements for the EMU feature, see System requirements for EMU on page 879.

Screens for administering Enterprise Mobility User

Screen name	Purpose	Fields
Class of Service	Configuring your system for the feature.	• **Personal Station Access**
Feature Access Code		• **Enterprise Mobility User Activation** • **Deactivation**
System-parameters features		• **EMU Inactivity Interval for Deactivation (hours)** • Emergency Extension Forwarding (min)
Station	Setting EMU options for stations.	• **Security Code** • **EMU Login Allowed**
Trunk Group	Defining options for calling party identification.	• **Send EMU Visitor CPN**

Configuring your system for Enterprise Mobility User

To configure your system for the Enterprise Mobility User feature:

1. Type **`display cos`** to view your Class of Service settings.

   The system displays the Class of Service screen. (Class of Service screen on page 884).

Figure 200: Class of Service screen

Page 1 of 2

CLASS OF SERVICE

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Auto Callback	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y
Call Fwd-All Calls	n	y	y	y	y	n	n	y	y	n	n	y	y	y	y	y
Data Privacy	n	y	y	n	n	y	y	y	y	n	n	n	n	y	y	y
Priority Calling	n	y	y	n	n	n	n	n	n	y	y	y	y	y	y	y
Console Permissions	y	y	n	y	n	n	n	n	y	n	n	n	y	n	y	n
Off-hook Alert	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Client Room	y	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n
Restrict Call Fwd-Off Net	y	n	n	y	y	y	y	y	n	y	y	y	y	y	n	n
Call Forwarding Busy/DA	n	y	y	n	n	n	n	n	y	n	n	n	n	y	y	y
Personal Station Access (PSA)	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**	**y**
Extended Forwarding All	n	y	y	n	n	n	n	n	y	n	n	n	n	y	y	y
Extended Forwarding B/DA	n	y	y	n	n	n	n	n	y	n	n	n	n	y	y	y
Trk-to-Trk Transfer Override	n	y	y	n	n	n	n	n	n	n	n	n	n	n	y	y
QSIG Call Offer Originations	n	y	y	n	n	n	n	n	y	n	n	n	n	n	n	n
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

2. Verify that the **Personal Station Access** (PSA) field is set to **y**. The PSA field applies to the primary telephone and must be set to yes for EMU.
3. Type **`display feature-access-codes`**.

   The system displays the Feature Access Codes screen.

Figure 201: Feature Access Code screen

```
display feature-access-codes                                  Page   2 of   8
                              FEATURE ACCESS CODE (FAC)
                  Data Origination Access Code: #09
                      Data Privacy Access Code: #10
              Directed Call Pickup Access Code: #11
    Emergency Access to Attendant Access Code: #12
        EC500 Self-Administration Access Code:
                   Enhanced EC500 Activation:        Deactivation:
          Enterprise Mobility User Activation:       Deactivation:
 Extended Call Fwd Activate Busy D/A #87  All: #86    Deactivation: #85
       Extended Group Call Pickup Access Code: #82
              Facility Test Calls Access Code: 177
                            Flash Access Code:
            Group Control Restrict Activation: #15    Deactivation: *15
                  Hunt Group Busy Activation: #16    Deactivation: *16
                               ISDN Access Code:
                Last Number Dialed Access Code: #18
   Leave Word Calling Message Retrieval Lock: #19
  Leave Word Calling Message Retrieval Unlock: #20
           Leave Word Calling Send A Message: #88
         Leave Word Calling Cancel A Message: #89
             Malicious Call Trace Activation: #23    Deactivation: *23
```

4. Page down till you see the fields for **Enterprise Mobility User Activation** and **Deactivation**.
5. The feature-access-codes (FAC) for both EMU activation and EMU deactivation must be set on all servers using EMU. You must enter the FAC of the server in the location where you are dialing from.

   Note:
   To avoid confusion, Avaya recommends that all the servers in the network have the same EMU feature-access-codes.
6. Administer the EMU timer on the system-parameters features screen (Figure 202). The EMU timer applies to the visited server only. You can administer the timer for each server in the system. The amount of time a visitor can remain registered during a period of inactivity is entered in the **EMU Inactivity Interval for Deactivation (hours)** field. From one to 24 hours may be entered. If the entry is left blank, the EMU timer will not be used and the visited station will remain registered until it becomes unregistered by other means.
7. Administer the Emergency Extension Forwarding timer on the system-parameters features screen (Figure 203). The amount of time that must elapse before a visitor can log in as EMU after making emergency calls from an EMU-activated station is entered in the **Emergency Extension Forwarding (min)** field. The default value is 10 minutes.

Figure 202: system-parameters features screen for EMU

```
change system-parameters features Page   3 of  17
                    FEATURE-RELATED SYSTEM PARAMETERS
TTI/PSA PARAMETERS

  WARNING!  SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE

       Terminal Translation Initialization (TTI) Enabled? y
               TTI State: voice        TTI Security Code: 12345


                        Default COR for Dissociated Sets: 1
                           CPN, ANI for Dissociated Sets: 33333
         Unnamed Registrations and PSA for IP Telephones? n
              Customer Telephone Activation(CTA) Enabled? n
 Don't Answer Criteria For Logged Off IP/PSA/TTI Stations? n

EMU PARAMETERS
           EMU Inactivity Interval for Deactivation(hours):

CALL PROCESSING OVERLOAD MITIGATION
           Restrict Calls: stations-first
```

Figure 203: system-parameters features screen for Emergency Extension Forwarding timer

```
change system-parameters features                               Page   5 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                    Switch Name:
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                              COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds)? 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? n    UCID Network Node ID:
```

Setting EMU options for stations

To set EMU options for stations:

1. Type **add station next**.

   The system displays the Station screen.

Figure 204: Station screen

```
add station next                                          Page   1 of   4
                                    STATION

Extension: 20096                        Lock Messages? n          BCC: 0
     Type: 6408D+                       Security Code: *            TN: 1
     Port:                            Coverage Path 1:            COR: 1
     Name:                            Coverage Path 2:            COS: 1
                                      Hunt-to Station:

STATION OPTIONS
              Loss Group: 2             Personalized Ringing Pattern: 1
             Data Module? n                        Message Lamp Ext: 20096
            Speakerphone: 2-way                 Mute Button Enabled? y
        Display Language: english

                                                  Media Complex Ext:
                                                       IP SoftPhone? n
                                                Remote Office Phone? n
```

2. The following entries must be made on the Station screen:

   You enter the security code of your primary telephone when you activate or deactivate EMU. The security code is administered on page one of the station form. The security code can be up to eight numbers. No letters or special characters are allowed. Once the security code is entered, the system displays a ***** in the **Security Code** field.

3. On the Station screen, page down till you find the **EMU Login Allowed** field.

   The **EMU Login Allowed** field applies to the visited station and must be set to **y** for EMU. The valid entries to this field are **y** or **n** with **n** as the default. You must set this field to a **y** to allow this telephone to be used as a visited station by an EMU user.

4. Click **Enter** to save your changes.

Defining options for calling party identification

To define the options for calling party identification:

1. Type **display trunk-group *x***, where ***x*** is the number of the trunk group.

   The system displays the Trunk Group screen (Trunk Group screen on page 888).

Figure 205: Trunk Group screen

```
add trunk-group next                                          Page 3 of x
                            TRUNK FEATURES
           ACA Assignment? _          Measured: ____      Wideband Support? _
 Long Holding Time(hours): _                             Maintenance Tests? _
  Short Holding Time(sec): _  Data Restriction? _     NCA-TSC Trunk Member: _
  Short Holding Threshold: __        Send Name: _      Send Calling Number: _
             Used for DCS? _                          Send EMU Visitor CPN? y

Suppress # Outpulsing? _  Numbering Format: _______
Outgoing Channel ID Encoding: _________     UUI IE Treatment: ______
                                      Maximum Size of UUI IE Contents: ___
                                            Replace Restricted Numbers? _
                                           Replace Unavailable Numbers? _
                                                 Send Connected Number: _
                                             Hold/Unhold Notifications? _

        Send UUI IE? _
          Send UCID? _                BRS Reply-best DISC Cause Value: __
                                                 Ds1 Echo Cancellation? _

                                       US NI Delayed Calling Name Update? _

                           Network (Japan) Needs Connect Before Disconnect? _

Time (sec) to Drop Call on No Answer:_
Outgoing ANI:_
R2 MFC Signaling:_

DSN Term? n       Precedence Incoming _______   Precedence Outgoing _______
```

2. Page down till you see the **Send EMU Visitor CPN** field.

   This field controls calling party identification, that is, the extension of the primary telephone or the extension of the visited telephone that is used when a call is made from a visited telephone using the visited telephone dial pad. If you want the system to display calling party information of the primary telephone, the **Send EMU Visitor CPN** field must be set to **y**. There are areas where public network trunks disallow a call if the calling party information is invalid. In this case, there can be instances where the extension of the primary telephone is considered invalid and the extension of the visited telephone must be used. To display the extension of the visited telephone, you must set the **Send EMU Visitor CPN** field to **n**.

3. Click **Enter** to save your changes.

Note:
For QSIG trunk groups working between the visited server and the home server, the **Send Calling Number** field must be set to **y** for calls that originate at a visited station using a feature button.

End-user procedures for Enterprise Mobility User

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Enterprise Mobility User:

EMU activation process

Use the following steps to activate a visited telephone:

1. At the visited telephone, enter the EMU activation facility-access-code (FAC). You must enter the EMU activation FAC of the server in the location where you are dialing from.
2. Enter the extension of your primary telephone set.
3. Enter the security access code of your primary telephone set. This is the security code administered on the primary telephone's station form on the home server.

   If the registration is successful, you hear confirmation tone.

   If the registration is not successful, you hear audible intercept. Audible intercept is provided when:

   - The registration was rejected by the home server.
   - The telephone where the registration attempt is made is not administered for EMU use.
   - The T1 timer expires at the visited server.

If the home server receives a request from a visited server for a telephone that already has an EMU visitor registration active, the old registration is terminated and the new registration is approved.

If the primary telephone is in-use when a registration attempt is made, the registration attempt fails.

EMU deactivate process

Use the following steps to deactivate the visited telephone:

1. At the visited telephone, enter the EMU deactivation FAC. You must enter the EMU deactivation FAC of the server in the location where you are dialing from.
2. Enter the extension number of the primary telephone.
3. Enter the security code of the visited telephone.

   If the visited telephone does not deactivate, the telephone remains in the visited state. To deactivate the visited telephone you can:

   - Perform a busy-out, release busy-out at the visited server.
   - Enter the EMU feature deactivation code and the security code of the visited telephone at the home server location.
   - Press the <mute> RESET function on the IP telephone.

   Note:
   Anytime the visited telephone performs a reset, the EMU registration is deactivated.

   - Unplug the visited DCP set for a period of one minute.

   Note:
   Unplugging or disconnecting a 4600 series set will not result in the set being deactivated.

Enbloc Dialing and Call Type Digit Analysis

Use the Enbloc Dialing and Call Type Digit Analysis feature to allow users to automatically place outgoing calls based on the telephone number information in the telephone's call log, without the user having to modify the telephone number.

For more information, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Detailed description of Enbloc Dialing and Call Type Digit Analysis

Enbloc Dialing is the ability of Communication Manager software to receive in one message all of the digits necessary to set up a call, or any time the terminal makes a request rather than receiving digits one at a time.

Call Type Digit Analysis is the ability for Communication Manager to decide how to route a call based on all of the digits in a telephone number in a call log. The system administrator maintains the Call Type Digit Analysis Table, which is similar to AAR and ARS Routing Tables. A phone signals for Call Type Digit Analysis when the user places a call from the phone's call log or from the contacts or corporate directory. The telephone sends to Communication Manager the information stored in the call log, or from the list of contacts or the corporate directory. Communication Manager uses the Call Type Digit Analysis Table to analyze the stored number, determines a corresponding dialable number, and makes the call.

The Enbloc Dialing and Call Type Digit Analysis feature is available with Communication Manager 4.0, or later. It works in conjunction with Avaya terminals (proprietary signaling protocol): DCP, IP (H.323) and IP (SIP) terminals (96xx H.323 IP telephones, Avaya one-X Mobile Edition for S60 3rd Edition Dual-Mode SIP phones).

When the Communication Manager software finds a match between a dialed digit-string and an entry on the Call Type Digit Analysis Table:

1. Communication Manager deletes and inserts digits according to the first priority administered for that string. Numbers on the Table indicate priority.
2. Communication Manager tests the modified digit string against the administered call type **ext**, **udp**, **aar**, or **ars**.

Note:
ext covers the extension entries in the dialplan analysis tables, and **udp** covers the entries in the uniform-dialplan tables. The value in the UDP Extension Search Order field on the dialplan parameters form determines the order for checking the tables.

3. If the modified digit string matches a digit analysis entry for the administered call type, in both digits and string length, Communication Manager routes the call.
4. If the modified digit string matches no entries for the administered call type, Communication Manager deletes and inserts digits according to the next priority administered for that string, and continues to test the modified digit string against the administered call type.
5. When Communication Manager finds no match between a dialed digit-string and an entry on the Call Type Digit Analysis Table, it routes the call using the system dial plan.
6. An IP phone receives notice that entries exist in the Call Type Digit Analysis Table when the phone registers. If there are no entries when the phone registers, the telephone will not use call type even when an entry is added after the telephone is registered. The telephone processes new entries after it unregisters and reregisters.

Recovery strategy and behavior

During server recovery, Enbloc dialing maintains full or partial functionality, depending on the type of server recovery.

Enbloc works as designed when the following servers are in local survival mode: server duplication, LSP, ELS, ATM WAN Spare Processor, SREPN, ESS.

High-level Capacities

Communication Manager provides four manipulations and call-type choices per Call Type Digit Analysis entry.

- Digit manipulations and call-type choices = groups of Del, Insert, Type, corresponding to the various ways one might need to interpret a single digit string to make it something routable.

See *Avaya Aura™ Communication Manager System Capacities Table*, 03- 300511 under Documentation on http://support.avaya.com for additional capacities information.

Administering Enbloc Dialing and Log Type Digit Analysis

The following steps are part of the administration process for the Enbloc Dialing and Log Type Digit Analysis feature:

This section describes:

- Any prerequisites for administering the Enbloc Dialing and Log Type Digit Analysis feature
- Complete administration procedures for the Enbloc Dialing and Log Type Digit Analysis feature

Prerequisites for administering Log Dialing Digit Analysis

You must complete the following actions before you can administer the Enbloc Dialing and Log Type Digit Analysis feature:

- Enbloc dialing is available with Communication Manager Release 4.0 or later and with software updates.
  Call Type Digit Analysis takes place automatically. There must be at least one entry in the Call Type Digit Analysis Table for Call Type Digit Analysis to take place.

Administering Call Type Digit Analysis

To administer Call Type Digit Analysis:

1. Enter **`change calltype analysis`**.

   The Call Type Digit Analysis Table appears.

2. In the **Match** field, enter the digits the system uses to match to the dialed string.

   The dialed string contains the digits that Communication Manager analyzes to determine how to process the call. For example, enter **303** to match any dialed number beginning with 303.

3. In the **length: Min Max** fields, enter the minimum and maximum number of dialed digits for the system to match.

4. Enter up to four digit manipulations for this Match string.

   Enter the number of digits to delete, the number of digits to insert, and the call type against which to test the modified digit string.

Note:
There must be at least one entry in the Call Type Digit Analysis Table for Call Type Digit Analysis to take place.

Example of Call Type Digit Analysis

The example shows an administered Call Type Digit Analysis Table.

```
display calltype analysis                                        Page 1 of x
                        CALL TYPE DIGIT ANALYSIS TABLE
                                    Location:   all
    Dialed String             Delete Insert     Type    Delete Insert       Type
Match: 303_________________ 1: 0      __________ ars  2: 0__    1___________ ars
length: Min 10 Max 10    __ 3: 3      __________ ext  4: 0      011_________ ars
```

In the example, Communication Manager analyzes 3035554927 for routing.

1. Communication Manager deletes 0 digits, inserts nothing, and searches the resulting 3035554927 against the ARS tables.
2. If there are no matching entries, Communication Manager deletes 0 digits, inserts the digit 1, and searches the resulting 13035554927 against the ARS tables.
3. If there are no matching entries, Communication Manager deletes 3 digits, inserts nothing, and searches the resulting 5554927 against numbers of ext type in the dial plan.
4. If there are no matching entries, Communication Manager deletes 0 digits, inserts 011, and searches the resulting 0113035554927 against the ARS tables.

Interactions for Enbloc Dialing and Call Type Digit Analysis

This section provides information about how the Enbloc Dialing and Call Type Digit Analysis feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Enbloc Dialing and Call Type Digit Analysis in any feature configuration.

- Call Detail Recording (CDR)
  In the custom CDR record for each call, a data element records whether or not Call Type Digit Analysis was used for the call.
- Call Management System (CMS)
  CMS receives the unmodified digit string as sent by the phone to Communication Manager.

- Extended Trunk Access (ETA)
  ETA node number manipulation takes place only after Enbloc Dialing fails to match the dialed string against the Call Type Analysis Table, and the call is routed to the Communication Manager dial plan.
- Integrated Management (IM)
  IM provides access to the Call Type Digit Analysis Table.
- Personal Central Office Line (PCOL)
  A call routed over a PCOL trunk does not receive Call Type Digit Analysis.

End User Procedures for Enbloc Dialing and Call Type Digit Analysis

To invoke Call Type Digit Analysis, the end user must dial all the digits of an outgoing call from the call log or from the contacts or corporate directory. A call made by dialing from the keypad follows Communication Manager dial plan routing.

Enhanced Call Forwarding

Use Enhanced Call Forwarding (ECF) feature to forward incoming calls to different destinations depending on whether they are from internal or external sources.

Detailed description of Enhanced Call Forwarding

This section provides a detailed description of the Enhanced Call Forwarding feature.

The Enhanced Call Forwarding feature requires Communication Manager Release 4.0 or later.

There are three types of Enhanced Call Forwarding:

- Use Enhanced Call Forwarding Unconditional to forward all calls
- Use Enhanced Call Forwarding Busy to forward calls when the user's line is busy
- Use Enhanced Call Forwarding No Reply to forward calls when the user does not answer the call

The user can activate or deactivate any of these three types from their phone, and can specify different destinations for calls that are from internal and external sources. Users receive visual display and audio feedback on whether or not Enhanced Call Forwarding is active.

Display messages on the phone guide the user through the process of activating and de-activating Enhanced Call Forwarding, and for viewing the status of their forwarding.

Users can choose whether they want, at any one time, Call Forwarding or Enhanced Call Forwarding activated. The regular Call Forwarding feature (called "Classic Call Forwarding" to distinguish it from Enhanced Call Forwarding) continues to be available to users and has not changed.

Each of the three types of Enhanced Call Forwarding can have different destinations based on whether a call is internal or external. Therefore, six different destinations are possible to set up:

- Enhanced Call Forwarding Unconditional - internal
- Enhanced Call Forwarding Unconditional - external
- Enhanced Call Forwarding Busy - internal
- Enhanced Call Forwarding Busy - external
- Enhanced Call Forwarding No Reply - internal
- Enhanced Call Forwarding No Reply - external.

Each of these types of call forwarding can be activated either by Feature Access Codes or by feature button.

When Enhanced Call Forwarding is deactivated, the destination number is kept. When the user activates Enhanced Call Forwarding again, the same destination number can be used without having to type it again.

When Enhanced Call Forwarding is not activated for a call, the call goes to a coverage path, if one has been set up.

Chained Call Forwarding

In Communication Manager Release 5.2, the Chained Call Forwarding feature allows the calls to be forwarded up to 10 hops (each calling station is considered to be one hop) using a pre-set coverage path within the same switch.

- The number of hops is in the range 3 through 10.
- A coverage path is assigned for calls forwarded to the principal or last station. This is possible when specifying a coverage path. Administer the **Station Coverage Path For Coverage After Forwarding** field to **principal** or **last-fwd**.
- Mixed use of standard call forwarding (including Call Forwarding All Calls and Call Forward Busy/Don't Answer) and enhanced call forwarding (including Enhanced Call Forwarding Unconditional, Enhanced Call Forwarding Busy, and Use Enhanced Call Forwarding No Reply) is allowed on stations in the forwarding chain.
- Forwarding stops before the chain gets into an infinite loop or before the call gets back to the originating station.
- Call forwarding override is enabled on any station in the chain, allowing the call to be transferred to the previous station in the chain.

Feature Button

The feature button **cfwd-enh** has been added.

- The feature button is valid only for station terminal types where feature buttons can be administered, except for attendant consoles, and have displays.
- Only one Enhanced Call Forwarding button with a blank destination is allowed per station. Buttons with entered extension number can be multiple-administered, but only one for the same extension number.
- The button label **ECfwd** will be used for stations requiring downloadable button labels. This button label appears on the station's display for the button administered with the Enhanced Call Forwarding feature. The button label can appear in English (default), Italian, French, or Spanish.

Administering Enhanced Call Forwarding

The following steps are part of the administration process for the Enhanced Call Forwarding feature:

Enhanced Call Forwarding can be activated and deactivated from the SAT. You can display on the SAT screen the setting of all forwarding destinations for a station and whether forwarding is activated. You can also change each forwarding destination, and activate or deactivate it.

Note:

There is a new class of service entry for Enhanced Call Forwarding. In the Class of Service screen, make sure the **Call Forwarding Enhanced** field is set to **y** to allow a user to activate and deactivate the ECF feature.

Viewing Station Status for Enhanced Call Forwarding

To display station status for Enhanced call forwarding:

1. Type **display status station *xxxxx***.
   The system displays the General Status screen.

Figure 206: General Status screen

```
status station 30001                                    page 2 of x

                                GENERAL STATUS

CONNECTED STATION INFORMATION
               Part ID Number: unavailable
                Serial Number: unavailable

          Station Lock Active? no               TOD Station Lock? y

UNICODE DISPLAY INFORMATION
       Native Name Scripts:N/A
   Display Message Scripts:0x08000001:latn;ChiS
 Station Supported
Scripts:0x000801b7:Latn;Lat1;LatA;Grek;Cyrl;Hebr;Arab...

CF Destination Ext:
Enhanced Call Forwarding Destinations
                  Internal           External
   Unconditional:                    5385502
            Busy:
        No Reply: 5385599
```

2. Page down till you find the **Enhanced Call Forwarding Destinations** field.
   You can view the forwarding destination of each active kind of ECF administered for the station.
3. Click **Enter** to exit the screen.

Enabling Feature Access Codes for Enhanced Call Forwarding

To enable Feature Access Codes (FACs) for Enhanced Call Forwarding:

1. Type **`change feature-access-codes`**.
   The system displays the Feature Access Codes screen.

Figure 207: Feature Access Codes screen

```
change feature-access-codes                                  Page 1 of x
                                  FEATURE ACCESS CODE (FAC)
             Abbreviated Dialing List1 Access Code: ____
             Abbreviated Dialing List2 Access Code: ____
             Abbreviated Dialing List3 Access Code: ____
    Abbreviated Dial - Prgm Group List Access Code: ____
                          Announcement Access Code: ____
                           Answer Back Access Code: ____
                             Attendant Access Code: ____
          Auto Alternate Routing (AAR) Access Code: ____
            Auto Route Selection ARS) Access Code1: ____  Access Code 2: ____
                      Automatic Callback Activation: ____   Deactivation: ____
    Call Forwarding Activation Busy/DA: ____   All: ____   Deactivation: ____
               Call Forwarding Enhanced Activation: ____   Deactivation: ____
                   Call Forwarding Enhanced Status: ____
____                           Call Park Access Code: ____
                             Call Pickup Access Code: ____
    CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                        CDR Account Code Access Code: ____
                              Change COR Access Code: ____
                         Change Coverage Access Code: ____
                           Contact Closure Open Code: ____     Close Code: ____
                          Contact Closure Pulse Code: ____
```

2. In the **Call Forwarding Enhanced Activation/Deactivation** field, enter a Feature Access Code number to allow users to activate and one to deactivate Enhanced Call Forwarding. The FACs for activation and deactivation must be administered together. One cannot exist without the other. In contrast, the FAC for status display can exist by itself and without the others.
3. In the **Call Forwarding Enhanced Status** field, enter a Feature Access Code number to allow users to display the status of Enhanced Call Forwarding.

4. Press **Enter** to save your changes.

Enabling Chained Call Forwarding

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** till you see the **Chained Call Forwarding?** field. See Figure 208.

Figure 208: Feature Related System Parameters- Redirection Notification

```
change system-parameters features                              Page  15 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

SPECIAL TONE
                                  Special Dial Tone? n
          Special Dial Tone for Digital/IP Stations: none

REDIRECTION NOTIFICATION
                            Display Notification for Do Not Disturb? n
                            Display Notification for Send All Calls? n
                              Display Notification for Call Forward? n
                     Display Notification for Enhanced Call Forward? y
                          Display Notification for a locked Station? n
         Display Notification for Limit Number of Concurrent Calls? n
                           Display Notification for Posted Messages? n
                                 Scroll Status messages Timer(sec.): ___




Chained Call Forwarding? n
```

3. Set **Chained Call Forwarding?** to **y.**
4. Press **Enter** to save your changes.

Note:

Consider the Class of Restriction settings on the stations in the chain before enabling chained forwarding. The SIP stations in the chain cannot activate enhanced call forwarding.

Specifying a coverage path

1. Type **change system-parameters coverage-forwarding**. Press **Enter**.
   The system displays the System Parameters screen for Call Coverage/Call Forwarding.
2. Click **Next** till you see the **Chained Call Forwarding** field. See Figure 209.

Figure 209: Call Coverage/ Call Forwarding System Parameters screen

```
 change system-parameters coverage-forwarding                  Page   2 of   2
SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING
COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)

                        Coverage Of Calls Redirected Off-Net Enabled? n




CHAINED CALL FORWARDING
                              Maximum Number Of Call Forwarding Hops: 3
                  Station Coverage Path For Coverage After Forwarding: principal
```

3. Specify the **Maximum Number Of Call Forwarding Hops** (a value between 3 and 10).
4. Set the **Station Coverage Path For Coverage After Forwarding** to the desired path.

   Note:
   The field is visible only when **Chained Call Forwarding** is enabled.
5. Press **Enter** to save your changes.

End-user procedures for Enhanced Call Forwarding

End-users can activate or deactivate certain system features and capabilities. End-users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Enhanced Call Forwarding:

Activating Enhanced Call Forwarding

To activate Enhanced Call Forwarding using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The phone goes off hook.
2. Press 1 to activate Enhanced Call Forwarding.
3. Press
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
4. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
5. Dial the destination number to which calls will be forwarded.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

To activate Enhanced Call Forwarding using a Feature Access Code:

1. Press the Feature Access Code for activating Enhanced Call Forwarding.

   The phone goes off hook.
2. Press:
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
3. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
4. Dial the destination number to which calls will be forwarded.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

Deactivating Enhanced Call Forwarding

To deactivate Enhanced Call Forwarding using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The phone goes off hook.
2. Press 2 to deactivate Enhanced Call Forwarding.
3. Press
   - 0 for all Enhanced Call Forwarding
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 to show the status for Enhanced Call Forwarding No Reply
4. Press
   - 1 for internal calls
   - 2 for external calls
   - 3 for all calls

   You hear a confirmation tone if the deactivation was successful.

To deactivate Enhanced Call Forwarding using a Feature Access Code:

1. Press the Feature Access Code for deactivating Enhanced Call Forwarding.

   The phone goes off hook.
2. Press
   - 0 to deactivate all Enhanced Call Forwarding
   - 1 to deactivate Enhanced Call Forwarding Unconditional
   - 2 to deactivate Enhanced Call Forwarding Busy
   - 3 to deactivate Enhanced Call Forwarding No Reply
3. Press
   - 1 for internal calls
   - 2 for external calls
   - 3 for all calls

   You hear a confirmation tone if the deactivation was successful.

Reactivating Enhanced Call Forwarding

To activate or reactivate Enhanced Call Forwarding using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The phone goes off hook.
2. Press 1 to reactivate Enhanced Call Forwarding
3. Press
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 to show the status for Enhanced Call Forwarding No Reply
4. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
5. Optionally, dial the destination number to which calls will be forwarded.

   If you do not enter a destination number, the previous destination number will be used.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the action was successful.

To reactivate Enhanced Call Forwarding using a Feature Access Code:

1. Press the Feature Access Code for activating Enhanced Call Forwarding.

   The phone goes off hook.
2. Press
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
3. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
4. Optionally, dial the destination number to which calls will be forwarded.

   If you do not enter a destination number, the previous destination number will be used.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the action was successful.

Displaying Status

To display Enhanced Call Forwarding status using a feature button:

1. Press the feature button labeled **cfwd-enh**

   The phone goes off hook.
2. Press 3 to display status.

   Your phone will display the status of the different types of Enhanced Call Forwarding.

To display Enhanced Call Forwarding status using a Feature Access Code:

1. Press the Feature Access Code for displaying Enhanced Call Forwarding status.

   The phone goes off hook.
2. Press 3 to display status.

   You phone will display the status of the different types of Enhanced Call Forwarding.

Activating and deactivating Enhanced Call Forwarding from an off-network phone

To activate Enhanced Call Forwarding from an off-network phone:

1. Dial the remote access number, including barrier code or authentication code.
2. Press the Feature Access Code for activating Enhanced Call Forwarding.
3. Press:
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
4. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
5. Dial the forwarding station extension.
6. Dial the destination number to which calls will be forwarded.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

To deactivate Enhanced Call Forwarding from an off-network phone:

1. Dial the remote access number, including barrier code or authentication code.
2. Press the Feature Access Code for deactivating Enhanced Call Forwarding.
3. Press:
   - 0 for all Enhanced Call Forwarding
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
4. Press
   - 1 for internal calls
   - 2 for external calls
   - 3 for all calls
5. Dial the forwarding station extension.

   You hear a confirmation tone if the activation was successful.

Activating and deactivating Enhanced Call Forwarding from a phone with console permission

To activate Enhanced Call Forwarding from a phone with console permission:

1. Press the Feature Access Code for activating Enhanced Call Forwarding.

   The phone goes off hook.
2. Press:
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
3. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
4. Dial the forwarding station extension.

5. Dial the destination number to which calls will be forwarded.

   Dial # at the end of an external destination number, or wait for the timeout to expire.

   You hear a confirmation tone if the activation was successful.

To deactivate Enhanced Call Forwarding from a phone with console permission:

6. Press the Feature Access Code for activating Enhanced Call Forwarding.

   The phone goes off hook.

7. Press:
   - 0 for all Enhanced Call Forwarding
   - 1 for Enhanced Call Forwarding Unconditional
   - 2 for Enhanced Call Forwarding Busy
   - 3 for Enhanced Call Forwarding No Reply
8. Press
   - 1 to forward internal calls
   - 2 to forward external calls
   - 3 to forward all calls
9. Dial the forwarding station extension.

You hear a confirmation tone if the activation was successful.

Interactions for Enhanced Call Forwarding

This section provides information about how the Enhanced Call Forwarding feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Enhanced Call Forwarding under all conditions. The following considerations apply to Enhanced Call Forwarding:

- Agents

  Agents who are logged in at a station cannot activate, reactivate or deactivate Enhanced Call Forwarding by dialing the Feature Access Code.

- Attendant console

  An attendant console with console permission can activate, reactivate, or deactivate Enhanced Call Forwarding in the same way stations with console permission can do, except that they can not enable call forwarding for themselves. An attendant console can override any kind of active Enhanced Call Forwarding.

- Automatic Callback

  A user cannot use Automatic Callback if Enhanced Call Forwarding is active at the called station. If a user activates automatic callback before Enhanced Call Forwarding is activated at the called station, the system redirects the callback call attempt to the forwarding destination.

- Bridging

  The system does not terminate calls to a bridged appearance when Enhanced Call Forwarding No Reply is active at the user station.

- Call Coverage

  The priorities between Call Coverage and Enhanced Call Forwarding are the same as those between Call Coverage and Classic Call Forwarding.

- Call Detail Recording

  If the forced entry of account codes is required, the system does not forward calls to an off-network destination.

- Call Forwarding

  The following describes the interactions between Enhanced Call Forwarding and the classic Call Forwarding feature:

  - Call Forwarding All Calls and Enhanced Call Forwarding Unconditional cannot be active on one station at the same time.
  - Call Forwarding Busy/Don't Answer and Enhanced Call Forwarding Busy cannot be active on one station at the same time.
  - Call Forwarding Busy/Don't Answer and Enhanced Call Forwarding No Reply cannot be active on one station at the same time.

- Call Park

  When a user activates Enhanced Call Forwarding and then Call Park, the Call Park is in effect at the forwarded station, not at the called station.

- Chained Call Forwarding

  The following summarizes interactions with chained forwarding:

  When a forwarded call terminates at a station in which Enhanced Call Forwarding Unconditional is active (with both internal and external forwarding active) and chained forwarding is enabled but falls below the limit for blocking forwarding, the call is forwarded to the destination, regardless of the status of the Enhanced Call Forwarding

  - Busy and No Reply features. If only one type of forwarding (internal or external) is active, then only that type of call is forwarded.

  - When a forwarded call terminates at a station in which Enhanced Call Forwarding Busy is active (with both internal and external forwarding active) and chained forwarding is enabled but falls below the limit for blocking forwarding, the call is forwarded to the destination. If only one type of forwarding (internal or external) is active, then only that type of call is forwarded.
  - When a forwarded call terminates at a station in which Enhanced Call Forwarding No Reply is active (with both internal and external forwarding active) and chained forwarding is enabled but falls below the limit for blocking forwarding, the call is forwarded to the corresponding destination. If only one type of forwarding (internal or external) is active, then only that type of call is forwarded.

- Enhanced 911

  Enhanced Call Forwarding has no effect on Enhanced 911 auto callback.

- Enterprise Mobility User

  The following summarizes interactions with EMU:

  - EMU visited stations are not allowed to use Enhanced Call Forwarding.
  - EMU visited stations cannot activate, reactivate or deactivate Enhanced Call Forwarding.
  - A user on a station with console permission can activate, reactivate, or deactivate Enhanced Call Forwarding by dialing a Feature Access Code or pushing an Enhanced Call Forwarding feature button, when the user on which the action should have the effect is in visiting mode.

- Leave Word Calling

  Leave Word Calling cannot be activated towards a station that has Enhanced Call Forwarding active. If Leave Word Calling was activated before the user of the called station activated Enhanced Call Forwarding, the callback attempt is redirected to the forwarded destination.

- Limit number on concurrent call

  Call Forwarding Busy active (both types) and Limit Number on Concurrent Call also active, the call is forwarded to the destination that is stored in the memory. If only one kind of Enhanced Call Forwarding Busy is active, then only the call corresponding to the origin call type will be forwarded.

- OPTIM

  Users cannot activate, reactivate, or deactivate Enhanced Called Forwarding from OPTIM stations.

- Personal Central Office Line

  The system does not forward Personal Central Office Line calls.

- Posted Messages

  The following summarizes interactions with the Posted Messages feature:

  - When the Posted Messages feature is activated and Enhanced Call Forwarding is active, the display is overwritten by the posted message.
  - When the Posted Messages feature is deactivated and Enhanced Call Forwarding is active, the display is overwritten by the Enhanced Call Forwarding message.
  - When the Posted Messages feature is activated, activation of Enhanced Call Forwarding (whether by Feature Access Code, feature button, or the SAT) will have no effect on the display.

- Priority Call

  When a priority call terminates at an active Enhanced Call Forwarding station, the call is forwarded.

- QSIG

  Users cannot remotely activate or deactivate Enhanced Call Forwarding from a QSIG network.

- Send All Calls

  If a user has both Send all Calls and Enhanced Call Forwarding Unconditional active, calls to that station that can immediately be redirected to coverage are redirected. Other calls, such as priority calls, are forwarded to the designated station.

Interactions for Chained Call Forwarding

- Chained Call Forwarding is only valid, if the calls stay on the local switch. Once the call leaves the local switch the Call Forwarding Chain is broken.
- When a call is forwarded to a busy or no-reply station in which Enhanced Call Forwarding Busy is active and Chained Call Forwarding is enabled for call override, the call is forwarded to the called station for all internal and external calls.
- When a call is forwarded to a busy or out-of-service station in which Enhanced Call Forwarding Busy is active and Chained Call Forwarding is enabled and reaches the maximum number of call forwarding hops with no call coverage path set, the caller hears a busy tone.
- When calls are forwarded using chained call forwarding the calls to the forwarding station from the origination station follow a call coverage path.

Expanded Meet-me Conferencing

Use the Expanded Meet-me Conferencing (EMMC) feature to set up multi-party conferences consisting of more than six parties. The Expanded Meet-me Conferencing feature supports up to 300 parties.

Detailed description of Expanded Meet-me Conferencing

This section provides a detailed description of the Expanded Meet-me Conferencing feature.

The Expanded Meet-me Conferencing feature is an enhancement to the Communication Manager six-party Meet-me Conference feature. The Expanded Meet-me Conferencing feature supports up to 300 parties.

The Expanded Meet-me Conferencing feature is supported on all Linux platforms of Communication Manager (S8700, S8500, S8500B, S8300) running Communication Manager Release 3.0 software or higher.

Note:

For more information on Expanded Meet-me Conferencing, see the *Installation and Troubleshooting the Expanded Meet-me Conferencing (EMMC), 04-300527, Issue 1, April 2005*. You can also find additional information in *SIP Support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx servers, 555-245-206, Issue 3, May 2005*.

Highlights of Expanded Meet-me Conferencing

The following are some of the highlights of the Expanded Meet-me Conferencing feature:

- The Expanded Meet-me Conferencing feature is available on your system if your system is licensed for the feature. The license file variable for your system defines the maximum number of Expanded Meet-me Conferencing ports. The maximum allowed for a system is 300 ports. This variable is set in increments of 50 ports. The number of ports that your system has is determined by the license file for your system.
- Communication Manager uses a SIP trunk interface to connect to the Avaya EMMC Media Server. The Avaya EMMC Media Server is a separate server, and SIP trunking provides the interface between Communication Manager and the Avaya EMMC Media Server.

- For Communication Manager Release 3.0, the EMMC Media Server is a S8500B. The EMMC Media Server runs the Red Hat Linux 8.0 operating system, and has a software-based conferencing solution.
- You must check the new field **Maximum Number of Meet-me Conference Ports** on the System Parameters Customer-Options screen. If this field has a non-zero value, your system is enabled for the Expanded Meet-me Conferencing feature.
- The Expanded Meet-me Conferencing feature also allows you to administer the maximum number of parties allowed on each conference.This could be a system wide limit, and cannot exceed the number of ports your system is licensed for.
- The Expanded Meet-me Conferencing feature is available to all endpoints and trunk calls using Communication Manager.
- The Expanded Meet-me Conferencing feature is applicable only to meet-me conferences where the conferees dial into a conference VDN. This feature does not apply to ad-hoc conferences using the Conference button on your telephone.
- The Expanded Meet-me Conferencing feature provides all the regular capabilities of the six-party Meet-me Conference feature. This includes selective display, entry and exit tones, passwords, conference display updates, far-end mute and drop capabilities.
- To support the maximum of 300 Expanded Meet-me Conferencing ports, Communication Manager must use a minimum of two trunk groups and two signaling groups. Each trunk group on Communication Manager supports 255 trunk members.
- The Expanded Meet-me Conferencing feature supports G.711MuLaw, and you may need to administer a dedicated Network Region and codec set for the EMMC Media Server.

Expanded Meet-me Conferencing vectors and VDNs

The Expanded Meet-me Conferencing feature does not require any new vector steps. It uses the same vectors as the six-party Meet-me conference.

The following are the options for meet-me vectors:

- Meet-me idle - Use this vector step to view membership status information, that is, if a caller is idle or active. This vector replaces the six-party Meet-me Conference method of checking membership status using call records.
- Meet-me-access - This vector step is the same as the six-party Meet-me Conference.
- Meet-me-full - Use this vector step to determine how many active members are on a conference against the maximum number allowed for your system. If a party tries to join the conference after the system-wide limit has been exceeded, the system sends denial feedback to the member.
- Route-to-meetme - Use this vector step to route the call based on whether the conference is a six-party Meet-me Conference or an Expanded Meet-me Conference.

- Route-to Number - Use this field to create an unique conference ID to route the call to a SIP trunk, and to the Avaya EMMC Media Server. If this vector step fails, processing continues to the next step and the system logs a report.
- Announcement - This vector step is the same as the six-party Meet-me Conference.

  For the Meet-me full vector step, the recommended announcement is "All ports on this meet-me conference are in use."

  If the Route-to vector step fails because all licensed ports are already in use, the recommended announcement is "Your call cannot be routed at this time. Please try again later."

Expanded Meet-me Conferencing display updates

The Expanded Meet-me Conferencing feature provides real-time display updates for up to 30 conferees. Display updates for up to 30 is expected to meet the needs of most business conferences.

If Expanded Meet-me Conferencing size exceeds 30 parties, all other parties that join the conference see a fixed display that shows “CONFERENCE >30” in the **nnn** field of the end-user telephone. The display message can also be ">30 party conference in progress."

Users can select the conf-dsp button to get details regarding number of parties on the conference, and scroll through the list of parties.

- If a user presses the **conf-dsp** button once, the user can view the conference count with the text **<nnn>-party conference** field.
- If a user presses the **conf-dsp** button again, the system provides updated information as other parties join the conference.
- Pressing the **conf-dsp** button again enables the user to scroll through the list of parties on a conference.

Note:
This applies to ad-hoc, six-party Meet-me Conferences and Expanded Meet-me Conferencing.

Note:
The **conf-dsp** button is located on the Station screen in the Button Assignments area. You can select this button from the drop down list.

Language translations are available for system displays. You can also administer this in a user-defined language by using the **`display-messages-transfer-conference`** command in the Language Translations screen.

Status screens for Expanded Meet-me Conferencing

You can view Expanded Meet-me Conferencing system capacities by typing the **`display capacity`** command. The system displays the System Capacity screen. The two fields **Meet-Me Conference VDNs per System** and **Maximum Number of Expanded Meet-me Conference Ports** show the used, available, and system wide port limits for your system.

You can also view the **Conference Bridge Ports** field on the General Status screen to view the number of parties on each call and the system wide limit.

Administering Expanded Meet-me Conferencing

The following steps are part of the administration process for the Expanded Meet-me Conferencing feature:

- Setting the maximum number of parties for each conference
- Changing or creating a VDN for Expanded Meet-me Conferencing
- Setting language translations

This section describes:

- Any prerequisites for administering the Expanded Meet-me Conferencing feature
- The screens that you use to administer the Expanded Meet-me Conferencing feature
- Complete administration procedures for the Expanded Meet-me Conferencing feature

Prerequisites for administering Expanded Meet-me Conferencing

You must complete the following actions before you can administer the Expanded Meet-me Conferencing feature:

- On the Optional Features screen, ensure that the **G3 Version** field is set to **V13** or later. If the **G3 Version** field is not set to **V13** or later, your system is not enabled for the Expanded Meet-me Conferencing feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- On the Optional Features screen, click **Next** until you see the **Enhanced Conferencing** field. Ensure that this field is set to **y**. If the **Enhanced Conferencing** field is set to **n**, your system is not enabled for the Expanded Meet-me Conferencing feature. Contact your Avaya representative before you continue with this procedure.

- On the Optional Features screen, a numeric value must appear on the **Maximum Number of Expanded Meet-me Conference Ports** field.The maximum value for this field is 300, and it corresponds to the number of Expanded Meet-me Conferencing ports that your system has. This number can be less than 300, and is determined by the license file for your system.
- On the Optional Features screen, the following fields must also be set to **y** :
  - **Maximum Administered SIP Trunks**
  - **Maximum TN2501 VAL Boards**
  - **Maximum G250/G350/G700 VAL Sources**
  - **ISDN-PRI**
  - **IP Trunks**
  - **Vectoring (Basic)**
  - **Vectoring (Prompting)**
  - **Vectoring (G3V4 Enhanced)**

Screens for administering Expanded Meet-me Conferencing

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 3.0 (V13) or higher.	• **G3 Version**
	Ensure that your system supports Expanded Meet-me Conferencing.	• **Enhanced Conferencing**

Screen name	Purpose	Fields
Optional Features	Shows the maximum number of Expanded Meet-me Conferencing ports for the system. Also shows the other fields that must be set for the EMMC feature.	• **Maximum Number of Expanded Meet-me Conference ports** • **Maximum Administered SIP Trunks** • **Maximum TN2501 VAL Boards** • **Maximum G250/G350/ G700 VAL Sources** • **ISDN-PRI** • **IP Trunks** • **Vectoring (Basic)** • **Vectoring (Prompting)** • **Vectoring (G3V4 Enhanced)**
Feature-Related System Parameters	Sets the maximum number of parties allowed to join each conference.	• **Maximum Number per Expanded Meet-me Conf** • **Trunk-to-Trunk Transfer**
Vector Directory Number	Changing or creating a VDN for Expanded Meet-me Conferencing	• **Meet-me Conferencing** • **Conference type** • **Route-to Number**
Language Translations	Setting language translations	• **^- party conference**

Setting the maximum number of parties for each conference

To set the maximum number of parties allowed for each Expanded Meet-me Conference:

1. Type **`change system-parameters features`**.

   The system displays the Feature-Related System Parameters screen (Figure 210: Feature-Related System Parameters Screen on page 919).

Figure 210: Feature-Related System Parameters Screen

```
change system-parameters features                              Page   7 of  14
                        FEATURE-RELATED SYSTEM PARAMETERS

CONFERENCE/TRANSFER

               Abort Transfer? n                 No Dial Tone Conferencing? y
       Transfer Upon Hang-Up? y       Select Line Appearance Conferencing? y
Abort Conference Upon Hang-Up? n                                   Unhold? y
   No Hold Conference Timeout: 60  Maximum Ports per Expanded Meet-me Conf: nnn

ANALOG BUSY AUTO CALLBACK
               Without Flash? n


AUDIX ONE-STEP RECORDING
                            Recording Delay Timer (msec): 500
Apply Ready Indication Tone To Which Parties In The Call? all
  Interval For Applying Periodic Alerting Tone (seconds): 15
```

2. In the **Maximum Number per Expanded Meet-me Conf** field, type a value between 3 to 300. This sets the maximum number of parties allowed for each conference on your system.
3. Press **Enter** to save your changes.

Note:
The range allowed for this field is between 3 to 300. But 7 and above is recommended as this allows the use of six-party Meet-me Conference, or Expanded Meet-me Conferencing for larger conferences.

Changing or creating a VDN for Expanded Meet-me Conferencing

To change or create a VDN for Expanded Meet-me Conferencing:

1. Type **change vdn xxxxx**, where ***xxxxx*** is the vector directory extension number.

   The system displays the Vector Directory Number screen (Figure 211: Vector Directory Number screen on page 920).

Figure 211: Vector Directory Number screen

```
change vdn 50300                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                           Extension: 50300
                                Name: EMMC VDN
                      Vector Number: 10

                Meet-me Conferencing? y

                                 COR: 1
                                  TN: 1
```

2. If the **Meet-me Conferencing field** is set to **y** on the first page of this screen, go to the next page of the Vector Directory Number screen.

The system displays the Vector Directory Number screen (Figure 212: Vector Directory Number screen on page 920).

Figure 212: Vector Directory Number screen

```
change vdn 50300                                          Page   2 of   3
                          VECTOR DIRECTORY NUMBER



                MEET-ME CONFERENCE PARAMETERS:

                  Conference Access Code: 123456
                   Conference Controller:
                         Conference Type: expanded
                         Route-to Number: 850280
```

3. In the **Conference Type** field, you can enter the conference type to be a **6-party** or **Expanded**. The default for this field is **6-party**.
4. In the **Route-to Number** field, enter the administered unique UDP extension for the VDN.
5. Press **Enter** to save your changes.

Note:
The Route-to Number can have a maximum of 16 digits, and must be unique across all Expanded Meet-me Conference VDNs.

Setting language translations

If Language translations are enabled for your system, users can view Expanded Meet-me Conferencing displays in a user-defined language:

1. Type **change display-messages transfer-conference**.

   The system displays the Language Translations screen.

Figure 213: Language Translations screen

```
LANGUAGE TRANSLATIONS
19. English: Mute
Translation: ****
20. English: ^-party conference:
Translation: ********************************
```

2. In the **^- party conference** field, enter the number of parties on the conference at the time of display, and at the first push of the **conf-dsp** button.
3. The translation display appears on the second line.

End-user procedures for Expanded Meet-me Conferencing

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Expanded Meet-me Conferencing:

- **Conf-dsp** button - The conf-display button shows real-time updates about an Expanded Meet-me Conference. For more information, see Expanded Meet-me Conferencing display updates on page 915.
- **Fe-mute** - Far end mute allows the user to selectively mute a party on an Expanded Meet-me Conference. If the **conf-dsp** button is administered, the user sees a **fe-mute** button on the display information and can use the far end mute capability.
- Selective drop - If the **conf-dsp** button is administered, a user can use the Drop button on the telephone or station to drop a party from a call. If you are an attendant, you can press the **forced-rel** button. This is an important capability in situations where a conference gets interrupted by a conferee putting the call on hold, or if the Music on Hold feature is active.

Interactions for Expanded Meet-me Conferencing

This section provides information about how the Expanded Meet-me Conferencing feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Expanded Meet-me Conferencing in any feature configuration.

- Bridged Call Appearance - When callers on a Bridged Call Appearance dial into an Expanded Meet-me Conference, both sets of callers become a single party on the Expanded Meet-me Conference.

Extended User Administration of Redirected Calls

Use Extended User Administration of Redirected Calls to change your lead-coverage path or your call forwarding extension from any onsite or off-site telephone.

Detailed description of Extended User Administration of Redirected Calls

With Extended User Administration of Redirected Calls, a user can change the lead coverage path or the call forwarding extension from any onsite or off-site telephone.

The Extended User Administration of Redirected Calls feature does not change the Call Coverage, Call Forwarding All Calls, or Call Forwarding Busy/Don't Answer features. Extended User Administration of Redirected Calls merely allows a user to select between one of two previously administered coverage paths, or to change the forwarding extension from any telephone.

A user must enter both a Feature Access Code (FAC) and a Station Security Code (SCC) to use Extended User Administration of Redirected Calls from an:

- Onsite telephone that is not assigned to the user
- Off-site telephone

SECURITY ALERT:
The system logs invalid extensions and invalid SCCs as security violations. If you enable Security Violation Notification (SVN), the system displays the following information on the Monitor Security-Violations Station Security Codes screen or report:

- The extension or the incoming trunk from which the user dialed the command sequence
- The FAC
- The command string that the user dialed

For more information, see the Security Violation Notification on page 1441.

Disabling the telecommuting access extension

If you want to quickly disable Extended User Administration of Redirected Calls for all users, change the **Telecommuting Access Extension** field on the Telecommuting Access screen to blank.

Extended User Administration of Redirected Calls and DCS

If your users operate in a Distributed Communication System (DCS) environment, you must assign a different telecommuting access extension to each server. You must tell your users which extension to use for telecommuting access.

A user can use Extended User Administration of Redirected Calls from any of the DCS nodes. A user must dial the telecommuting access extension of the node on which the user telephone is defined, before the user can use any of the extended FACs.

Extended User Administration of Redirected Calls and Class of Service

Table 79: COS and Extended User Administration of Redirected Calls and Call Forwarding on page 924 shows the relationship between Class of Service (COS) and the ability to forward calls from the telephone that is assigned to a user without a security code, or from any onsite or off-site telephone with a security code.

Table 79: COS and Extended User Administration of Redirected Calls and Call Forwarding

If the COS of the user is set as follows:				The user can:	
Call Fwd All COS	**Call Fwd B/DA COS**	**Extended Call Fwd Activate All COS**	**Extended Call Fwd Activate Busy D/A COS**	**Forward calls from the user telephone without a security code**	**Forward calls from the user telephone or from another telephone with a security code**
Yes	Yes	Yes	Yes	Yes	Yes
No	No	Yes	Yes	No	Yes
Yes	Yes	No	No	Yes	No

Extended User Administration of Redirected Calls and COR

The user Class of Restriction (COR) controls the use of the change coverage option of Extended User Administration of Redirected Calls. If the **Can Change Coverage** field on the Class of Restriction screen is set to **y**, the user can use the FAC for Change Coverage Feature Access Code to change the coverage option.

Extended User Administration of Redirected Calls from an off-site telephone

To use Extended User Administration of Redirected Calls from an off-site telephone, a user must first access the telecommuting access extension. If the user makes a request through Direct Inward Dialing (DID), the user must precede the extension with the correct public network prefix. If the user makes the request through a trunk group that is dedicated to remote access, the user must dial the public network number for the trunk group.

The system provides dial tone after the user accesses the telecommuting access extension. After the dial tone, the user can enter only one of the four following FACs that are associated with Extended User Administration of Redirected Calls:

- Extended Call Fwd All Activate
- Extended Call Fwd Busy D/A Activate
- Extended Call Fwd Deactivation
- Change Coverage

Administering Extended User Administration of Redirected Calls

The following steps are part of the administration process for the Extended User Administration of Redirected Calls feature requires the following hardware:

- Assigning a Station Security Code to a user

This section describes:

- Any prerequisites for administering the Extended User Administration of Redirected Calls feature
- The screens that you use to administer the Extended User Administration of Redirected Calls feature

- Complete administration procedures for the Extended User Administration of Redirected Calls feature

Prerequisites for administering Extended User Administration of Redirected Calls

You must complete the following actions before you can administer the Extended User Administration of Redirected Calls feature:

- Ensure that the feature is enabled for your system.
- Assign a telecommuting access extension for your system.
- Assign the following extended Feature Access Codes (FACs) for your system.
  - Extended Call FWD Activates Busy D/A
  - Extended Call Fwd Activate All
  - Extended Call Fwd Deactivation
  - Change Coverage
- Assign the Class of Service (COS) for extended forwarding.
- Assign a Class of Restriction (COR) that allows a user to change coverage from an onsite or an off-site telephone.
- View the Optional Features screen, and ensure that the **Cvg Of Calls Redirected Off-Net** field is set to **y**. If the **Cvg Of Calls Redirected Off-net** field is set to **n**, your system in not enabled for the Extended User Administration of Redirected Calls feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

To assign a telecommuting access extension for your system:

1. Type **`add telecommuting-access`**. Press **Enter**.

   The system displays the Telecommuting Access screen (Figure 214: Telecommuting Access screen on page 926).

Figure 214: Telecommuting Access screen

```
add telecommuting-access
                          TELECOMMUTING ACCESS

                Telecommuting Access Extension: ________
```

2. In the **Telecommuting Access Extension** field, type an extension that conforms to your system dial plan. This extension can consist of 1 to 7 digits.
3. Press **Enter** to save your changes.

To assign the extended FACs for your system:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen (Figure 215: Feature Access Code (FAC) screen on page 927).

Figure 215: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 1 of 7

                          FEATURE ACCESS CODE (FAC)

            Abbreviated Dialing List1 Access Code: ____
            Abbreviated Dialing List2 Access Code: ____
            Abbreviated Dialing List3 Access Code: ____
   Abbreviated Dial - Prgm Group List Access Code: ____
                         Announcement Access Code: ____
                          Answer Back Access Code: ____
                            Attendant Access Code: ____
         Auto Alternate Routing (AAR) Access Code: ____
          Auto Route Selection (ARS) Access Code1: ____  Access Code 2: ____
                    Automatic Callback Activation: ____   Deactivation: ____
   Call Forwarding Activation Busy/DA: ____   All: ____   Deactivation: ____
                           Call Park Access Code: ____
                         Call Pickup Access Code: ____
   CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                     CDR Account Code Access Code: ____
                           Change COR Access Code: ____
                      Change Coverage Access Code: ____

                     Data Origination Access Code: ____
                         Data Privacy Access Code: ____
                 Directed Call Pickup Access Code: ____
```

2. In the **Change Coverage Access Code** field, type the FAC to change a coverage path from an onsite or an off-site telephone.
3. Click **Next** until you see the **Extended Call Fwd Activate Busy D/A All** field (Figure 216: Feature Access Code (FAC) screen on page 928).

Figure 216: Feature Access Code (FAC) screen

```
display feature-access-codes                                    Page   2 of 7
                              FEATURE ACCESS CODE (FAC)
                  Data Origination Access Code:
                      Data Privacy Access Code:
              Directed Call Pickup Access Code:
    Emergency Access to Attendant Access Code:
                    Enhanced EC500 Activation: *45    Deactivation: *46
  Extended Call Fwd Activate Busy D/A      All:       Deactivation:
       Extended Group Call Pickup Access Code:
              Facility Test Calls Access Code:
                           Flash Access Code:
            Group Control Restrict Activation:       Deactivation:
                  Hunt Group Busy Activation:       Deactivation:
                           ISDN Access Code:
                Last Number Dialed Access Code: *03
    Leave Word Calling Message Retrieval Lock: *33
  Leave Word Calling Message Retrieval Unlock: *34
           Leave Word Calling Send A Message: *35
         Leave Word Calling Cancel A Message: *37
              Malicious Call Trace Activation:       Deactivation:
        Meet-me Conference Access Code Change:
```

4. In the **Extended Call Fwd Activate Busy D/A All** field, type the FAC to activate Call Forwarding from an onsite or an off-site telephone.
5. In the **Call Fwd Activate Busy D/A All Deactivation** field, type the FAC to deactivate Call Forwarding from an onsite or an off-site telephone.
6. Press **Enter** to save your changes.

Note:
The system displays the FACs only if the **Cvg Of Calls Redirected Off-Net** field on the Optional Features screen is set to **y**.

To assign a Class of Service (COS) for extended forwarding:

1. Type **change cos**. Press **Enter**.

   The system displays the Class of Service screen (Figure 217: Class of Service screen on page 929).

Figure 217: Class of Service screen

```
change cos                                                    Page 1 of 1
                          CLASS OF SERVICE

                                  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

    Auto Callback                 n y y n y n y n y n  y  n  y  n  y  n
    Call Fwd-All Calls            n y n y y n n y y n  n  y  y  n  n  y
    Data Privacy                  n y n n n y y y y n  n  n  n  y  y  y
    Priority Calling              n y n n n n n n n y  y  y  y  y  y  y
    Console Permissions           n n n n n n n n n n  n  n  n  n  n  n
    Off-hook Alert                n n n n n n n n n n  n  n  n  n  n  n
    Client Room                   n n n n n n n n n n  n  n  n  n  n  n
    Restrict Call Fwd-Off Net     n y y y y y y y y y  y  y  y  y  y  y
    Call Forward Busy/DA          n n n n n n n n n n  n  n  n  n  n  n
    Personal Station Access (PSA) n n n n n n n n n n  n  n  n  n  n  n
    Extended Forwarding All       n n n n n n n n n n  n  n  n  n  n  n
    Extended Forwarding B/DA      n n n n n n n n n n  n  n  n  n  n  n
    Trk-to-Trk Restriction Override n n n n n n n n n n  n  n  n  n  n  n
    QSIG Call Offer Originations  n n n n n n n n n n  n  n  n  n  n  n
    Automatic Exclusion           n n n n n n n n n n  n  n  n  n  n  n
```

2. In the **Extended Forwarding All** field, type **y** in the column of each COS that allows a user to use extended Call Forwarding.
3. In the **Extended Forwarding B/DA** field, type y in the column of the COSs that allow a user to use extended Call Forwarding Busy/Don't Answer.
4. Press **Enter** to save your changes.

To assign a COR to change coverage from an onsite or an off-site telephone:

1. Type **change cor *n***, where ***n*** is the number of the COR to which you want to assign a COR to change coverage from an onsite or an off-site telephone. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 218: Class of Restriction screen on page 930).

Figure 218: Class of Restriction screen

```
change cor 1                                                  Page   1 of   4
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 7                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? y
         Priority Queuing? n                Direct Agent Calling? y
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                  Can Change Coverage? y

            Access to MCT? y             Fully Restricted Service? n
Group II Category For MFC: 7             Hear VDN of Origin Annc.? y
         Send ANI for MFE? n              Add/Remove Agent Skills? y
            MF ANI Prefix:               Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? y
                         Can Be Picked Up By Directed Call Pickup? n
                                     Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

2. In the **Can Change Coverage?** field, perform one of the following actions:
   - If you want users to change coverage from an onsite or an off-site telephone, type **y**.
   - If you do not want users to change coverage from an onsite or an off-site telephone, type **n**.
3. Press **Enter** to save your changes.

Screens for administering Extended User Administration of Redirected Calls

Screen name	Purpose	Fields
Feature Access Code (FAC)	Specify the FAC for extended administration of Call Forward Busy/Don't Answer and Call Forward All Calls.	• **Extended Call Fwd Activate Busy D/A All** • **Extended Call Fwd Activate Busy D/A All Deactivation**
	Specify the FAC for extended administration of the lead-coverage path.	**Change Coverage**
Class of Restriction	Administer a COR that allows the use of extended administration of the lead-coverage path.	**Can Change Coverage**
Class of Service	Administer a Class of Service (COS) that allows the use of extended administration of Call Forward Busy/Don't Answer and Call Forward All Calls.	• **Extended Forwarding All** • **Extended Forwarding B/DA**
Optional Features	Enable Extended User Administration of Redirected Calls.	**Cvg Of Calls Redirected Off-Net**
Station	Specify a Station Security Code (SSC) for a user.	• **Security Code** • **Coverage Path 1** • **Coverage Path 2**
Telecommuting Access	Define a telecommuting access extension for the system.	**Telecommuting Access Extension**

Assigning a Station Security Code to a user

To assign a Station Security Code (SSC) to a user:

1. Type **`change station n`**, where ***n*** is the number of the user extension to which you want to assign an SSC. Press **Enter**.

   The system displays the Station screen, (Figure 219: Station screen on page 932).

Figure 219: Station screen

```
change station 1014                                          Page 1 of 3
                              STATION

Extension: 1014               Lock Messages? n                  BCC: 0
     Type:                    Security Code:                     TN: 1
     Port:                  Coverage Path 1:                    COR: 1
     Name:                  Coverage Path 2:                    COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2            Personalized Ringing Pattern: 3
            Data Module? n                       Message Lamp Ext: 1014
           Speakerphone: 2-way                Mute button enabled? y
       Display Language? English                 Expansion Module?
                   Model:

 Survivable GK Node Name:                          Media Complex Ext:
                                                        IP Softphone? y
                                                  Remote Office Phone? y
```

2. In the **Security Code** field, type SSC.

   The **Minimum Security Code Length** field on the Feature-Related System Parameters screen determines the length of the SSC.

   The user must have a Coverage Path 1 and a Coverage Path 2. For more information, see the "Call Coverage" feature.

3. Press **Enter** to save your changes.

End-user procedures for Extended User Administration of Redirected Calls

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Extended User Administration of Redirected Calls:

- Changing Call Coverage or activating Call Forwarding from an onsite telephone that is not assigned to the user
- Deactivating Call Forwarding from an onsite telephone that is not assigned to the user

Changing Call Coverage or activating Call Forwarding from an onsite telephone that is not assigned to the user

To change Call Coverage or to activate Call Forwarding from an onsite telephone that is not assigned to the user:

1. Perform one of the following actions:
   - If you want to change the Call Coverage path, dial the Feature Access Code (FAC) for Change Coverage.
   - If you want to change Call Forward Busy Don't Answer, dial the FAC for Extended Call Fwd Activates Busy D/A All.

   The system generates a dial tone to prompt you for the extension.
2. Perform one of the following actions:
   - If the telephone has only bridged appearances, dial the telephone extension and then the pound sign (#).
   - If you want the system must use the extension of the currently active bridged appearance, dial the pound sign (#).
3. Dial the Station Security Code (SSC) for the extension, and then the pound sign (#)

   The system generates a dial tone to prompt you for the forwarded-to extension
4. Dial the forwarded-to extension

   The system generates a confirmation tone to indicate that the forwarded-to extension is valid.
5. Perform one of the following actions:

   If the change request is for the first coverage option, dial 1.

   If the change request is for the second coverage option, dial 2.

   The system generates a confirmation tone to indicate that the coverage is changed.

Deactivating Call Forwarding from an onsite telephone that is not assigned to the user

To deactivate Call Forwarding from an onsite telephone:

1. Dial the Extended Call Fwd Activates Busy D/A All Deactivation FAC

   The system generates a dial tone to prompt for the extension.
2. Perform one of the following actions:

- If the telephone has only bridged appearances, dial the telephone extension and then the pound sign (#).
- If you want the system must use the extension of the currently active bridged appearance, dial the pound sign (#).

  If you are at a BRI telephone with a display, the system displays all the information that you enter, until you complete the command sequence to change Call Coverage or to activate Call Forwarding.

  If you are at a telephone with a display, but the telephone is not a BRI telephone, the pound sign (#) is the last character that the system displays, until you complete the command sequence to change Call Coverage or to activate Call Forwarding.

3. Dial the SSC for the extension, and then the pound sign (#).

   The system generates a dial tone to prompt for the forwarded-to extension

Interactions for Extended User Administration of Redirected Calls

This section provides information about how the Extended User Administration of Redirected Calls feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Extended User Administration of Redirected Calls in any feature configuration.

- Bridged Appearance

  When a user presses the pound key (#) from a bridged appearance immediately after the user dials any of the Feature Access Codes (FACs) for Extended User Administration of Redirected Calls, the system allows the user can administer the extension of the currently active bridged extension. After the user enters the initial pound key (#), the user must dial the Station Security Code (SSC) of the currently active bridged extension to complete the command sequence.

  If the station has bridged appearances only, the user must dial a station extension after the FAC to complete the command sequence.

- Call Coverage

  Users can use the Extended User Administration of Redirected Calls feature to change the lead coverage path.

  The system denies an attempt to activate Send All Calls, if the coverage criteria of the currently active coverage path does not allow Send All Calls.

  If a user activates Send All Calls, and then changes the coverage path to a path that does not allow Send All Calls, the Send All Calls button remains lit. If the user changes the coverage path back to a path that allows Send All Calls, Send All Calls is automatically available to the user.

- Call Forwarding

  When Call Forwarding is active, the status lamps for the active features for that extension are lit. When Call Forwarding is deactivated, the status lamps for both Call Forward All Calls and Call Forward Busy/Don't Answer buttons for that extension are not lit.

  The system does not support forwarding to an off-network location.

- Distributed Communications System (DCS)

  You must assign a different telecommuting access extension for each server. Users can use Extended User Administration of Redirected Calls from any of the DCS nodes. The user must dial the extension of the node on which the telephone of the user is defined before the user dials the FAC.

- Security Violation Notification (SVN)

  If you enable SVN, the system tracks and reports Extended User Administration of Redirected Calls security violations for SSCs.

- Tenant Partitioning

  The system denies the request if the tenant number of the extension that a user dials is not accessible by the tenant number from which the user dials an FAC for Extended User Administration of Redirected Calls.

  If a user dials an FAC from an onsite telephone, the tenant number of the telephone from which the user dials the FAC must have access to the tenant number of the extension that the user dials. If the user dials the FAC from an off-site telephone, the tenant number of the incoming trunk must have access to the tenant number of the extension that the user dials.

Extension to Cellular

Use the Extension to Cellular feature to extend your office calls and Communication Manager features to a cellular telephone.

For user information for Extension to Cellular, see the *Avaya Extension to Cellular User's Guide*, 210-100-700.

For information on administration screens, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Detailed description of Extension to Cellular

This section provides a detailed description of the *Extension to Cellular* feature.

- Overview
- Conditional Call Extending Feature
- Shared Voice Connections Feature
- Sharing Mappings among CM PBXs
- SPFMC OPTIM Application
- one-X Mobile Server and Application Support
- Application RTUs for Fixed Mobile Convergence
- ARS/AAR routing
- Basic Extension to Cellular operation
- Call Detail Recording
- CDR Reports for Extension to Cellular Calls
- Call filtering
- Caller ID from the cell phone
- Capacity limitations
- Configuration sets
- Extension to Cellular Feature Access Codes
- EC500 Activation/Deactivation
- Self Administration Feature Access Code

- Conditional Call Extending
- Feature buttons on the office telephone
- Feature Name Extensions
- Multiple sets of Feature Name Extensions
- Mobile Call (CTI) Extension
- Multiple applications
- one-X Mobile Server and Application Support
- R2MFC trunks
- Security features
- Security codes
- Security tones
- Shared Voice Connections
- Sharing Mappings among CM PBXs
- SPFMC OPTIM Application
- Telephones supported
- Voice mail
- Voice Mail Avoidance
- Use timing to route calls
- Prevent coverage by cellular voice mail
- Cellular Voice Mail Avoidance Using Confirmed Answer

Overview

The Avaya Extension to Cellular feature provides users with the capability to have one administered telephone that supports Communication Manager features for both an office telephone and one outside telephone. An office telephone is a telephone that is directly under the control of Communication Manager, such as a desk telephone in an office. The outside telephone is a cellular or wireless telephone and is referred to in this text as a “cell phone.” Extension to Cellular works with any type of wireless or cellular service.

With Extension to Cellular, users can receive and place office calls anywhere, any time. People calling into an office telephone can reach users even if the users are not in the office. In addition, users can access Communication Manager features through the cell phone. Users can enable and disable Extension to Cellular so that the cell phone does not always receive office telephone calls. Users can also switch between the cell phone and office telephone during an ongoing Extension to Cellular telephone call.

When Extension to Cellular is administered and active, a call to the office telephone extension alerts both the office telephone and the cell phone simultaneously. In addition, Extension to Cellular maintains consistency in contact information. The cell phone takes on the identity of the office telephone when calls are made from the cell phone to another number on the same switch. In this circumstance, the cell phone sends the caller ID information of the office telephone. Therefore, calls from the cell phone appear to be from the office telephone number.

A user operates a cell phone as if it were a standard, caller ID-enabled telephone extension connected directly to the Avaya server running Communication Manager. The cell phone acts as an extension because it is mapped to the main office telephone. All other types of cell phone calls, such as direct calls to and from the published cell phone number, are not affected by Extension to Cellular. The cell phone performs exactly as it did before enabling Extension to Cellular. If your Cellular Service Provider (CSP) provides this service, Extension to Cellular is always enabled. You can also enable or disable Extension to Cellular by using a Feature Name Extension (FNE), as described in Setting up Feature Name Extensions set on page 968.

Note:
EC500 and CSP work only with ISDN-PRI, ISDN-BRI, H.323, Multi Frequency Compelled (MFC), and SIP trunks.

Cellular service providers who resell the Extension to Cellular service use the CSP or SPFMC (Service Provider Fixed-Mobile Convergence for dual mode phones) application type. CSP/SPFMC support ISDN, H.323, and SIP trunks. CSP/SPFMC is essentially the same as the Extension to Cellular application. Unlike Extension to Cellular, CSP/SPFMC is always enabled. Under CSP/SPFMC, users cannot disable Extension to Cellular.

The Extension to Cellular feature also supports the Fixed Mobile Applications (FMC), Public Fixed Mobility (PBFMC) and Private Fixed Mobility (PVFMC). The FMC applications are used for wireless endpoints that support a one-X Mobile Client application and have two modes called SMode (Single Mode) and DMode (Dual Mode). The FMC applications (PBFMC, PVFMC, and SPFMC) are the only OPTIM application that supports the CTI Mobility Integration feature.

When both PBFMC and the PVFMC applications are administered for a station, calls to that station extend calls out to both the public and private destinations specified in the station-mapping administration. If the private FMC application receives a message indicating that the far-end is alerting, the public FMC application cancels the call. Reception of an alerting indication means that the wireless endpoint must be present in the private wireless network and therefore cannot be in the cellular network.

See also Application RTUs for Fixed Mobile Convergence on page 941.

Conditional Call Extending Feature

Conditional Call Extending used to administer up to six different independent settings, controls which type of calls to extend when EC500 is enabled. You can administer the Conditional Call Extending settings and apply these settings to a specific application instead of the station as a whole. In addition to the administrator, the user can also set the Conditional Call Extending settings. Conditional Call Extending feature is used by FMC applications such as PBFMC, PVFMC, and SPFMC. This feature is not supported for PVFMC application when administered as a dual mode pair (DMX) with a ONE-X application. Conditional Call Extending feature is also not supported for OPS application.

The six different independent settings to control the type of call to extend are as follows:

- Standard calls to the station
- Calls covered or forwarded to the station
- Calls to the station through a hunt group
- Intercom calls to the station
- Priority calls to the station
- Calls restricted by a Class of Restriction (COR) permission matrix

Shared Voice Connections Feature

Shared Voice Connections allows two voice calls to share a single trunk connection between the cell phone and the PBX. For example, if the user is talking to someone and they wish to put the call on hold, using the cell phone second call appearance the user dials the Hold FNE (or uses the FMC application). The first call looks to be dropped at the cell phone, but is really on hold in Communication Manager. When you initiate or answer a second cell phone call, the first call is put on hold at the PBX and its voice connection is dropped; it is combined with the new active call as a shared connection. You can access and connect the held call using Recall FNE. You can use shared voice connection option only with the FMC applications such as PBFMC, PVFMC, and SPFMC.

Sharing Mappings among CM PBXs

The Sharing Mappings feature allows the station name and the station mapping information to be acrossed multiple Communication Managers. When you call into a PBX other than your own, the called station displays your name and number as administered on your own PBX. Extension to Cellular users can be recognized on another PBX where they are not administered. When the PBX acquires the shared information, it creates a temporary mapping to associate the shared cell phone number with the shared extension and the station name. Any calls with a calling number matching a temporary mapping use the shared station name and displays the extension for incoming call.

SPFMC OPTIM Application

Communication Manager Release 5.2 supports PBFMC RTU. An SPFMC Application that is used for support of service providers offering Extension to cellular is tied to the PBFMC RTU. An SPFMC application can be associated with a PVFMC application to support a dual-mode cell phone. You can define the application to be part of a dual-mode pair. There may be two sets of dual-mode pairs.

one-X Mobile Server and Application Support

Communication Manager Release 5.2 allows use of one-X Server to configure and control a set of features. The one-X Server controls alerting of any off-PBX telephone and its associated desk set by indicating which particular phone rings when an incoming call is received. Each extension can support four one-X applications. The one-X Server can extract information from Communication Manager. A SIP subscription is used as a transport mechanism between the one-X Server and the Communication Manager.

Class of Restriction (COR) permission determines whether the one-X Server is allowed to control a station.

Application RTUs for Fixed Mobile Convergence

The Fixed Mobile Convergence (FMC) application is used for wireless endpoints that support one-X Mobile Client.

FMC supports two modes called the following:

SMode (Single Mode) - Provides functionality for phones operating in the public cellular network. The existing RTU for Extension to Cellular can continue to be used to support the one-X Mobile Client application.

DMode (Dual Mode) - Provides functionality for dual mode wireless phones that operate in both the public cellular network and in a wireless SIP network.

An Extension to Cellular license provides an EC500 RTU or a Cellular Service Provider (CSP) RTU. A Single mode license provides an EC500 or CSP or SPFMC RTU or PBFMC RTU. A Dual Mode license provides an EC500 RTU CSP or SPFMC RTU or PBFMC RTU (single mode) and a private FMC (PVFMC) (dual mode) RTU.

Each dual-mode telephone requires two applications. The PBFMC application works similarly to Extension to Cellular and supports the cellular aspects of the dual-mode phone. The PVFMC application supports the SIP WiFi aspects of the dual mode phone. The two applications work together to support mobility features such as handover. If the dual mode endpoint is in both the WiFi and GSM range, WiFi gets priority and the call to the endpoint is routed through WiFi.

When you administer both public and private FMC applications for a station, calls to that station extend to public and private destinations as specified in administration for station mapping.

ARS/AAR routing

Extension to Cellular builds on a Communication Manager feature that allows extensions to be remotely connected over an ISDN trunk. Unlike traditional off-premises extensions, the stations are not tied to fixed channels on the T1/E1 interface. Instead, channels are allocated dynamically with each new call, allowing significantly more efficient use of the T1/E1 interfaces through traffic engineering.

Routing of Extension to Cellular extended calls takes the following path:

1. ARS (or AAR) digit conversion is applied to the administered dial prefix and cell phone number.
2. ARS (or AAR) analysis is applied to the result of Step 1.
3. The ARS (or AAR) analysis selects a routing pattern.
4. Each entry in the routing pattern is tried in order. However, if the trunk group for a particular entry is non-ISDN or non-IP and not R2FMC, the trunk group is skipped.
5. A trunk group is chosen for the Extension to Cellular call and the call is sent.

If no trunk is available, the Extension to Cellular call is not extended. However, the original call is not affected. The caller continues to hear ringback tone either until voice mail covers the call or the caller hangs up.

When the multiple locations customer option is enabled on Communicator Manager, location-based routing tables are chosen as follows:

For calls sent to the cell phone the location used is:

1. The location administered on the off-pbx station-mapping form
2. The location of station

For calls dialed from the cell phone the location used is:

1. The location administered on the off-pbx station-mapping form
2. The location of the incoming trunk

Basic Extension to Cellular operation

Calls to the desk set also ring on an associated cell phone. This is called termination mapping.

When an Extension to Cellular call is made to the cell phone:

- Status of office telephone shows both the Extension to Cellular status and the regular station status.
- Any other station linked to the call as part of a bridge or temporary bridge can bridge on to the cell phone call.
- The same calling number presented to the desk set is sent to the cell phone

When a user answers a call with a cell phone, Communication Manager treats the call as a local answer of a station.

Sometimes users do not require physical office numbers. Therefore, you can map the cell phones to an administration without hardware (AWOH) extension.

Extension to Cellular depends on ISDN PRI/BRI, R2MFC or SIP facilities to the PSTN. The customer must have ISDN PRI/BRI , R2MFC or SIP trunks enabled and have the appropriate circuit packs and the service from the PSTN.

Extension to Cellular users can access standard cellular features such as incoming call waiting and caller ID. If the cell phone and cellular network support call waiting, you can administer Extension to Cellular to deliver calls to a busy cell phone. Users can use cell phone features, such as swapping calls or conference calls, to answer the second call and manipulate the two calls.

If the cell phone and network support calling number identification, Communication Manager delivers the calling number to the cell phone. For calls that originate internally, the calling number can be presented in either the national numbering plan format or as an extension. You can control the number format through the administration of calling number identification. Note, some networks may not be able to carry an extension as a valid number. Some cell phone networks only pass calling number information in the national format, while others are more flexible.

Call Detail Recording

Extension to Cellular provides Call Detail Recording (CDR) options for calls to cellular/external telephones. Use the CDR feature to record information on incoming, outgoing, and tandem calls for each trunk group that you administer for CDR. The system records information on each trunk-group call and each station-to-station call. Call records might be desirable if you want to track calls to cell phones for reporting or charging purposes. Calls to cell phones are treated as either trunk calls or calls to an internal station extension. However, CDR is not generated for Feature Name Extensions (FNEs) or Feature Name URI's (FNUs).

For more general information, see the Call Detail Recording feature description in this document.

For more information about administering Call Detail Recording, see *Administering Avaya Aura™ Communication Manager,* 03-300509.

CDR Reports for Extension to Cellular Calls

The originating extension of the call is either:

- The office telephone extension to which the Extension to Cellular station is mapped
- The cell phone number

Extension to Cellular telephones are tagged on an intra-call CDR report when the call originates from an Extension to Cellular telephone. All Extension to Cellular CDR reports have an account code consisting of all 8s. An example account code is 8888. The code length can be up to the maximum administered length of the CDR Account Code.

If the principal station is being tracked in the Intra-Switch CDR report, a CDR record is generated for the station-side of the call. The CDR record contains the calling and called parties. This report is in addition to the CDR report for the Extension to Cellular call.

Two CDR reports can be generated for each Extension to Cellular call:

- The trunk CDR record containing the cell phone number
- The principal and the intraswitch CDR record containing the principal office telephone and the original calling party

When an intraswitch call and a trunk call originate at an Extension to Cellular telephone, only the trunk call gets reported in the CDR.

For more information, see Table 80: Enhanced CDR output for OPTIM originating calls, and Table 81: Enhanced CDR output for OPTIM terminating calls on page 946.

Table 80: Enhanced CDR output for OPTIM originating calls

"CDR Report?" field on the Trunk Group screen	"CDR for Calls to OPTIM Destination" field on the Configuration Set screen	OPTIM (or Principal in bridging setup) in the Intra-Switch CDR screen	Outcome	
			Type of CDR records (Trunk or Intra-switch)	Contents of interest
Yes	Yes	No	Trunk CDR	Destination + cell phone/SIP phone number + principal + OPTIM tag (88888)
Yes	Yes	Yes	1 CDR record (Trunk or Intra-switch)	Trunk CDR: Destination + cell phone/SIP phone number + principal + OPTIM tag Intra CDR: Destination + desk set extension
Yes	No	No	No CDR	N/A
Yes	No	Yes	Intra-switch CDR	Destination + desk set extension
No	Yes	No	No CDR	N/A
No	Yes	Yes	Intra-switch CDR	Destination + desk set extension
No	No	No	No CDR	N/A
No	No	Yes	Intra-switch CDR	Destination + desk set extension

Table 81: Enhanced CDR output for OPTIM terminating calls

"CDR Report?" field on the Trunk Group screen	"CDR for Calls to OPTIM Destination" field on the Configuration Set screen	OPTIM (or Principal in bridging setup) in the Intra-Switch CDR screen	Outcome	
			Type of CDR records (Trunk or Intra-switch)	Contents of interest
Yes	Yes	No	Trunk CDR	Cell phone/SIP phone number + principal + OPTIM tag (88888)
Yes	Yes	Yes	1 CDR record (Trunk or Intra-switch)	Trunk CDR: Cell phone/SIP phone number + principal + OPTIM tag Intra CDR: Principal + calling party
Yes	No	No	No CDR	N/A
Yes	No	Yes	Intra-switch CDR	Principal + calling party
No	Yes	No	No CDR	N/A
No	Yes	Yes	Intra-switch CDR	Principal + calling party
No	No	No	No CDR	N/A
No	No	Yes	Intra-switch CDR	Principal + calling party

Call filtering

With call filtering, you can manage cell phone costs by limiting the call type extended to the cell phone. Call filtering is based on the incoming call type received at the cell phone. You can choose to deliver external calls, internal calls, all calls, or no calls. All these calls can be delivered on a per-user basis.

Internal call filtering allows the switch to extend Extension to Cellular calls for all internally originated calls. External call filtering does the same for all public network incoming calls.

When call filtering does not allow a call, the cell phone does not receive the Extension to Cellular call. If so, the call can then be forwarded, or coverage treatment can be applied.

Call filtering only applies to Extension to Cellular calls extended to the cell phone; calls to the desk set are unaffected. If not answered, the call will go to the coverage path.

For more information, see Administering call filtering.

Caller ID from the cell phone

If administered with Origination Mapping, the Extension to Cellular telephone gains the identity of the user's office extension when calling into the Communication Manager. Origination mapping means that the cell phone is administered to present the office caller ID. When the cell phone user calls into the office, the person receiving the call sees the office name and office number of the caller, not the cell phone caller ID. This type of administration provides in-house caller identification at the destination telephone because the cell phone is mapped to the office telephone.

An Extension to Cellular telephone that is administered to gain the identity of the office telephone has the following functionality:

- When calling a number at the office (Communication Manager), the name and extension for the office telephone appear as the caller ID displayed on the destination telephone.
- A user can initiate a call to the office on an Extension to Cellular cell phone and pick up that same call in progress on the office telephone.
- When calling into the same office switch on which Extension to Cellular is administered, the Extension to Cellular cell phone functions as if it were an office telephone extension. For example, a corporate voice messaging system receives an Extension to Cellular cell phone call; the system recognizes the call as an extension on the switch.
- Origination mapping allows feature invocation by Feature Name Extension (FNE).

In some parts of the world, the calling number from a cellular phone may or may not include the country code. The support for origination mapping allows mapping a calling number to a station regardless of whether the calling party number contains a country code.

Sometimes an incoming international calling number will be prefixed by the international access code. To handle the international access code in front of a calling party number, you must administer it in the **International Access Code** field on the Locations Parameters screen (change location-parameters command).

To handle calling numbers with country codes, enter the country code (CC) in the **CC** field on the off-pbx station mapping screen. Communication Manager will match the calling number either with or without its country code with the office extension.

Capacity limitations

Extension to Cellular applications are allocated on a per station basis.

Note:
Use traffic engineering to ensure that there are enough trunks available to handle the traffic sent to the cell phones.

Extension to Cellular impacts trunk utilization extensively if a large percentage of the switch users are Extension to Cellular users. In many cases, the outbound trunk calls might not actually complete since the user can answer at the Extension to Cellular station.

The number of simultaneous call terminations towards the off-PBX station is limited to the maximum number of call appearances for each extension on the switch. However, this call limit number is usually less than the maximum call appearances. For example, Extension to Cellular users normally want the call limit at two, since most cell phones can handle only two calls at a time.

Configuration sets

A configuration set defines several call treatment options for Extension to Cellular cell phone calls. Extension to Cellular administration allows up to 99 configuration sets. All configuration sets begin populated in the system using default values. Because there are 99 configuration sets available, multiple combinations of the options can be administered, thus accommodating requirements for many cellular service providers.

For more information, see Changing configuration sets.

Extension to Cellular Feature Access Codes

A user can activate Communication Manager features related to Extension to Cellular through telecommuter Feature Access Codes (FACs). A user can access an FAC by one of these methods:

- Dialing the telecommuter number
- Dialing the remote access number
- Dialing the idle appearance select FNE

These FACs require the entry of a station extension and Station Security Code.

For more information about Extension to Cellular Feature access codes, see the *Avaya Extension to Cellular User's Guide,* 210-100-700.

EC500 Activation/Deactivation

The Enhanced EC500 Activation Feature Access Code enables the delivery of calls to the cell phone when the associated office telephone receives a call. It applies to the EC500 and PBFMC applications (all other applications are always enabled).

The Enhanced EC500 Deactivation Feature Access Code disables the delivery of calls to the cell phone when the associated office telephone receives a call. It applies to the EC500 and PBFMC applications (all others applications are always enabled and are unaffected by this feature).

For more information, see Creating FACs to enable/disable Extension to Cellular.

Self Administration Feature Access Code

The Self Administration Feature Access Code for EC500 (SAFE) can be altered by a user to change to the **dial prefix**, **CC** (country code), and **phone number** fields of the station-mapping form. This feature can be used for Extension to Cellular, Cellular Service Provider (CSP), Service Provider Fixed-Mobile Convergence (SPFMC), and Public Fixed Mobility (PBFMC) applications.

With SAFE, you can administer the **dial prefix** and the **country code** fields and the telephone number. Enhanced SAFE uses the asterisk (*) as the field delimiter between the dial prefix, the country code, and the phone number fields. SAFE also recognizes the sequence "**#" as meaning remove existing entries in the field (**dial prefix**, **country code**, and **phone number**).

The SAFE Access Code allows users to self-administer cell phone numbers for use with Extension to Cellular. The user calls one of up to four SAFE access codes and enters the cell phone number to add or change. SAFE automatically enables Extension to Cellular, and the cell phone number is recorded in the Stations with Off-PBX Telephone Integration screen (**`change off-pbx telephone station-mapping`**) on the **Phone Number** field.

The administration sequence for the user differs based on what phone is used to access SAFE. See the *Avaya Extension to Cellular User's Guide*, 210-100-700 for more information.

You cannot enter a destination number through SAFE if a user's desk set is restricted from calling that number.

For more information, see Creating a Self Administration Feature access code.

Conditional Call Extending

With the Conditional Call Extending feature, you can limit the type of calls that are extended to the cell phone when EC500 is enabled. You can administer the Conditional Call Extending settings and apply these settings to a specific application instead of the station as a whole. User can also set the Conditional Call Extending settings. Conditional Call Extending feature is used by the SIP and FMC applications such as PBFMC, PVFMC, and SPFMC. With the Conditional Call Extending feature, you can reduce the cellular use by restricting the undesired calls which results in improved productivity.

You can use the Conditional Call Extend Enable FNE and the Conditional Call Extend Disable FNE to enable and disable conditional call extending settings. To do that, you can use the Conditional Call Extend Activation FAC and the Conditional Call Extend Deactivation FAC.

You cannot administer the Conditional Call Extending state on the users' stations. User cannot make all Conditional Call Extending setting changes. User can administer the Conditional Call Extend FNEs or FACs on the station. To activate the Conditional Call Extending settings, you must enable the EC500 state for the user's station. Conditional Call Extending settings do not work when you disable the EC500 state.

You can set six different independent settings to decide the type of call to extend:

1. Standard calls to the station
2. Calls covered or forwarded to the station
3. Calls to the station through a hunt group
4. Intercom calls to the station
5. Priority calls to the station
6. Calls restricted by a COR permission matrix

For more information, see Administering Conditional Call Extending.

Feature buttons on the office telephone

You can enable Extension to Cellular applications with office telephone feature buttons. For example, you can administer feature buttons for enabling and disabling Extension to Cellular. You can also administer an optional timer for Extension to Cellular through the enable and disable feature button for H.323 and DCP phones. The Extension to Cellular feature button is available on telephones that support administrable feature buttons. With the Extend Call feature button, users can answer an Extension to Cellular call on the office telephone, and then move the call seamlessly to the cell phone.

The feature button will not enable or disable Extension to Cellular when a cellular service provider (CSP) or Service Provider Fixed-Mobile Convergence (SPFMC), application provides the Extension to Cellular capability.

The extend call button is available on wired office telephones. It is used to add the cell phone to an existing call at the office telephone.

For more information, see Administering a feature button to extend a call.

Feature Name Extensions

When the Extension to Cellular is enabled, a cell phone user can activate certain Communication Manager features by dialing a Feature Name Extension (FNE). Each FNE requires a direct inward dialing (DID) number. You, as the administrator, create the FNEs. The FNEs must comply with your dial plan and are administered system-wide.

For more information, see Setting up Feature Name Extensions set.

Multiple sets of Feature Name Extensions

You can use the Communication Manager to gain multi-country switch access by administering multiple sets of Feature Name Extensions (FNEs). You can have one Communication Manager with different gateways in multiple locations. Each gateway can have its own FNE set. The FNE sets are administered on the off-pbx-telephone feature-name-extensions screen. Each FNE is administered on its own form. For example, you can have one Communication Manager with gateways in France, Poland and Germany. The user can use the FNEs on the gateways closest to the user's physical location. If the user is in France and has to conference a call, the user can use the FNE on the gateway in France. In this way, you can reduce long distance charges by allowing you to choose a gateway that can most optimally process the call.

Mobile Call (CTI) Extension

This feature allows a CTI application to control extending of calls to Single and Dual mode applications: EC500, CSP, SPFMC, PBFMC, and PVFMC. If multiple applications are administered for an endpoint, the desk set applies the MCE only to the supported applications. The feature is invoked by making the office telephone call the Mobile Call Extension. This causes a call to be launched to the phone number of the application. This extension is administered on the off-pbx mobile-feature-ext screen.

When the call is answered, any FNE-based operation can be applied to the call, such as, recall, conference or transfer. After the conference or transfer, the cell phone call remains an OPTIM call associated with the calling station.

The user receives intercept tone for invalid calls to the Mobile Call Feature Extension, such as a call initiated from off the switch, or from a desk set that does not have a supported OPTIM application administered.

Multiple applications

You can administer up to four Extended Access applications on one telephone. Extended Access applications include Extension to Cellular, Cellular Service Provider (CSP), Service Provider Fixed-Mobile Convergence (SPFMC), SIP, and Public Fixed Mobility (PBFMC) PBFMC and Private Fixed Mobility PVFMC. You can also administer more than one instance of an application on one telephone. For example, you can map one office telephone to two different cell phones through Extension to Cellular.

When you map an office telephone to multiple applications, any Communication Manager feature enabled on one endpoint, such as the cell phone, applies to all other endpoints.

The EC500 status button shows a single station-wide state of EC500 activation regardless of the number of applications administered.

The Extend Call Button extends an active call to all mapped endpoints.

Extend call FNU is invoked at a mobile SIP endpoint or an OPS SIP station and extends an active call to all mapped mobile endpoints. The Extend Call FNU when invoked at an OPS SIP station or a mobile SIP endpoint will not extend the call back to itself.

Bridging tone applies when a call is active and a user on another mapped endpoint attempts to bridge on to the call. The following occurs:

- If a cell phone bridges to desk set on an active call – no tone will be heard.
- If the desk phone user attempts to bridge on a call that is active on cell phone - the cell phone user will hear intrusion tone.
- If the SIP OPS desk phone user attempts to bridge on a call that is active on cell phone - the cell phone user will hear intrusion tone.
- If a cell phone bridges to SIP OPS desk phone on an active call – the cell phone user will hear intrusion tone.
- If desk phone user attempts to bridge on a call that is active on a SIP OPS desk phone - the SIP OPS phone user will hear intrusion tone.
- If a SIP OPS desk phone user attempts to bridge on a call that is active on desk phone - no tone will be heard.

Self Administration FAC for EC500 allows a user to self-administer a cell phone number on the **phone number** field of the off-PBX telephone station-mapping screen for the EC500 and CSP applications. SAFE only applies to EC500, CSP, SPFMC, and PBFMC.

Exclusion will apply to all mapped endpoints; they will be excluded from an active call other than the endpoint that invoked exclusion.

All features invoked at any OPTIM endpoint will apply to all other endpoints. For example, SAC will apply to all mapped endpoint regardless of which one invoked SAC.

Multiple applications or single applications only allow one origination-mapping per phone number whereby the same cell phone number can not be administered more than once as both or origination.

one-X Mobile Server and Application Support

Communication Manager Release 5.2 allows use of one-X Server to configure and control a set of CM features. The one-X Server controls alerting of any off-PBX telephones and the desk set by indicating which particular phone rings when an incoming call is received. Each extension can support four one-X applications. The one-X Server can extract information from CM. A SIP subscription is used as a transport mechanism between the one-X Server and the CM. The SIP trunk is used for signaling and cannot be used to send voice traffic. The application data is passed in the message bodies of the Subscribe, Notify, and associated Response messages.

You can use Class of Restriction (COR) to control the stations that have one-X Server support. You can see the control status of a station using the status station command.

The one-X Server feature provides a way to control ringing of multiple phones tied to one extension and to provide real time calling information for a synchronized call log. Each one-X Server subscribes to one or more event packages.

The avaya-cm-one-x-call event package is used to convey control information from the one-X Server and the status information from Communication Manager. The avaya-cm-one-x-config event package conveys configuration information to a mobile client. The avaya-cm-one-x-call package conveys information in the bodies of SIP Subscribe, Notify, and Response messages. The message information is in XML format. Communication Manager provides administrative capabilities for the one-X Server feature. The one-X Server feature supports the following:

Static Call Handling	This enables the server to provide phone numbers for up to 4 off-PBX telephones. The server can control alerting of any off-PBX telephones and the desk-set. It indicates whether the particular phone must ring when an incoming call is received. A static mapping is used when a trigger mapping fails due to loss of connectivity between the Communication Manager and the one-X Server.
Triggered Call Handling	When this option is active, an incoming call does not alert the desk-set or any off-PBX telephone. Communication Manager must consult with the one-X Server for each incoming call with enough information to apply pre-existing screening rules. It responds to Communication Manager with a list of the phone numbers to alert. The phone numbers can be any combination of the desk-set extension and up to four off-pbx phone numbers.
Call Progress Reporting	A report is sent to the one-X Server for calls to and from a station with the one-X application at each of the following times: • Station initiates an outbound call • Station receives a call • Station answers a call • Station ends a call This report is not a Call Detail Recording (CDR) report.
Extended Access	This allows the off-PBX telephones to invoke a subset of Communication Manager features by dialing a DID number. These numbers are converted into Feature Name Extensions.
Autonomous Operation	Autonomous Operation occurs when there is a loss of communications between one-X Server and Communication Manager. In this case Static Call Handling can remain enabled. During autonomous operation Triggered Call Handling and Call Progress Reporting are disabled. The Static Call Handling profile is used when the Triggered Call Handling fails. When no Static Call Handling profile exists only the desk set is alerted.

For more information, see Administration for one-X Mobile Server and Application Support.

R2MFC trunks

OPTIM applications available with a Single mode license support calls over high function digital Multi Frequency Compelled (MFC) Signaling trunks. The digital MFC trunks provide answer supervision and can transmit calling number information. MFC trunks are supported only if answer supervision information is provided.

To get better digit processing, the administrator can insert 9 (or equivalent ARS or AAR Access Code) to use the digit conversion table which is administered on the ARS Digit Conversion screen. The **ANI Reqd** field indicates whether ANI must be requested for MFC trunk. This field has to be set for Extension to Cellular origination features to work.

The MFC trunks support the following features:

- Origination mapping
- Termination mapping
- SAFE
- FNEs
- Configurations Set Options
  - Calling Number Style
  - CDR for calls to Extension to Cellular destination
  - CDR for origination
  - Cellular voice mail avoidance
  - Barge-in tone

Security features

Extension to Cellular security features include security codes and security tones.

Security codes

Station security codes (SSC) provide security to station users by preventing other users from accessing functions associated with a station. Security codes are used with remote activation of Extension to Cellular. Remote activation allows off-premises users to dial in to the Communication Manager using a special DID number, that maps to a Remote Access Extension number. Users can then enter the security code, and can use any feature that can be accessed through Feature Access Codes. SAFE requires SSCs. Conditional Call Extending also requires SSC.

However, security codes are not always necessary for Extension to Cellular activation or deactivation.

- If the user's Class of Service provides console permissions, then a SSC is not needed.
- Users do not need a security code if the enable/disable Extension to Cellular button is administered on the office telephone.
- Enabling/disabling Extension to Cellular through an FNE used on a mapped cell phone does not require a Station Security Code.

As administrator, you can create a system-wide SSC change Feature Access Code (FAC) that users can invoke to change their desk phone's SSC. You must also administer and provide specific SSCs to users. A user cannot change a blank SSC. An SSC can be administered for an AWOH station.

The Extension to Cellular feature allows users to enable or disable all mapped extensions at one time, using the Station Security Code for the office telephone.

Security tones

The Conference and Barge-In tones can deliver more security for Extension to Cellular calls. A user hears a tone during an Extension to Cellular cell phone if someone picks up the office telephone mapped to the cell phone.

When an office telephone is mapped to multiple applications, a barge-in tone indicates when another user attempts to bridge on to a call through another telephone mapped to the office telephone. The following table summarizes when cell phone users hear a barge-in tone. The cell phones and SIP endpoints in the table are mapped to one office telephone with multiple applications.

Barging-in telephone		Active call	Tone
cell phone	bridges onto	office telephone	no
office telephone		cell phone	yes
SIP office telephone		cell phone	no
cell phone		SIP office telephone	no

If additional security is required, administer one of the exclusion features from Avaya. When you enable exclusion, this security feature applies to all off-PBX applications on one telephone.

Shared Voice Connections

In the Shared Voice Connections feature, you can share a single trunk for multiple calls as follows:

The user makes a call that is connected to the Communication Manager and they make another very short call (dialing an FNE) to put that call on hold. The connection between the cell phone and the Communication Manager is still active and can be used to dial another call. In this way one connection between the cell phone and the Communication Manager is used to manage two phone calls.

Any time you initiate or answer the second cell phone call, the first call is put on hold at the PBX and its voice connection is dropped; it is combined with the new active call as a shared connection. You can use shared voice connection option only with the FMC applications such as PBFMC, PVFMC, and SPFMC.

You can use the Recall FNE, Conference Complete FNE, and Transfer Complete FNE with the shared voice connection feature as follows:

- When you have a shared connection having an active voice call and a held call you can dial the Recall FNE to put the active call on hold and connect to the previously held call.
- You can use the Conference Complete FNE or the Transfer Complete FNE when there is an active call and a held call in a shared connection. The Conference Complete FNE conferences the two voice calls together while the Transfer Complete FNE transfers the held call to the active voice call.

  Note:
  If the long hold recall timer is administered, then you do not need to use the Recall FNE. The held call will be connected as soon as the long hold recall timer is expired and the active call will be placed on hold at office telephone.
- With the PVFMC application you need not use the Shared Voice Connection feature since SIP supports signaling hold, transfer, and conference.
- When your OPTIM application is part of one shared voice connection, you cannot be part of any other shared voice connection. You can use the same call appearance in multiple shared voice connection when the connections are associated with different OPTIM applications.

When you establish a shared connection, additional calls initiated or answered by the cell phone do not have any effect on the existing calls. When the active voice calls drops and only held call is there, then the shared connection becomes a residual shared connection. When the cell phone initiates or answers a new call, then the new call is added to the residual shared connection to form a shared connection. You can use the Held Appearance Select FNE to connect to the held call in a residual shared connection.

Sharing Mappings among CM PBXs

With the Sharing Mapping among CM PBXs feature, you can share the station name and station mapping information among multiple Communication Managers using SIP subscriptions. Extension to Cellular users can be recognized on another PBX where they are not administered. When the foreign Communication Manager acquires the shared information, it creates a temporary mapping to associate the shared cell phone number with the shared extension and the station name. Any calls with a calling number matching a temporary mapping can use the shared station name and extension for incoming call displays.

A SIP signaling group is needed for each pair of Communication Managers that share mappings. No SIP trunk group is required. Up to three such pairs may be administered allowing up to four Communication Managers to shared mappings.

For more information, see Administering Sharing Mapping among CM PBXs.

SPFMC OPTIM Application

Service Provider Fixed-Mobile Convergence (SPFMC) is similar to the Cellular Service Provider (CSP) application, but for service providers that support dual mode phones. SPFMC is always enabled and can handle anonymous SIP calls by blocking the caller's identity. SPFMC ignores the EC500 state of a station.

An SPFMC application can be associated with a PVFMC application to support a dual-mode cell phone. You can define the application to be part of a dual-mode pair. There may be two sets of dual-mode pairs. A **Dual Mode** field on the station mapping screen indicates which application is part of a dual-mode pair. **Dual Mode** field can have three values: **dm1**, **dm2**, or **blank**. If **Dual Mode** field is **blank** then application is not part of a dual-mode pair. Only FMC applications can have a non blank value in the **Dual Mode** field. The values of **dm1** and **dm2** indicate if the application belongs to a dual-mode pair. There can be two sets of dual-mode pairs (two dual mode phones) mapped to a desk set.

Telephones supported

The following telephone types can be administered as the office telephone for Extension to Cellular:

2402	4601	4610	4621	4625	6402	6408+	6416D+
2410	4602	4612	4622	4626	6402D	6408D	6424D+

2420	4606	4620	4624	4630	6408	6408D+	1603
1608	16CC	9620	9630	9640	9650		

Voice mail

Because the cell phone is treated as a local extension on the Avaya server running Communication Manager, the telephone can be completely integrated with the corporate voice messaging system. However, the cell phone can also keep the cellular service provider voice mail. This dual messaging capability presents an issue of where a user wants the message to go: corporate voice mail or cellular voice mail.

With regards to voice mail functionality and Extension to Cellular:

- The office number retains the primary extension on the Avaya server running Communication Manager.
- Calls to the office number simultaneously ring the office number and the cell phone. If neither answers, standard coverage arrangements take effect.
- As needed, you can disable Extension to Cellular when not in use to ensure that all unanswered calls go to the corporate voice messaging system.

The system administrator can control in-service and out-of-service status of the mapped extensions through a busy out and release maintenance capability. An unanswered call either ends at the corporate voice mail system or at the cellular service provider (CSP) voice mail system. The amount of control over the terminating voice mail system is limited. As administrator, you can use Cellular Voice Mail Avoidance and ring timing to direct Extension to Cellular calls to the appropriate voice mail coverage. See also Cellular Voice Mail Avoidance Using Confirmed Answer.

Voice Mail Avoidance

Communication Manager Extended Access Cellular Voice Mail Avoidance reduces the uncertainty as to where unanswered calls to the cell phone go for coverage. An unanswered call typically either ends at the corporate voice mail system or at the cellular service provider (CSP) voice mail system. You have limited control over the terminating voice mail system. You can administrator the number of ring cycles before a call goes to the corporate and cellular voice mail systems and enable Cellular Voice Mail Avoidance through Communication Manager.

The cellular voice mail system can lead to several problems for the user. The cellular network routes calls to cellular voice mail when any of the following conditions exist:

- Users do not answer a ringing call.
- The cell phone is in a bad coverage area.

- The cell phone is turned off.

With Cellular Voice Mail Avoidance, Communication Manager detects when the cell phone is not the entity answering the call and the call goes to Cellular Voice Mail. Communication Manager then “brings the call back” so that the call follows normal coverage treatment. The office telephone rings an appropriate number of times before sending the call to coverage.

Use timing to route calls

Unanswered office telephone calls are usually routed to a corporate voice messaging system after a predetermined number of rings. Similarly, most cellular service providers allow customers to route unanswered calls after a specified number of rings.

The number of times the desk phone or cell phone rings can be manipulated to help direct a call to the system of choice. To only receive voice messages through the corporate voice messaging system set the voice mail feature on the cell phone to a higher number of “unanswered rings” than the corporate system. For example, say the corporate voice messaging system automatically picks up an unanswered call on the third ring. The user then sets the cell phone voice mail system to pick up unanswered calls on the fourth or fifth ring.

Timing cannot ensure which voice mail system covers an unanswered call.

Users who cannot adjust the number of rings on the cell phones must contact the cellular service provider for assistance.

See also Cellular Voice Mail Avoidance Using Confirmed Answer.

Prevent coverage by cellular voice mail

Most cellular service providers route calls automatically to the cellular voice mail system when a cell phone is turned off or in an out-of-coverage area. To prevent work-related calls from being automatically routed to a cellular voice mail system, tell users to disable Extension to Cellular before shutting down the cell phone. Then, the corporate voice messaging system covers incoming calls to the office number and the cellular voice mail system picks up personal calls.

Note:
If a cell phone is used exclusively for business purposes, users can request that the cellular service provider disable voice mail.

See also Cellular Voice Mail Avoidance Using Confirmed Answer.

Cellular Voice Mail Avoidance Using Confirmed Answer

The Communication Manager supports the Confirmed Answer option for cellular voice mail avoidance for any OPTIM application, including Extension to Cellular. With Confirmed Answer set to **yes** on the user's Configuration Set screen, when answering the phone, the user hears the dial tone. The user must then press one of the digits on the cellular phone's keypad. Until the system receives a digit, the system does not treat the call as answered. The time to wait for the digit can be administered from 5-20 seconds, with a default of 10 seconds. Communication Manager plays recall dial-tone to indicate that input is expected. During the response interval, the original call continues to alert at the desk set and any stations bridged to the call. If a user does not enter a digit before the time-out interval expires, the call is pulled back from the cell phone.

If the user wishes to use the cell phone for both personal and business calls, the Confirmed Answer option can be used to both guarantee that business calls (to the enterprise phone number) do not end up in cellular voice mail. The Confirmed Answer option also notifies the user on answer whether the call went to the enterprise phone number, or directly to the cell phone number.

- In some businesses with the Extension to Cellular (such as for after hours support), it is critical that a call be treated as answered only if a person answers the call. In such a scenario, Confirmed Answer is the only reliable voice mail avoidance method.
- Confirmed Answer is the most reliable form of cellular voice mail avoidance. An added benefit of the feature is that the dial-tone is a signal to the user that the call is a business call, not a personal call.

See also Setting up a Cellular Voice Mail Avoidance timer.

Administering Extension to Cellular

The following steps are part of the administration process for the Extension to Cellular feature:

- Mapping an office telephone to a cell phone
- Setting up Feature Access Codes
- Creating a telecommuting access number
- Setting up Feature Name Extensions set
- Creating a Self Administration Feature access code
- Administer the office extension
- Administer the Feature Access Code
- Creating FACs to enable/disable Extension to Cellular

- Creating a Station Security Code FAC
- Creating a system-wide SSC change FAC
- Defining the Station Security Code length
- Administering an enable/disable feature button
- Changing the EC500 state on the station form
- Administering a feature button to extend a call
- Setting the optional timer
- Reviewing feature button assignments
- Sending 10-digit caller identification for locally originated calls
- Administering call filtering
- Administering voice mail coverage
- Setting up a Cellular Voice Mail Avoidance timer
- Using timing to route calls to voice mail
- Setting up Call Detail Recording
- Enable CDR for the outgoing trunk
- Enable CDR for Extension to Cellular
- Generating two CDR records
- Changing configuration sets
- Administering the barge-in tone
- Displaying System Capacity

This section describes:

- Any prerequisites for administering the Extension to Cellular feature
- The screens that you use to administer the Extension to Cellular feature
- Complete administration procedures for the Extension to Cellular feature

Prerequisites for administering Extension to Cellular

You must complete the following actions before you can administer the Extension to Cellular feature.

Plan extensions and codes

Prepare a plan for Extension to Cellular users including the following numbers and codes:

- Station security code associated with the office number
- Feature access code (FAC) for the change Station Security Code
- Self administration FAC (SAFE)
- Extension to Cellular enable and disable FACs
- Avaya Extension to Cellular telecommuting access number
- Extension number for the Avaya Extension to Cellular telecommuting access number
- Extension to Cellular activation and deactivation codes to enable and disable Extension to Cellular
- Feature access code for changing the Station Security Code
- List of all the Feature Name Extensions (FNEs) that you set up, and the features that they are mapped to

Review customer options

To review customer options on the **Optional Features** screen and ensure that you can administer Extension to Cellular (EC500) extensions:

1. Type **`display system-parameters customer-options`**. Click **Enter**.

   The system displays the Optional Features screen.
2. Verify that the **G3 Version** field is set to **V14** or later.
3. Verify that the **Maximum Off-PBX Telephones - EC500** field shows the number of licenses purchased for Extension to Cellular plus the number of licenses purchased for SMODE.
4. Verify that the **Maximum Off-PBX Telephones - PBFMC** field shows the number of licenses purchased for DMODE.
5. Verify that the **Maximum Off-PBX Telephones - PVFMC** field shows the number of licenses purchased for DMODE.
6. Verify that trunks are administered:
   - If using H.323 trunks, page down and verify that **Maximum Administered H.323 Trunks** field is set to a value greater than zero
   - If using SIP trunks, page down and verify that **Maximum Administered SIP Trunks** field is set to a value greater than zero.
7. Page down to find the **ARS** field and verify that the **ARS** field is set to **y**.
8. Page down and verify that:
   - The **Enhanced EC500** field is set to **y**.

     When the **Enhanced EC500** field is set to **y**, all remaining screens that are tied to the **`off-pbx-telephone`** commands become available.

- Either the **ISDN-BRI Trunks** field, the **ISDN-PRI** field, or **Multifrequency Signaling** field, or all three fields are set to **y**.
- For H.323 and SIP stations, the **IP Trunks** field is set to **y**.
- The **Extended Cvg/Fwd Admin** field is set to **y**.

  This setting allows you access to the Telecommuting Access Number screen where you set the EC500 access code.

9. Click **Enter** to exit the screen.

For more information on *the **Optional Features** screen*, see *Avaya Aura™ Communication Manager Screen Reference,* 03-602878.

Screens for administering Extension to Cellular

Screen name	Purpose	Fields
Stations with Off-PBX Telephone Integration	Map station extensions to application types and external telephone numbers.	All
Off-PBX Telephone Mobile-Feature-Ext	Administer CTI feature	**Mobile Call (CTI) Extension**
Feature Access Code (FAC)	Set up access codes for Communication Manager features	Feature Access Code
Extension to Call Which Activate Features by Name	Map a dialed extension to activate a feature (FNE) within Communication Manager from a cell phone. Some FNEs require FAC administration.	Extension
Telecommuting Access	Create an Extension to Cellular remote access number	All
Security-Related System Parameters	Define a system-wide Station Security Code length	Minimum Station Security Code Length
Station	Assign feature buttons and timers	Button Assignments
Language Translations	To review the office telephone feature button assignments	All
Numbering-Public/ Unknown Format	Assign 10-digit caller identification	All

Screen name	Purpose	Fields
Coverage Path	Set up number of unanswered rings before coverage	Number of Rings
Trunk Group	Enable Call Detail Recording for outgoing trunk	CDR Reports
DS1 Circuit Pack	Administer a DS1 Circuit pack for R2MFC for Extension to Cellular use.	Signaling Mode: CAS Interconnect: CO
Trunk Group	Administer a DID trunk group for R2MFC signalling and Extension to Cellular use.	Group Type: did Trunk Type: immed-start **Incoming Dial Type: mf** (for MFC signaling)
Trunk Group	Administer a DOID trunk group for R2MFC signalling and Extension to Cellular use.	Group Type: diod Trunk Type: immed-start Trunk Type: immed-start Outgoing Dial Type: mf (for MFC signaling) **Incoming Dial Type: mf** (for MFC signaling) **Receive Answer Supervision? y**
Multifrequency-signaling-related-parameters	Administer MFC parameters needed for Extension to Cellular.	Incoming Call Type: group-ii-mfc (for MFC signaling) Outgoing Call Type: group-ii-mfc (for MFC signaling) Request Incoming ANI (non-AR/ARS)? y
System Capacity	Verify used, available, and system station limits	Off-PBX Telephone - EC500 Off-PBX Telephone - OPS Off-PBX Telephone - PBFMC Off-PBX Telephone - PVFMC

Mapping an office telephone to a cell phone

To map an office telephone to an Extension to Cellular cell phone:

1. Type **`add off-pbx-telephone station-mapping`**. Click **Enter**.

   The system displays the Stations with Off-PBX Telephone Integration screen.

Figure 220: Stations with Off-PBX Telephone Integration screen

```
add off-pbx-telephone station-mapping                              Page 1 of 3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station     Application   Dial     CC    Phone Number          Trunk       Config
Extension                 Prefix                             Selection   Set
43001         EC500       ____ -   1     9736831204            ars         1
43001         OPS         ____ -         12345                 ars         5
43009         PBFMC       ____ -         67890                 aar         2
43011         CSP         ____ -   998   6095343211            ars         3
```

2. Fill in the information in all fields for each **Station Extension**. You can add up to sixteen associations between an office telephone and an external telephone. You can add up to four associations for the same extension.
3. Page down to the second page of the Stations with Off-PBX Telephone Integration screen (Figure 221: Stations with Off-PBX Telephone Integration screen, page 2 on page 965).

Figure 221: Stations with Off-PBX Telephone Integration screen, page 2

```
add off-pbx-telephone station-mapping                              Page 2 of 3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station          Call       Mapping        Calls       Bridged
Extension        Limit      Mode           Allowed     Calls          Location
43001            2          both           all         both
43001            2          both           all         both           255
43009            2          both           all         both           5
43011            2          both           all         both
```

The information you entered in the **Station Extension** field on the first page appears as read-only information on this second page.

4. Enter the **Mapping Mode** for each **Station Extension**.
5. Enter the category of **Calls Allowed** for each **Station Extension**.
6. Enter the type of **Bridged Calls** allowed.
7. Tab over to the **Location** field. Enter the Location value for each OPS, PBFMC or PVFMC application that you have administered on Page 1. The location values can be 1 to 255. You can find the location value on the **Locations** screen (**`change locations`**).
   - For a DCP set, enter the location of the media gateway.
   - For an IP set, enter the location of the network region for the set.
   - If blank, use the location of the incoming trunk. The default for this field is blank.

8. Page down to next page, Stations with Off-PBX Telephone Integration, page 3 (Figure 222: Stations with Off-PBX Telephone Integration screen, page 3).

Figure 222: Stations with Off-PBX Telephone Integration screen, page 3

```
add off-pbx-telephone station-mapping                          Page 3 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station        Appl     Share Calls Accepted
Extension      Name     Level S C H I P R-COR
43001          EC500    5
43001          OPS
43009          PBFMC    5     y y y y y y 1
43009          PVFMC    _     y y y y y n ___
43011          SPFMC    5     y y n y y y 101
43011          PVFMC    _     y y y y y y 99
```

9. For Sharing Mappings among CM PBXs feature, enter the Share Level value for EC500, CSP, PBFMC, and SPFMC applications (See Administering Sharing Mapping among CM PBXs).
10. For Conditional Call Extending feature, enter **Calls Accepted S C H I P R** and **COR** field values (See Administering Conditional Call Extending).
11. Click **Enter** to save your changes.

For more information about *the **Stations with Off-PBX Telephone Integration** screen and field descriptions*, see the *Avaya Aura™ Communication Manager Screen Reference,* 03-602878.

For more information on the **Location** field, see the *Avaya Aura™ Communication Manager Screen Reference,* 03-602878.

For more information about the **`off-pbx-telephone station-mapping`** commands, see the *Maintenance Commands for Avaya Aura™ Communication Manager Media Gateways and Servers*, 03-300431.

Setting up Feature Access Codes

To administer Feature Access Codes (FACs):

1. Type **`change feature-access-codes`**. Click **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 223: Feature Access Code (FAC) screen on page 967).
2. Type access codes according to your dial plan for the applicable features. Page down to access all pages of this screen.

Figure 223: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page   1 of   x
                              FEATURE ACCESS CODE (FAC)
                Abbreviated Dialing List1 Access Code: 0101
                Abbreviated Dialing List2 Access Code: 0102
                Abbreviated Dialing List3 Access Code: 0103
     Abbreviated Dial-Program Group List Access Code: 0104
                           Announcement Access Code: 0105
                            Answer Back Access Code: 0106

            Auto Alternate Routing (AAR) Access Code:
              Auto Route Selection (ARS) Access Code:
                       Automatic Callback Activation: 0107  Deactivation: 0108
                  Call Forwarding Activation Busy/DA: 0110  Deactivation: 0111
                                Call Park Access Code: 0112
                              Call Pickup Access Code: 0113
      CAS Remote Hold/Answer Hold-Unhold Access Code: 0114
                          CDR Account Code Access Code: 0115
                                Change COR Access Code: 0116
                           Change Coverage Access Code: 0117
                  Conditional Call Extend Activation: *39   Deactivation: #39
                            Contact Closure Open Code:        Close Code:
```

3. Click **Enter to save your changes**.

   A user can now activate Communication Manager features from any telephone through the FACs. A user can access the FACs through one of these three methods:

   - Dialing the telecommuter number
   - Dialing the remote access number
   - Dialing the Select Idle FNE

   After hearing the dial tone, the user enters the FAC.

Creating a telecommuting access number

To configure the Avaya server running Communication Manager for Extension to Cellular access by a remote user:

1. Type **`change telecommuting-access`**. Click **Enter**.

   The system displays the Telecommuting Access screen (Figure 224: Telecommuting Access screen on page 968).

Figure 224: Telecommuting Access screen

```
change telecommuting-access                                  Page   1 of   1
                              TELECOMMUTING ACCESS

                      Telecommuting Access Extension: 5437
```

2. In the **Telecommuting Access Extension** field, type an extension in accordance with your dial plan. The telecommuting number must be a direct inward dialing (DID) or central office (CO) trunk destination for off-premises features to work.
3. Click **Enter to save your changes**.
4. Provide your users with the telecommuting access number to enable or disable Extension to Cellular, or to change their Station Security Code.

Setting up Feature Name Extensions set

To map a dialed extension to a Communication Manager feature:

1. Type **`change off-pbx-telephone feature-name-extensions set <n>`**. Click **Enter**.

   The system displays the Extensions to Call which Activate Features By Name screen for the set identified in the command. See Figure 225 and Figure 226: Off-Pbx-Telephone Feature Feature Name Extensions (FNE). Set numbers can be 1 through 99.

Figure 225: Off-Pbx-Telephone Feature Feature Name Extensions (FNE)

```
change off-pbx-telephone feature-name-extensions set 5              Page 1 of 2
EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
Set Name: Set Number 5


Active Appearance Select: 55227
Automatic Call Back: 55220
Automatic Call-Back Cancel: 55221
Call Forward All: 55320
Call Forward Busy/No Answer: 55360
Call Forward Cancel: 55321
Call Park: 55270
Call Park Answer Back: 55271
Call Pick-Up: 55278
Calling Number Block: 55263
Calling Number Unblock: 55264
Conditional Call Extend Enable: 55233
Conditional Call Extend Disable: 55234
Conference Complete: 55222
Conference on Answer: 55262
Directed Call Pick-Up: 55327
Drop Last Added Party: 55357
```

Figure 226: Off-Pbx-Telephone Feature Feature Name Extensions (FNE)

```
change off-pbx-telephone feature-name-extensions set 5              Page 2 of 2
EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME


Exclusion (Toggle On/Off): 55392
Extended Group Call Pickup: 55347
Held Appearance Select: 55427
Idle Appearance Select: 55527
Last Number Dialed: 55563
Malicious Call Trace: 55628
Malicious Call Trace Cancel: 55629
Off-Pbx Call Enable: 55670
Off-Pbx Call Disable: 55671
Priority Call: 55072
Recall: 55770
Send All Calls: 55720
Send All Calls Cancel: 55721
Transfer Complete: 55820
Transfer On Hang-Up: 55864
Transfer to Voice Mail: 55888
Whisper Page Activation: 55972
```

2. From your dial plan, enter the FNE numbers in the **Extension** field next to each feature.
3. Click **Enter** to save your changes.
4. Provide the FNEs to the user.

Note:
Administer up to 10 FNE sets on S8400 servers. Administer up to 99 FNE sets on S8500 and S8700 servers.

Note:
A pocket-sized FNE reference card is located on the last page of the *Avaya Extension to Cellular User's Guide,* 210-100-700.

A user can now access any of these Communication Manager features from their cell phone by dialing an FNE.

Creating a Self Administration Feature access code

To create a Self Administration Feature (SAFE) access code, you must complete the following procedures:

- Administer the office extension
- Administer the Feature Access Code

Note:
The SAFE feature only works with EC500, PBFMC, SPFMC, and CSP. SAFE applies to any EC500, PBFMC, SPFMC, or CSP phone number administered. A system administrator must enter all other mapped phone numbers.

Administer the office extension

You must also set up the office telephone extension to accept an Extension to Cellular telephone number before the user can self administer their cell phone number using SAFE.

To prepare an extension for a user to administer their cell phone number using SAFE:

1. Type **`add off-pbx-telephone station-mapping`**. Click **Enter**.

   The system displays the Stations with Off-PBX Telephone Integration screen (Figure 221: Stations with Off-PBX Telephone Integration screen, page 2 on page 965).
2. For the office telephone extension, leave the **Phone Number** field blank.
3. Click **Enter** to save your changes.

   This procedure maps an office telephone extension to a blank cell phone.

4. Provide the SAFE access code to the user. The user calls the SAFE access code and enters their cell phone number.

   The cell phone number is now mapped to the office telephone. With SAFE, the user can also change their cell phone number.

   Immediately after the user enters a phone number, the system verifies that the phone number can be routed.

   - If the phone number is routable, the user hears confirmation tone.
   - If the phone number is not routable, the user hears intercept tone. The connection is not made.

Administer the Feature Access Code

To administer the SAFE access code:

1. Type **`change feature-access-codes`**. Click **Enter**.

   The system displays the **Features Access Code (FAC)** screen.

2. Page down to advance to the page containing the **EC500 Self Administration Access Codes** fields (Figure 227: Feature Access Code (FAC) screen, SAFE, page 2 on page 971).

Figure 227: Feature Access Code (FAC) screen, SAFE, page 2

```
change feature-access-codes                                    Page 2 of   x
                              FEATURE ACCESS CODE (FAC)
                    Contact Closure Pulse Code: *35

                 Data Origination Access Code:
                     Data Privacy Access Code:
              Directed Call Pickup Access Code:
    Emergency Access to Attendant Access Code: *11
       EC500 Self Administration Access Codes: *03   *04   *05   *06
                    Enhanced EC500 Activation: *81     Deactivation:#81
         Enterprise Mobility User Activation:          Deactivation:
 Extended Call Fwd Activate Busy D/A: *23 All: *24     Deactivation:#23
       Extended Group Call Pickup Access Code:
              Facility Test Calls Access Code:
                           Flash Access Code: *88
            Group Control Restrict Activation: *15     Deactivation: #15
                   Hunt Group Busy Activation: *81     Deactivation: #81
                            ISDN Access Code:
               Last Number Dialed Access Code: *54
    Leave Word Calling Message Retrieval Lock: *48
  Leave Word Calling Message Retrieval Unlock: #45
            Leave Word Calling Send A Message: *60
          Leave Word Calling Cancel A Message: #60
             Malicious Call Trace Activation:          Deactivation:
        Meet-me Conference Access Code Change:
```

3. In the **EC500 Self Administration Access Codes** field, type the access code according to your dial plan.

   You can administer up to four SAFE FACs for up to four applications, including EC500, PBFMC, CSP, and SPFMC supported on your system. The order of the SAFE FACs administered in this field applies to the order of the SAFE supported applications as they appear on the station mapping form. In the example above, the *03 SAFE FAC applies to the first SAFE supported application administered on the station mapping form.

4. Click **Enter** to save your changes.

The Extension to Cellular user can administer only one Extension to Cellular telephone number using SAFE. An administrator must map all other telephone numbers to the office telephone.

For more information about the **Feature Access Code** screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Creating FACs to enable/disable Extension to Cellular

To administer FACs to enable or disable Extension to Cellular:

1. Type **`change feature-access-codes`**. Click **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Page down to advance to the page containing the **Enhanced EC500 Activation** field (Figure 227: Feature Access Code (FAC) screen, SAFE, page 2 on page 971).

3. Type access codes according to your dial plan for the following fields.
   - **Enhanced EC500 Activation** field, used for remote activation of Extension to Cellular.
   - **Enhanced EC500 Deactivation** field, used for remote deactivation of Extension to Cellular.

4. Click **Enter to save your changes**.

Note:
Users also have the option to activate and deactivate Extension to Cellular through a feature button on their office telephone. However, that feature button must be administered.

Creating a Station Security Code FAC

To create a system-wide Station Security Code FAC, you must complete the following procedures:

- Creating a system-wide SSC change FAC
- Defining the Station Security Code length

Creating a system-wide SSC change FAC

To create a system-wide SSC change Feature Access Code:

1. Type **change feature-access-codes**. Click **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Page down until the page displays the **Station Security Code Change Access Code** field (Figure 228: Feature Access Code (FAC) screen, Station Security Code Change page 3 on page 973).

Figure 228: Feature Access Code (FAC) screen, Station Security Code Change page 3

```
change feature-access-codes                                    Page   3 of x
                            FEATURE ACCESS CODE (FAC)

 PASTE (Display PBX data on Phone) Access Code: 410
  Personal Station Access (PSA) Associate Code:         Dissociate Code:
        Per Call CPN Blocking Code Access Code:
     Per Call CPN Unblocking Code Access Code:

                 Priority Calling Access Code: 0142
                          Program Access Code: 0143

       Refresh Terminal Parameters Access Code: 0144
              Remote Send All Calls Activation:        Deactivation:
               Self Station Display Activation: #1
                    Send All Calls Activation: *4     Deactivation: *5
         Station Firmware Download Access Code:
                      Station Lock Activation:        Deactivation:
     Station Security Code Change Access Code: #5
              Station User Admin of FBI Assign:                  Remove:
  Station User Button Ring Control Access Code:
             Terminal Dial-Up Test Access Code: 0151
```

3. Type a code valid for your dial plan in the **Station Security Code Change Access Code** field.

   This number is the FAC for this feature.

4. Click **Enter to save your changes**.

Defining the Station Security Code length

To define the minimum Station Security Code length:

1. Type **change system-parameters security**. Click **Enter**.

   The system displays the Security-Related System Parameters screen.

2. Page down until the **Minimum Station Security Code Length** field appears (Figure 229: Security-Related System Parameters screen on page 974).

Figure 229: Security-Related System Parameters screen

```
change system-parameters security                              Page   2 of   2
                      SECURITY-RELATED SYSTEM PARAMETERS

 SECURITY VIOLATION NOTIFICATION PARAMETERS

   SVN Station Security Code Violation Notification Enabled? n




 STATION SECURITY CODE VERIFICATION PARAMETERS

                            Minimum Station Security Code Length: 4
 Station Security Code for Terminal Self-Administration Required? y
```

3. Based on your dial plan, type a number in the **Minimum Station Security Code Length** field.

   This number determines the minimum required length of the SSC. Longer codes are more secure

4. Click **Enter to save your changes**.

   Users can now change their SSC only to a number with the specified number of digits.

For more information about security, see *Administering Avaya Aura™ Communication Manager, 03-300509*.

Administering an enable/disable feature button

To administer a feature button to enable or disable Extension to Cellular, you must complete the following procedures:

- Changing the EC500 state on the station form
- Administering the feature button
- Setting the optional timer

Note:
Feature buttons are only available on desk set telephone types that support administrable feature buttons.

Changing the EC500 state on the station form

EC500 state can be changed using page 2 of the Station administration screen.

To set up an Extension to Cellular feature button:

1. Type change station n where n is the extension of an Extension to Cellular station, 1034 in this example. Click **Enter**.

   The system displays the Station screen. See Figure 230.

2. Go to page 2. Set the EC500 State as **enabled** or **disabled**.

Figure 230: Station screen

```
change station 58105                                          Page 2 of 4
STATION
FEATURE OPTIONS
          LWC Reception: spe                Auto Select Any Idle Appearance? n
         LWC Activation? y                          Coverage Msg Retrieval? y
 LWC Log External Calls? n                                  Auto Answer: none
            CDR Privacy? n                             Data Restriction? n
  Redirect Notification? y                       Idle Appearance Preference? n
Per Button Ring Control? n                     Bridged Idle Line Preference? n
  Bridged Call Alerting? n                         Restrict Last Appearance? y
 Active Station Ringing: single

       H.320 Conversion? n            Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed                          EC500 State: enabled
        Multimedia Mode: enhanced
                                                Display Client Redirection? n
             AUDIX Name:                       Select Last Used Appearance? n
                                                Coverage After Forwarding? s

                                             Direct IP-IP Audio Connections? y
Emergency Location Ext: 58105     Always Use? n        IP Audio Hairpinning? y
```

Administering the feature button

To set up an Extension to Cellular feature button:

1. Type **change station *n*** where ***n*** is the extension of an Extension to Cellular enabled station, ***1034*** in this example. Click **Enter**.

   The system displays the Station screen.

2. Page down until the **Button Assignments** field displays (Figure 231: Station screen on page 976).

Figure 231: Station screen

```
change station 1034                                          Page   4 of   4
                                    STATION
 SITE DATA
      Room:                                            Headset? n
      Jack:                                            Speaker? n
     Cable:                                           Mounting: d
     Floor:                                       Cord Length: 0
  Building:                                         Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                            5:extnd-call
 2: call-appr                            6:
 3: call-appr                            7:
 4: ec500    Timer? y                    8:
```

3. Select an available feature button under the **Button Assignments** header. Button **4** is used in this example. Type **ec500** to administer an Extension to Cellular feature button on the office telephone.
4. Click **Enter to save your changes**.

   The user of station 1034 can now use that feature button to enable and disable Extension to Cellular.

Note:
The **Timer?** subfield is displayed next to the ec500 **Button Assignment**, and defaults to **n**. Leaving the default setting of **n** excludes the timer state.

Setting the optional timer

Users can also use a timer to temporarily disable Extension to Cellular.

To set the optional timer:

1. In the **Station** screen (Figure 231: Station screen on page 976), locate the **Timer** subfield next to the ec500 **Button Assignment**.
2. Set the **Timer?** subfield to **y** to enable an Extension to Cellular timer state for the administered feature button.

3. Click **Enter to save your changes**.

   The corresponding feature button on the office telephone is now administered for Extension to Cellular. The user can activate a one-hour timer to temporarily disable Extension to Cellular through this administered feature button.

Administering a feature button to extend a call

To set up an Extend Calls feature button:

1. Type **`change station n`** where ***`n`*** is the extension of an Extension to Cellular-enabled station, ***`1034`*** in this example. Click **Enter**.

   The system displays the Station screen.

2. Page down until you see the **Button Assignments** field (Figure 231: Station screen on page 976).
3. Select an available feature button under the **Button Assignments** field. Button **5** is used in this example. Type **extnd-call** (all lowercase).
4. Click **Enter to save your changes**.

   The corresponding feature button on the office telephone is now administered to extend calls between the office telephone and the Extension to Cellular cell phone.

Reviewing feature button assignments

To review the feature assignments for the office telephone feature buttons:

1. Type **`change display-messages view-buttons`**. Click **Enter**.

   The system displays the Language Translations screen (Figure 232: Language Translations screen on page 978).

Figure 232: Language Translations screen

```
change display-messages view-buttons                          Page x of x
                              LANGUAGE TRANSLATIONS

English                                  Translation

 1. Station Lock                          1. ************************
 2. License Error                         2. ************************
 3. Conference Display                    3. ************************
 4. Conf/Trans Toggle-Swap                4. ************************
 5. Far End Mute                          5. ************************
 6. Paging 1st Link Alarm                 6. ************************
 7. Paging 2nd Link Alarm                 7. ************************
 8. EC500                                 8. ************************
 9. No Hold Conference                    9. ************************
10. Posted Messages                      10. ************************
11. Audix Recording                      11. ************************
12. Extend Call                          12. ************************
```

2. Page down to view subsequent screens.

   If you assigned feature buttons to enable/disable Extension to Cellular and to extend a call between the office and cell phone, you can see **EC500** and **Extend Call** in the feature button list.

Note:
The **EC500** button refers to the Extension to Cellular enable/disable feature button.

3. Click **Enter** to save your changes.

To view the button labels for the feature buttons:

1. Type **`change display-messages button-labels`**. Click **Enter**.

   The system displays the Language Translations screen (Figure 233: Language Translations screen on page 979).

Figure 233: Language Translations screen

```
change display-messages button-labels                          Page x of x
                              LANGUAGE TRANSLATIONS

English                                  Translation

 1. Directory                              1. ************
 2. Dir Pickup                             2. ************
 3. Disp Charges                           3. ************
 4. DoNotDisturb                           4. ************
 5. EC500                                  5. ************
 6. Exclusion                              6. ************
 7. ExtDoNotDstrb                          7. ************
 8. Extend Call                            8. ************
 9. Far End Mute                           9. ************
10. Flash                                 10 . ************
11. FTC Alarm                             11. ************
12. Goto Cover                            12. ************
13. GrpPg                                 13. *****
14. GrpDoNotDstrb                         14. ************
15. Hunt NS                               15. **********
16. InCaalID                              16. ********
```

2. Page down to view all screens. If administered, you see the **EC500** and **Extend Call** labels.
3. Click **Enter** to save your changes.

Sending 10-digit caller identification for locally originated calls

The following procedure is for cell phone use only.

To administer 10-digit caller identification for stations associated with either ISDN or IP trunks:

1. Type **`change public-unknown-numbering`**. Click **Enter**.

   The system displays the Numbering – Public/Unknown Format screen (Figure 234: Numbering – Public/Unknown Format screen on page 980).

Figure 234: Numbering – Public/Unknown Format screen

```
change public-unknown-numbering 5                                Page 1 of 2
                          NUMBERING - PUBLIC/UNKNOWN FORMAT
                                     Total                                Total
Ext Ext    Trk       CPN             CPN   Ext Ext    Trk       CPN        CPN
Len Code   Grp(s)    Prefix          Len   Len Code   Grp(s)    Prefix     Len

 4  1                73285            10
```

2. **Under the Ext Len** field, type an extension length between 0 and 7.
3. **Under the Ext Code** field, type the starting digit(s) of the extension, such as the country code.
4. **Leave the Trk Grp(s)** field blank to apply to all trunks in the system.
5. Under the **CPN Len** field, type 10 to indicate a 10-digit calling number.
6. Click **Enter to save your changes**.

   This administration adds a prefix to extensions to create a 10-digit calling number for locally sourced calls.

Administering Confirmed Answer for Cellular Voice Mail Avoidance

To administer Confirmed Answer so that unanswered Extension to Cellular calls do not cover to cellular voice mail:

1. Type **change off-pbx-telephone configuration-set *n***, where ***n*** is the number assigned to the **Configuration Set** field of the user's off-pbx-telephone station-mapping screen. Press Enter. The system displays the Configuration Set screen.
2. In the **Confirmed Answer** field, type **y**.
   The system displays the **Timeout** field with a default value of 10. The values are 5 to 20 (seconds).
3. Press Enter to save your changes and exit the system.

Administering call filtering

To administer call filtering:

1. Type **add off-pbx-telephone station-mapping**. Click **Enter**.

   The system displays the Stations with Off-PBX Telephone Integration screen.

2. Proceed to page 2 of the Stations with Off-PBX Telephone Integration screen (Figure 221: Stations with Off-PBX Telephone Integration screen, page 2 on page 965).

   The information you entered in the **Station Extension** field on the first page appears as read only information on this second page.

3. Enter the acceptable type of call under the **Calls Allowed** field for each **Station Extension**.

   Calls allowed can be internal, external, all, or none.

4. Click **Enter** to save your changes.

For more information on the **Calls Allowed** field, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Administering voice mail coverage

To administer Extension to Cellular voice mail coverage, you can complete the following procedures:

- Setting up a Cellular Voice Mail Avoidance timer
- Using timing to route calls to voice mail

Setting up a Cellular Voice Mail Avoidance timer

To administer Cellular Voice Mail Avoidance to send unanswered calls to the corporate voice mail after a predetermined number of seconds:

1. Type **`change off-pbx-telephone configuration-set n`**, where ***n*** is the number assigned with a coverage path. Click **Enter**.

   The system displays the Configuration Set screen (Figure 235: Configuration set screen on page 982).

Figure 235: Configuration set screen

```
change off-pbx-telephone configuration-set 2                    Page 1 of  1

CONFIGURATION SET: 2

            Configuration Set Description:
                      Calling Number Style: network
      CDR for Calls to EC500 Destination? y
                       CDR for Origination: phone-number
              Fast Connect on Origination? n
             Post Connect Dialing Options: dtmf
            Cellular Voice Mail Detection: Timed (seconds): 8s
                            Barge-in Tone: y
              Calling Number Verification: y
 Call Appearance Selection for Origination: primary-first
                          Confirmed Answer: y Timeout (seconds): 10s

             Use Shared Voice Connections? n
```

2. In the **Cellular Voice Mail Detection** field, type **timed**.

   The system displays the **(seconds)** field, with the default value of **4**. The values are **1** to **9**.

   Note:
   The default value for this field changed from **none** to **timed** starting in Communication Manager Release 5.0. However, if the system is upgraded from older releases, the default setting will remain as **none**.

3. If you want to increase the time before the cell phone routes to coverage, change the **(seconds)** field. For example, set the timer to **5** seconds.
4. Click **Enter to save your changes**.

   In this example, a call to an Extension to Cellular enabled cell phone will be pulled back, if it is answered within 5 seconds. The desk set will continue to ring.

For more information about the **Configuration Set** screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Using timing to route calls to voice mail

To change the number of unanswered rings on the office telephone number before coverage:

1. Type **`change coverage path n`** where ***n*** is the number assigned with a coverage path. Click **Enter**.

   The system displays the Coverage Path screen (Figure 236: Coverage Path screen on page 983).

Figure 236: Coverage Path screen

```
change coverage path 1                                          Page   1 of   1
                                COVERAGE PATH

                  Coverage Path Number: 1
                                                  Hunt after Coverage? n
                      Next Path Number:           Linkage

COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
              Active?             n               n
                Busy?             y               y
       Don't Answer?              y               y         Number of Rings: 2
                 All?             n               n
 DND/SAC/Goto Cover?              y               y

COVERAGE POINTS

    Terminate to Coverage Pts. with Bridged Appearances? n

  Point1: 694000    Rng:    Point2: h99       Rng:    Point3:
  Point4:                   Point5:                   Point6:
```

2. Change the value in the **Number of Rings** field as appropriate. The number of rings must be less than the number of unanswered rings before the cellular service provider voice mail covers a call.
3. Click **Enter to save your changes**.
4. Remind users that they must disable Extension to Cellular before turning off their cell phone. This action prevents messages from automatically going to cellular voice mail and ensures that corporate voice mail covers all business calls.
5. Remind users with business-only cell phones that they can ask their cellular provider to turn off cellular voice mail.

Setting up Call Detail Recording

To enable Call Detail Recording (CDR) for calls to a cell phone, you must complete the following procedures:

- Enable CDR for the outgoing trunk
- Enable CDR for Extension to Cellular
- Generating two CDR records

Enable CDR for the outgoing trunk

To enable CDR for the outgoing trunk:

1. Type **add trunk-group *n***, where ***n*** is a new trunk group number. Click **Enter**.

   The system displays the **Trunk Group** screen (Figure 237: Trunk Group screen on page 984).

Figure 237: Trunk Group screen

```
add trunk-group n                                          Page   1 of  x
                              TRUNK GROUP

Group Number: 3                    Group Type: isdn          CDR Reports: y
  Group Name: OUTSIDE CALL               COR: 1        TN: 1        TAC: 103
   Direction: two-way        Outgoing Display? n                 PRI/BRI:
 Dial Access? n                Busy Threshold: 255         Night Service:
Queue Length: 0           Country: 1                Incoming Destination:
   Comm Type: voice                Auth Code? n   Digit Absorption List:
    Prefix-1? y                  Trunk Flash? n         Toll Restricted? y

TRUNK PARAMETERS
            Trunk Type:
    Outgoing Dial Type: tone                             Cut-Through? n
     Trunk Termination: rc                    Disconnect Timing(msec): 500

            Auto Guard? n    Call Still Held? n     Sig Bit Inversion: none
     Analog Loss Group: 6                          Digital Loss Group: 11
                                  Trunk Gain: high

 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 10            Receive Answer Supervision? n
```

2. Type **y** in the **CDR Reports** field to enable CDR.
   - Type **y** to track calls to cell phones for reporting or charging purposes.

     If you type **y**, the configuration set administered on the Station screen determines whether a CDR record is generated.
   - Type **n** if you want to treat the Extension to Cellular cell phones as totally internal stations and do not require CDR reporting.
3. Click **Enter** to save your changes.

Enable CDR for Extension to Cellular

To enable CDR for an Extension to Cellular cell phone:

1. Type **change off-pbx-telephone configuration-set *n*** where ***n*** is the number assigned with a coverage path. Click **Enter**.

   The system displays the **Configuration Set** screen (Figure 238: Configuration Set screen on page 985).

Figure 238: Configuration Set screen

```
change off-pbx-telephone configuration-set 2                    Page 1 of  1

CONFIGURATION SET: 2

      Configuration Set Description:
                Calling Number Style: network
 CDR for Calls to EC500 Destination? y
                 CDR for Origination: phone-number
        Fast Connect on Origination? n
       Post Connect Dialing Options: dtmf
      Cellular Voice Mail Detection: Timed (seconds): 8s
                     Barge-in Tone: y
        Calling Number Verification: y
             Identity When Bridging: principal
                   Confirmed Answer: y Timeout (seconds): 10s
```

2. In the **CDR for Calls to EC500 Destination** field, type **y** to enable CDR.
3. Click **Enter** to save your changes.

   When this field is set to **y**, an outgoing trunk CDR report is created for each Extension to Cellular call.

Generating two CDR records

To generate two CDR records:

1. Type **change system-parameters cdr**. Click **Enter**.

   The system displays the CDR System Parameters screen.
2. Set the **Intra-Switch CDR** field to **y**.
3. Click **Enter** to save your changes.
4. Log off and log back into the switch.

5. Type **change intra-switch-cdr**. Click **Enter**.

   The system displays the Intra-Switch CDR screen.

6. Type any extension you want to track with this screen.
7. Click **Enter** to save your changes.

Note:
There is no intra-switch-cdr record when using originating CDR.

Changing configuration sets

To customize a configuration set:

1. Type **change off-pbx-telephone configuration-set *n*** where ***n*** is the number assigned to a configuration set. Click **Enter**.

   The system displays the Configuration Set screen (Figure 239: Configuration Set screen on page 986).

Figure 239: Configuration Set screen

```
change off-pbx-telephone configuration-set 2                    Page 1 of  x

CONFIGURATION SET: 2

            Configuration Set Description:
                      Calling Number Style: network
       CDR for Calls to EC500 Destination? y
                       CDR for Origination: phone-number
              Fast Connect on Origination? n
             Post Connect Dialing Options: dtmf
            Cellular Voice Mail Detection: Timed (seconds): 8s
                          Barge-in Tone: y
              Calling Number Verification: y
Call Appearance Selection for Origination: primary-first
                         Confirmed Answer: y Timeout (seconds): 10s


Use Shared Voice Connections? n
```

2. In the **Configuration Set Description** field, type in a description of the configuration set, up to 20 characters.

3. Type in the **Calling Number Style as either network or pbx.**

   The Calling Number Style field determines the caller ID format for calls from a local switch extension to an Extension to Cellular cell phone.

4. Type an entry in the **CDR for Origination** field to determine the source of an incoming CDR.

   The CDR report either provides the calling number that came in over the trunk, the station extension, or none. If the **extension** option is chosen, the internal Extended Access extension is reported as the calling party. If the **phone number** option is chosen, the 10-digit cell phone is reported on the CDR report. If you use the **none** option**,** there will be no originating CDR record.

5. Enter **y** or **n** for the **Fast Connect on Origination** field to determine whether some additional processing occurs on the switch before connecting a call. This option can be used in the future for capabilities provided by the cell phone provider. Currently Avaya recommends the default value of **n**.

6. Verify that the default **dtmf** is the entry for the **Post Connect Dialing Options** field. The **Post Connect Dialing Options** field determines whether additional capabilities are available for incoming ISDN trunk calls that are mapped into Extension to Cellular stations. These capabilities are beyond standard ISDN dialing.

7. Verify that the **Calling Number Verification** field is set to the default value **y**.

   Important:
   The default value **y** restricts incoming calls to “network provided” or “user provided verified and passed” calling numbers. When the switch is part of a private network and you are not screening calling numbers, change the field to **n**.

8. In the **Confirmed Answer** field, enter **y** or **n**. If **y**, set the timeout period for waiting for user input of a digit. When set to **y**, a digit must be received within the timeout period, or the call is not treated as answered. The default timeout period is 10 seconds.

9. In the **Call Appearance Selection for Origination** field, enter **primary-first** if you want to select regular call appearance first for origination or enter **first-available** if you don’t care whether a regular or bridged appearance is selected for origination.

10. In the **Use Shared Voice Connections** field, enter **y** if you want to share a single trunk for a cell phone call and a PBX call. You can use shared voice connection option only with the FMC applications such as PBFMC, PVFMC, and SPFMC.

11. Click **Enter to save your changes**.

12. Use the **`change off-pbx-telephone configuration-set n`** command as needed to change additional configuration sets.

Administering the barge-in tone

Note:
Before the barge-in tone can be used, a **Intrusion** tone must be set up on the Tone Generation Customized Tones screen. To verify that a **Conference** tone is set up, type **`change tone-generation n`**, where ***n*** is a number between **1** and **25**.

Important:
The barge-in tone is a type of intrusion tone. You may have to set up an intrusion tone if the default is silence. If default intrusion tone is not set to silence (as in the United States), you do not have to administer it, but you can change the characteristics of the tone.

To administer the barge-in tone for security purposes:

1. Type **`change off-pbx-telephone configuration-set n`** where ***n*** is the number assigned with a coverage path. Click **Enter**.

   The system displays the **Configuration Set** screen (Figure 240: Configuration Set screen on page 988).

Figure 240: Configuration Set screen

```
change off-pbx-telephone configuration-set 2                    Page 1 of  x

CONFIGURATION SET: 2

             Configuration Set Description:
                      Calling Number Style: network
       CDR for Calls to EC500 Destination? y
                       CDR for Origination: phone-number
              Fast Connect on Origination? n
             Post Connect Dialing Options: dtmf
            Cellular Voice Mail Detection: Timed (seconds): 8s
                            Barge-in Tone: y
              Calling Number Verification: y
Call Appearance Selection for Origination: primary-first
                         Confirmed Answer: y Timeout (seconds): 10

             Use Shared Voice Connections? n
```

2. In the **Barge-in Tone** field, select **y** to enable or **n** to disable.

3. Click **Enter** to save your changes.

   When the barge-in tone is enabled, all parties on a call hear a conference tone if all of the following conditions are true:

   - The conference tone is administered in the country form
   - Extension to Cellular is enabled
   - The exclusion feature is not enabled
   - A user is on the conference call on their cell phone
   - Another user tries to join this call on the Extension to Cellular-associated office telephone

Displaying System Capacity

To display the system capacity for the Extension to Cellular features:

1. Type **`display capacity`**.

   The system displays the System Capacity screen.

Figure 241: System Capacity screen

```
display capacity                                          Page   9 of  x
                              SYSTEM CAPACITY

                 TOTAL SUBSCRIBED PORTS
                                                                   System
                                                Used Available     Limit
                                               ----------------------
                          Station and Trunk Ports:  212    2588      2800
                                     SBS Stations:    0       0         0
                                Radio Controllers:    0       0         0
                               Wireless Terminals:    0       0         0
                                 XMOBILE Stations:    4     196       200
                                           EC500:     0
                                            DECT:     4
                                             PHS:     0
                        Off-PBX Telephone - EC500:    20      40        60
                          Off-PBX Telephone - OPS:    20      40        60
                        Off-PBX Telephone - PBFMC:    20      40        60
                        Off-PBX Telephone - PVFMC:    20      40        60
                        Off-PBX Telephone - SCCAN:    20      40        60
```

2. Page down to the **Off-PBX Telephone - PBFMC**, **Off-PBX Telephone - PVFMC** fields.

3. View the capacities and press **Next**.

   System displays OFF-PBX-TELEPHONE MEMORY CAPACITY screen.

Figure 242: Memory Capacity screen

```
display capacity                                          Page  10 of  x
                      OFF-PBX TELEPHONE MEMORY CAPACITY



                                Application Memory     Mapping Memory

          System Limit (units):     1039500                72000

 Administered Applications (%):           4                    4
  Enterprise Mobility User (%):           0                    0
  Acquired Shared Mappings (%):           0                    0
     one-X server Mappings (%):           0                    0
```

4. View the memory capacities and press **Cancel** to exit the screen.

Administering Conditional Call Extending

To administer conditional call extending:

1. Type **`change off-pbx-telephone station-mapping`**. Click **Enter**.

   The system displays the Stations with Off-PBX Telephone Integration screen.
2. Fill in the information in all fields for each Station Extension.
3. Proceed to page 3 of the Stations with Off-PBX Telephone Integration screen. The information that you entered in the **Station Extension** and **Application** fields on the first page appear as read only information on this third page.

Figure 243: Off-pbx-telephone station-mapping page 3

```
change off-pbx-telephone station-mapping 58101                    Page 3 of x
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station     Appl  Share    Calls Accepted
Extension   Name   Level    S C H I P R-COR
58101       EC500    5
58101       PBFMC    5      y y y y y y 1
58101       PVFMC    _      y y y y y n ___
58101       SPFMC    5      y y y y y y 100
```

4. Type **y** in the desired call type in the **Calls Accepted** field. Type **n** in the call type that you want to restrict. The call types that you can allow or restrict are:

S	Standard calls to the station
C	Calls covered or forwarded to the station
H	Calls to the station through a hunt group
I	Intercom calls to the station
P	Priority calls to the station
R	Calls restricted by a COR permission matrix

5. Type the class of restriction number in the **COR** field.
6. Click **Enter** to save your changes.

Administering Sharing Mapping among CM PBXs

With Sharing Mapping among CM PBXs feature, you can share the station name and station mapping information among multiple Communication Managers. A CM acquires mapping information from the other CM by using a SIP subscription. Communication Managers subscribe for the shared mapping on the Off-Pbx-Telephone Mapping-Subscriptions form. SIP trunks or Subscription Aggregator is used to interconnect the Communication Managers to share mapping information. So Each CM can make 3 subscriptions.

To administer Sharing Mapping among Communication Managers:

1. Type **`change off-pbx-telephone mapping-subcriptins`**. Click **Enter**.

   The system displays the Off-PBX Telephone Mapping Subscriptions screen.

Figure 244: Off-pbx-telephone station-mapping page 1

```
change off-pbx-telephone mapping-subscriptions                    Page 1 of x

MAPPING SUBSCRIPTIONS
      Signaling      Far-end Domain                                    Level
      Group
    1 10       lab1n360.avaya.com                                      5
    2 12       usae.avaya.com                                          5
    3 15       133.9.66.88                                             5
Enter Sip Signaling Group specifying Far-end Domain of PBX or Subscription
aggregator (IP address or URI) that will share off-pbx telephone mappings.


When mappings are acquired from a subscription, the level within the acquired
mapping is compared to the level on this form. If the level in mapping is less
than the one on this form, the mapping is discarded.


Maximum Percentage of Mapping Storage Allowed for Acquired Mappings: 30
```

2. Fill in the **Signaling Group** for a **Far-end Domain** of PBX or Subscription aggregator.
3. Specify the Subscription Level for that PBX or Subscription aggregator. This Level is compared to the **Subscription Level** of the acquired mapping administered on page 3 of the off-pbx-telephone station-mappings (see Figure 245). If the **Share Level** is less than the **Level** on this form, the mapping is discarded.
4. Specify the **Maximum Percentage of Mapping Storage that is allowed for the Acquired Mappings**. Mapping storage is shared between Administered Mappings, Enterprise Mobility Users, Acquired Mappings, and ONE-X mappings.

Figure 245: Off-pbx-telephone station-mapping page 3

```
change off-pbx-telephone station-mapping 58101                    Page 3 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION
Station             Appl   Share     Calls Accepted
Extension            Name  Level      S C H I P R-COR
58101               EC500    5
58101               PBFMC    5        y y y y y y 1
58101               PVFMC    _        y y y y y n ___
58102               SPFMC    5        y y y y y y 100
```

5. The information that you entered in the **Station Extension** and **Application** fields on the first page appear as read-only information on this third page.
6. Acquired mappings may be listed using the **`list mappings-acquired`** command.

Figure 246: mappings-acquired page 1

```
list mappings-acquired                                                Page   1

                    MAPPINGS ACQUIRED FROM OTHER PBXS

HOME PBX        Country                     Home PBX                  Signaling
User Extension   Code    Phone Number       User Name                   Group

591-0001          91     9765999888         Shah, Sandeep                 6
591-0001                 30412847           Shah, Sandeep                 6
591-0002                 30412697           Mohan, Anup                   6
591-0002          91     9512365478         Mohan, Anup                   6
591-0003          91     9865987777         Mishra, Prashant              6
591-0003                 30412556           Mishra, Prashant              6
591-0004          91     9111121212         Sonawane, Dinesh              6
591-0004                 30412553           Sonawane, Dinesh              6
591-0006          91     9111910006         Sarode, Suhas                 6
591-0007          91     9764986569         Kesineni, Janardhanarao       6
591-0008          91     9632587412         Paithankar, Anand             6
591-0009          1      7326549876         Milton, Steve                 6
591-0009          1      7328522112         Milton, Steve                 6
591-0010          1      7328523362         Zawadzki, John                6
```

Administration for one-X Mobile Server and Application Support

You can use Class of Restriction (COR) to control the stations that have one-X Server support.

1. Enter command **change cor *n***, then go to page 3 of the forms.

Figure 247: COR screen, page 3

```
change cor 1                                                    Page 3 of 23
CLASS OF RESTRICTION

           SAC/CF Override by     Team Btn? n    Priority Call? n    Dialing? n
SAC/CF Override Protection for    Team Btn? n    Priority Call? n    Dialing? n


                       one-X Server Access? y
Team Btn Silent if Active? n  Priority Ring? n
Team Btn Display Name? n      Pick Up by Going Off Hook? n
```

2. Set the **one-X Server Access** to **y** to allow one-X control.

3. You can list the stations currently under one-X control using the **`list off-pbx-telephone station-mappings`** command.

Figure 248: List off-pbx-telephone station-mappings page 1

```
list off-pbx-telephone station-mapping                                  Page   1

                    STATION TO OFF-PBX TELEPHONE MAPPING

Station         Appl   CC  Phone Number     Config Trunk   Mapping      Calls
Extension                                   Set    Select  Mode         Allowed

591-0001        EC500  91  9765999888       1  /   aar     both         all
591-0001        OPS        5910001          1  /   aar     both         all
591-0001        PVFMC      59101            1  /   aar     both         all
591-0001        PBFMC      30412847         1  /   ars     both         all
591-0002        EC500      30412697         1  /   ars     both         all
591-0002        OPS        5910002          1  /   aar     both         all
591-0002        SPFMC  91  9512365478       1  /   ars     both         all
591-0003        EC500  91  9865987777       1  /   ars     both         all
591-0003        SPFMC      30412556         1  /   ars     both         all
591-0004        EC500  91  9111121212       1  /   ars     both         all
591-0004        SPFMC      30412553         1  /   ars     both         all
591-0006        PBFMC  91  9111910006       1  /   ars     both         all
591-0006        PVFMC      59106            1  /   aar     both         all
591-0007        PBFMC  91  9764986569       1  /   ars     both         all
```

4. You can see the one-X status of the stations that are controlled using **`status station`** command. Field **one-X Status** values are: **blank**, **“normal”**, **“no-ring”**, **“trigger”**, **“coverage”**, **“voicemail”**, or **“N/A”**. If the value is **“normal”**, then the station’s behavior is unaffected by the one-X Server. When the value is **“no-ring”**, then the station will not ring under any conditions. If the value is **“triggered”**, the decision to ring the station is controlled by the one-X Server on a call by call basis. If the value is **“coverage”** or **“voicemail”** calls to the station will immediately cover, if possible.

Figure 249: Status station page 1

```
status station 53003                                          Page 1 of 8
GENERAL STATUS
    Administered Type: 4624                 Service State: in-service/on-hook
      Connected Type: 4612 TCP Signal              Status: connected
           Extension: 53003
                Port: S00000           Parameter Download: complete
         Call Parked? no                    SAC Activated? no
     Ring Cut Off Act? no
Active Coverage Option: 1              one-X Server Status: trigger

         EC500 Status: N/A           Off-PBX Service State: in-service/idle
  Message Waiting:
  Connected Ports:


 Limit Incoming Calls? no

     User Cntrl Restr: none                     HOSPITALITY STATUS
   Group Cntrl Restr: none                    Awaken at:
                                               User DND: not activated
                                             Group DND: not activated
                                            Room Status: non-guest room
```

End-user procedures for Extension to Cellular

End-users can activate or deactivate certain system features and capabilities. End-users can also modify or customize some aspects of the administration of certain features and capabilities. For more information on end-user procedures, see the *Avaya Extension to Cellular User's Guide*, 210-100-700.

Considerations for Extension to Cellular

This section provides information about how the Extension to Cellular feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Extension to Cellular under all conditions. The following considerations apply to Extension to Cellular.

Upgrades from prior versions

Extension to Cellular is available only with Communication Manager Release 1.3 or later. The Extension to Cellular releases can be administered and operated concurrently on the same Avaya server running Communication Manager. You can continue to support users with Extension to Cellular releases 1 through 4.1. Or you can upgrade all users to the latest version of Communication Manager Release 5.2.

If you are converting from Extension to Cellular versions 1-4 you must perform the following steps to update to the latest version as part of Communication Manager Release 5.2:

1. Type **`change station`** ***`n`*** command, where ***`n`*** is the station you want to change. Click **Enter**.

   The system displays the Station screen.

2. Set the **XMOBILE Mapping Mode** to **none**.

   All previous mapping of XMOBILE stations, the way Extension to Cellular used to be administered, cannot interfere with Extension to Cellular.

3. Set up the new office telephone to cell phone mapping in Mapping an office telephone to a cell phone on page 964.

4. Test the system.

5. If the system works, remove the XMOBILE station records.

   This last step frees up stations that go toward the maximum number of stations allowed.

Starting with Extension to Cellular 5.0 (Communication Manager Release 2.0) introduced support for the **Off-PBX Telephone Integration and Mobility** (OPTIM). Once XMOBILE Mappings are converted to OPTIM, further upgrades from that release to higher releases are automatic. Only new capabilities need to be administered when upgrading to new releases. Some of those include:

- Support of up to 4 OPTIM applications per station extension – up to 4 phone number mappings can be administered per station extension.
- Self Administration Feature (SAFE) Access Codes so users can enter and change their own cell phone numbers. For more information, see Creating a Self Administration Feature (SAFE) access code. This feature allows for up to 4 SAFE Access Codes per extension, allowing modification of up to four phone numbers per extension.
- Administration of the barge-in tone for added security. For more information, see Administering the barge-in tone.
- Mapping dialed extensions to the new Feature Name Extensions. For more information, see Setting up Feature Name Extensions (FNE) s.
- Support of multiple sets of Feature Name Extensions.
- Fixed Mobile Convergence (FMC) applications support - PBFMC, SPFMC, and PVFMC applications – allows support for dual-mode cellular phones.

See Detailed description of Extension to Cellular on page 937 for a list of all OPTIM capabilities.

Upgrade from Extension to Cellular Version 5

The following administration tasks are new in Extension to Cellular Version 6.

- Set up the Self Administration Feature (SAFE) Access Code so users can enter and change their own cell phone number. For more information, see Creating a Self Administration Feature access code on page 970.
- Administer the barge-in tone for added security. For more information, see Administering the barge-in tone on page 988.
- Map dialed extensions to the new Feature Name Extensions. For more information, see Setting up Feature Name Extensions set on page 968.

Upgrade from Extension to Cellular Version 4

To administer an Extension to Cellular feature button and include the optional Extension to Cellular timer:

1. Type **change station *n*** where ***n*** is the extension of an Extension to Cellular-enabled station. Press **Enter**.

   The system displays the Station screen.

2. Press the **Next Page** button twice to display page 3 of the Station screen (Figure 250: Station screen, page 3 on page 997).

Figure 250: Station screen, page 3

```
change station 1034                                          Page   3 of   4
                                    STATION
 SITE DATA
      Room:                                            Headset? n
      Jack:                                            Speaker? n
     Cable:                                           Mounting: d
     Floor:                                       Cord Length: 0
  Building:                                         Set Color:

ABBREVIATED DIALING
     List1:                     List2:                     List3:

BUTTON ASSIGNMENTS
 1: call-appr                            5:
 2: call-appr                            6:
 3: call-appr                            7:
 4: EC500    Timer? y                    8:
```

3. Select an available feature button under **BUTTON ASSIGNMENTS** and type **EC500**.

4. Press **Enter**.

   The **Timer** subfield appears and defaults to **n**. Leaving the default setting of **n** excludes the timer state.

5. Set the optional **Timer** subfield to **y** to include an Extension to Cellular timer state for the administered feature button.

   When the timer state is included, the Extension to Cellular user can activate a one-hour timer to temporarily disable Extension to Cellular.

6. Press **Enter**.

   The corresponding feature button on the office telephone is now administered for Extension to Cellular, and configured with the optional Extension to Cellular timer.

Note:

The feature status button on the office telephone indicates the current state of Extension to Cellular. The status is displayed regardless of whether the feature was enabled remotely or directly from the office telephone.

Upgrade from Extension to Cellular Version 3

The following process is to change the Extension to Cellular configuration to work without the loopback trunks. Let us eliminate the loopback connections for station 5462.

Eliminating the loopback trunks is optional and must be accompanied by changing the **Mobility Trunk Group** field on the Station screen to **ars**.

1. Eliminate the DS1 or IP loopback trunks associated with Extension to Cellular Version 2.0 or 3.0.

   This step includes removing the loopback trunks and signaling groups through switch administration and physically from the switch.

   Loopback trunk configuration can coexist with the Extension to Cellular R4 if you choose to do so. If you decide to eliminate the loopback trunks, the removed equipment can be reused for other trunk solutions. You can change gradually over to a total loopback elimination. If you decide to have the loopback and non loopback configurations coexist, you must remember there are capacity restrictions when using the DS1.

2. Type **change station 5462**. Press **Enter**.

   The system displays the Station screen for extension 5462 (Figure 251: Station screen, page 1 on page 999).

Figure 251: Station screen, page 1

```
change station 5462                                          Page 1 of 4

                                    STATION
 Extension: 5462                  Lock Messages? n                    BCC: 0
      Type: XMOBILE                     Security: *                     TN: 1
                                  Coverage Path 1:                    COR: 1
      Name: John Doe              Coverage Path 2:                    COS: 1
                                  Hunt-to Station:

 STATION OPTIONS
              XMOBILE Type: EC500                    Message Lamp Ext: 5462
                            Display Module? n     Message Waiting Type: none
       Mobility Trunk Group: ars
          Configuration Set: 1                          Calls Allowed: all

   CELL PHONE NUMBER MAPPING
                 Dial Prefix:
          Cell Phone Number: 732-123-4567
               Mapping Mode: termination
```

3. In the **Mobility Trunk Group** field, type **ars**.

   The field must be changed to **ars** for loopback elimination.

4. Press **Enter to** save your changes.

   Note that If the **Dial Prefix** field contains the ars Feature Access Code, remove the prefix.

For more information, see the *Administering Avaya Aura™ Communication Manager,* 03-300509.

Upgrade from Extension to Cellular Version 2

Implement changes as described for upgrade from Extension to Cellular Version 3.

Starting with Version 3, there is a field on the Station screen called **Mapping Mode**. There is a command, **`list xmobile mapping`**, that makes it easy to find out the XMOBILE extensions and primary extension associated with a cell phone number. The **`status station`** command now explicitly shows the Extension to Cellular state: enabled or disabled.

To implement office caller ID for an existing Extension to Cellular user:

1. Identify the station bridged to the second call appearance of the primary extension.

   The **`list bridged-extensions <primary ext>`** command provides this information.

2. Type **`change station <xmobile ext>`**. Press **Enter**.

   The system displays the Station screen.

3. Change the **Mapping Mode** field to **both**.
4. Press **Enter** to save your changes.

Note:
If the **Cell Phone Number** field contains a dial prefix such as 1 for long distance, re-administer the cell phone number and place the prefix number in the **Dial Prefix** field. Also make sure that the full number, including area code, is in the **Cell Phone Number** field. This number is necessary for office caller ID to function.

For information on installation and administration of Version 2 of Extension to Cellular, see *Avaya EC500 Extension to Cellular Installation and Administration Guide*, Issue 2, July, 2001.

Upgrade from Extension to Cellular Version 1

Starting with Version 2, you can administer cell phone numbers on the Station screen. There are three fields related to administration of the cell phone number:

- **Dial Prefix**
- **Cell Phone Number**
- **Mapping Mode**

For pre-existing stations, you can continue to use ARS digit conversion to convert the extension to a cell number or they can be changed to use the new fields on the Station screen.

To add the cell phone number to a station:

1. Type **`change station <xmobile ext>`**. Press **Enter**.

   The system displays the Station screen.
2. Type each dial prefix, if any in the **Dial Prefix** field. For example, type 1 for long distance, but not 9 for external access.
3. Type the full cell phone number including area code in the **Cell Phone Number** field.
4. Type **termination** in the **Mapping Mode** field.
5. Press **Enter** to save your changes.

Implement changes described for upgrade from Extension to Cellular Version 2.

For information on installation and administration of Version 1 of Extension to Cellular, see *Avaya EC500 Extension to Cellular Installation and Administration Guide*, Issue 1, February 8, 2001.

Interactions for Extension to Cellular

This section provides information about how the Extension to Cellular feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Extension to Cellular in any feature configuration.

Attendant

If the **Calls Allowed** field on the Stations with Off-PBX Telephone Integration screen (see Figure 221: Stations with Off-PBX Telephone Integration screen, page 2 on page 965) is **internal**, attendant-originated and attendant-extended calls are not delivered.

Call coverage

Manipulate the number of unanswered rings on the cell phone If you want to ensure that unanswered calls go to office voice mail instead of the cell phone's voice mail. Set the value in the **Number of Rings** field on the Coverage Path screen for the office telephone to a lower number than the voice mail coverage setting on the corresponding cell phone. For more information, see Administering voice mail coverage on page 981.

Call Detail Recording

A Call Detail Recording (CDR) record is generated for calls that originate from an Extension to Cellular cell phone. For this feature to work, incoming trunk CDR must be turned on. The system does not generate a CDR if the user dials a Feature Name Extension (FNE) that does not result in a call.

Cellular service provider voice mail

Office stations can have standard Avaya server running Communication Manager voice mail coverage such as CM Messaging. But cell phones usually have voice mail coverage from the cellular service provider. There are now two ways to coordinate the two systems.

First, you can administer Communication Manager Extended Access Cellular Voice Mail Avoidance. Use the Cellular Voice Mail Avoidance feature to reduce the uncertainty as to where unanswered Extension to Cellular calls go. An unanswered call ends either at your office telephone voice mail, or at your cell phone voice mail system.

Communication Manager detects when the cell phone is not the entity that answers the call and brings the call back to the server. The call is treated as a normal call on the telephone with Extension to Cellular enabled. The call is then processed with the normal number of rings set on your call coverage.

Second, you can set up the number of unanswered rings so that one of the voice mail systems always answers first. However, there are coverage options in both the Avaya server running Communication Manager and the network that send a call immediately to the respective voice mail. Examples of these options include “busy,” “active,” or “send-all-calls” in Communication Manager and “cell phone unavailable” or “network congested” in the network. Users must understand that an unanswered call can result in a voice mail message in either mailbox.

Class of Restriction

For calls toward an Extension to Cellular station, Class of Restrictions are applied normally for a call terminating to a station. In particular, if the station is mapped, then the Class of Restriction (COR) of the office telephone applies. Any restrictions imposed by call filtering are applied after those imposed by the COR. Calling party restrictions pertaining to trunks do not effect the launching of Extension to Cellular calls. These restrictions include “outward,” “tac-toll,” and “all-toll.”

Its important to note that a phone may be restricted from making outside calls but the Extension to Cellular calls can be extended to the cell phone.

Distributed Communications System

Interswitch calls on Distributed Communications System (DCS) trunks are treated as internal calls.

- When an Extension to Cellular user has the **Calls Allowed** field on the Stations with Off-PBX Telephone Integration screen set to **internal** or **all**, DCS calls are delivered to the cell phone.
- When an Extension to Cellular user has the **Calls Allowed** field set to **external** or **none**, DCS calls are not delivered.

Distinctive alerting

Cell phones might not receive distinct rings for different types of calls. Check with your cellular service provider.

Extension to Cellular enable and disable

Extension to Cellular can be enabled or disabled. Users can enable or disable Extension to Cellular calls with either FACs or the enable and disable feature status button.

Users who receive their Extension to Cellular service through their cellular service provider (CSP) cannot enable or disable their Extension to Cellular calls. Through CSP, Extension to Cellular is always enabled.

Feature Access Codes

A user can activate Communication Manager features through Feature Access Codes (FACs). A user can access a FAC by one of these three methods:

- Dialing the telecommuter number
- Dialing the remote access number
- Dialing the “Select Idle” FNE

After hearing dial tone, the user enters the FAC.

Feature Name Extensions

When Extension to Cellular is enabled, a user can activate a Communication Manager feature through dialing a Feature Name Extension (FNE) from the cell phone or SIP endpoint. Feature name extensions correspond to a direct inward dialing (DID) number for each feature. Each FNE must match your dial plan, and are administered system-wide.

Message waiting indication

Cell phones cannot receive a screen that indicates a message waiting directly from Communication Manager.

“Notify me” under Unified Messenger for MS Exchange

The “notify me” feature of Unified Messenger® for Microsoft Exchange® (Version 4.0 or later) notifies users of messages in the corporate voice mailbox through the cell phone display. For more information on using this feature, see “Setting Notify Me” in the *Unified Messenger Telephone User Interface Online Guide*, accessed through http://www.avaya.com/support.

Note:
The cell phone must support text messaging to use this feature.

Office caller ID for another Extension to Cellular user

Incoming calls from other Extension to Cellular users are internal calls if office caller ID is enabled for the station associated with the cell phone.

- When an Extension to Cellular user has the **Calls Allowed** field set to **internal** or **all**, the Extension to Cellular calls are delivered.
- When an Extension to Cellular user has the **Calls Allowed** field set to **external** or **none**, calls from other Extension to Cellular users are not delivered.

QSIG

Inter-PBX calls on QSIG trunks are treated as internal calls.

- When an Extension to Cellular user has the **Calls Allowed** field set to **internal** or **all**, QSIG calls are delivered.
- When an Extension to Cellular user has the **Calls Allowed** field set to **external** or **none**, QSIG calls are not delivered.

Troubleshooting Extension to Cellular

This section lists the known or common problems that users might have with the Extension to Cellular feature.

Installation and administration test

After you have administered Extension to Cellular, use the following installation test procedures to ensure that the Extension to Cellular solution performs as expected. These tests are for Extension to Cellular cell phone use only.

The Extension to Cellular installation test and customer acceptance procedures follow the same guidelines used for testing a new station added to the switch. However, a review of the basic test procedures is provided in this section.

Test procedures

When performing these tests, you might need to place several calls to the Extension to Cellular cell phone.

To test the functionality of Extension to Cellular and coverage to voice mail:

1. Dial the office telephone number with any other touchtone telephone.

   Ensure that the office number and the Extension to Cellular cell phone ring simultaneously.
2. When the cell phone rings, verify that a ten digit ANI is displayed on the cell phone.

3. Verify that the call covers to the primary voice mail account (which is usually the corporate office voice mail box).

   If the call does not cover properly, review the coverage path number of rings and setup for corporate voice mail coverage.

   To get the voice mail coverage that you want, you can experiment with the number of rings set for the cellular service provider and for the office number coverage path. For more information about sending office caller ID, voice mail administration, and call forwarding, see the Detailed description of Extension to Cellular.

To test whether the second call appearance for the cell phone is in service:

1. Dial the office telephone number with a touch-tone telephone.
2. Answer the call that is ringing on the cell phone to start your “test” conversation.
3. With the test conversation in place and active, place another call to the office telephone number using any other touchtone telephone.

   The call must ring at the second call appearance on the office telephone, and at the cell phone. The display screen on the cell phone must show the second incoming call.
4. Answer the second call with the call waiting feature on the cell phone.

If any of the test procedures fail, you must verify that all administration entries were input correctly. If they were administered correctly, see the following table for further resolution procedures.

Problem	Possible Cause	Action
Users cannot receive Extension to Cellular calls on their cell phones.	For more information on possible sources of the problem, see Users cannot receive Extension to Cellular calls on their cell phones on page 1014.	For detailed instructions on troubleshooting this problem, see Users cannot receive Extension to Cellular calls on their cell phones on page 1014.
No CDR for Extension to Cellular calls.	The Configuration Set for the Extension to Cellular station has the **CDR for Calls to EC500 Destination** field set to **n**. The Extension to Cellular station is still using loopback trunks. The CDR Reports option on the trunk being used is **n**.	Check administration of Configuration Set screen, the Stations with Off-PBX Telephone Integration screen, or the Trunk Group screen, and change if necessary.
	Neither the principal station or other station extension is administered in the intra-switch-cdr screen.	Add one or both extensions in the intra-switch-cdr screen.

Problem	Possible Cause	Action
Call drops when user answers a cell phone.	Cellular Voice Mail Avoidance timeout is too long.	Shorten timeout. Train user to wait before answering cell phone. Remove user from Cellular Voice Mail Avoidance.
FNEs not working.	• Misadministration. • Calling Number Verification set to **y** on Configuration Set screen.	• Verify that the telephone number on off-pbx station-mapping screen is a full national number (10-digits in America and UK) and does not contain any a prefix digits like country code • For security, the option should be set to **y**. However, if calls always come over private trunks, you can set the option to **n**.

Problem	Possible Cause	Action
The user cannot access Feature Name Extensions by dialing the corresponding FNE.	There is no corresponding number administered on the **off-pbx-telephone feature-name-extension** screen or the mapping mode is not origination or both.	Administer an extension on the off-pbx-telephone feature-name-extension screen, or change the mapping mode to origination, or both.
User reports many unanswered calls are going to cellular voice mail.	Cellular Voice Mail Detection option (in user's configuration set) is not appropriate for cellular service provider. The no answer timeout for cellular voicemail is too short	Change the Cellular Voice Mail Detection option to timeout. This will handle any cell network condition (congestion, cell phone off, and so on) that causes the call to go immediately to cellular voicemail. Have user contact service provider to lengthen the no answer timeout so that it is longer than the coverage path timeout. This will ensure that unanswered calls ringing at the cell phone will go to the corporate voicemail. Discuss with user using the confirmed answer option. This option handles a common occurrence not handled above. A cell phone out of network coverage will go to cellular voicemail after about 3 rings. This is too long for Cellular Voice Mail Detection and too short for a coverage path fix.
User reports desk set does not ring, rings only once, or that callers are sent immediately to cellular voice mail.	Cell phone is off and calls are immediately being sent to cellular voicemail.	Change the Cellular Voice Mail Detection option to timeout (in user's configuration set).

Problem	Possible Cause	Action
The user reports that the cell phone is not receiving caller identification numbers for calls from the Avaya server running Communication Manager. But, the office number that the cell phone is mapped to does.	The Avaya server running Communication Manager has not been administered properly for sending caller identification numbers. Most cellular service providers require a number in national format.	Recheck the outbound trunk screen to ensure that the **Send Calling** field is set to **y**.
	External trunks serving the cell phone are using a non-ISDN trunk.	Change the routing administration to route over an ISDN trunk.
The user reports that the person being calling is receiving the incorrect caller ID.	The Configuration Set screen has the **Calling Number Style** field set to **PBX**.	Change the **Calling Number Style** field on the Configuration Set screen to **network**.
	There is an incorrect entry on the ISDN public-unknown numbering screen.	Verify that the entries on the ISDN public-unknown numbering screen are correct.

Problem	Possible Cause	Action
The user reports that the cell phone is receiving a switch default caller identification number for calls from the Avaya server running Communication Manager.	The ISDN Service Provider (SP) is replacing the caller identification with a fixed caller ID.	This is generally not solvable within the PBX. Escalate the issue to your Telecom Manager. The manager can contact your ISDN SP to request a solution or an alternate ISDN SP that allows the caller identification to pass. Some service providers will pass the caller ID if special application SA8931 is enabled. This sends the user's station (DID) number as a redirecting number in addition to the original calling number. In some instances special application SA8983 is helpful. When this option is on, the user's station (DID) number is sent as the calling number to the cell phone. This distinguishes EC500 calls from direct calls to the cell phone.
	The switch is blocking the outgoing caller identification and is passing a default caller ID.	Change your switch administration to allow caller identification to go outside the switch.
The user hears a beep while on a call originating from the Avaya server running Communication Manager. The user cannot use the call waiting feature on the cell phone to switch to the other call.	Most likely the user is hearing the tone provided by the Avaya server running Communication Manager when call waiting is enabled at the switch.	You have two possibilities: 1) Communicate to the user that when a call waiting indication is heard, but the user cannot switch the call, the user must hang up on the first call to receive the second call, OR 2) Disable call waiting at the switch level. The regular call waiting capability provided by the cellular service provider then handles the call waiting feature.

Problem	Possible Cause	Action
The Extension to Cellular cell phone call into the office switch fails to provide the office caller ID.	The **Cell Phone Number** field administered for the **Extension to Cellular** station does not have the required entry, which almost always is the full national number.	Type the full caller ID number in the **Cell Phone Number** field. Remove any dialing prefixes such as long distance access code (1 in US and Canada, 0 in Europe and many other countries), international access code (011 in US and Canada, 00 in Europe and many other countries), or country code. The dialing prefixes should be administered in the **dial prefix** field, and country code in the **country code** field.
	Calling Number Verification set to **y** on Configuration Set screen.	Set Calling Number Verification to **n**. See FNEs not working. on page 1006.
	The **Mapping Mode** field administered for the **Extension to Cellular** station does not contain **origination** or **both**.	Type **origination** or **both** in the **Mapping Mode** field.
	The external inbound call is not entering into the switch over an ISDN trunk.	Contact the ISDN Service Provider to ensure that inbound calls come into the switch through an ISDN trunk.
	The external inbound call does not come into the switch on which the Extension to Cellular cell phone station is administered.	Create a station for the Extension to Cellular cell phone with the proper mapping on the switch that the call enters.
	The calling number is manipulated on the Inbound Trunk screen.	Administer the Extension to Cellular station **Cell Phone Number** field to match the modified calling number.
	The cellular service provider does not send the calling number.	Call the cellular service provider to allow the caller ID to be sent.

Problem	Possible Cause	Action
	Someone else was on a call simultaneously on the office telephone and on the same line appearance as the originating Extension to Cellular cell phone call.	Move the mapped line appearance to a button that is not likely used by another telephone call.
The Avaya server running Communication Manager does not allow a default entry of extensions. For example, you cannot enter the # key alone to replace entering the extension followed by the # key.	The cell phone number is improperly mapped.	See The Extension to Cellular cell phone call into the office switch fails to provide the office caller ID. in this table.
An intercept tone is received when attempting to enable/ disable Extension to Cellular For example, the tone chimes when you type the Feature Access Code, #, Station Security Code, and #.	The user has used the Station Security Code of the Extension to Cellular extension and the code is different from that of the principal.	The user must type the code of the principal extension.
	The Station Security Code is blank for the principal.	The Station Security Code for the principal must be administered.
When attempting to enable/ disable Extension to Cellular, the user receives an intercept tone.	The **Applications** field administered on the Stations with Off-PBX Telephone Integration screen for the Extension to Cellular station is not **EC500** or **PBFMC**.	Change the **Applications Extension** field on the Stations with Off-PBX Telephone Integration screen for the Extension to Cellular station to **EC500** or **PBFMC**.
	The **Applications** field administered on the Stations with Off-PBX Telephone Integration screen for the Extension to Cellular station is **EC500**. But, the **Configuration Set** is not administered for **DTMF**.	Access the associated Configuration Set screen and ensure that the entry in the **Post Connect Dialing Option** field is **DTMF**.
The office caller ID is that of the origination mapped Extension to Cellular station and not of the host extension.	The Extension to Cellular station is not mapped to the host telephone.	Map the Extension to Cellular station to the host extension.

Problem	Possible Cause	Action
The administered Extension to Cellular feature button on the office telephone flashed for 2 seconds at the broken flutter rate.	The Extension to Cellular administration somehow got corrupted.	Disable, then enable, Extension to Cellular.
User cannot “engage” the Extension to Cellular timer through the administered feature button on the office telephone.	The optional Extension to Cellular timer was not configured.	Configure the optional Extension to Cellular timer on the Station screen. See Figure 231: Station screen on page 976, and the related steps identifying how to set the timer.
The user receives the error **Contact System Administrator** when trying to enable/disable Extension to Cellular through the administered feature button on the office telephone.	The Stations with Off-PBX Telephone Integration screen was not correctly administered.	Verify that all required information, in the correct format, is included on the Stations with Off-PBX Telephone Integration screen. In particular check that the **Dial Prefix**, **Country Code**, and **Phone Number** fields are administered correctly.
An Extension to Cellular station is mapped to a principal station, and the principal station later adds a configured Extension to Cellular feature access button. The **`status station`** command for the principal station shows that Extension to Cellular is disabled. The **`status station`** command for the mapped Extension to Cellular station shows that Extension to Cellular is enabled.	A previously administered and enabled Extension to Cellular station was mapped to a principal station that does not have an Extension to Cellular feature access button configured.	Configure an Extension to Cellular feature access button on the principal station. The principal station must support configurable feature buttons. See Administering an enable/disable feature button on page 974. When configured, press the Extension to Cellular feature access button to enable Extension to Cellular. This action synchronizes the enable/disable state between the principal station and its mapped Extension to Cellular station.

Problem	Possible Cause	Action
User reports cannot use Idle Appearance Select FNE to call certain extensions or external destinations.	The user is misdialing. The PBX has multiple locations, and an incorrect location is used for interpreting the dialed digits.	Administer the **location** field on the Stations with Off-PBX Telephone Integration screen with the location of the user's desk set. Since this field is not administrable for the EC500 application, it may need to be changed to **PBFMC**.
User hears dial-tone when answered an EC500 call.	User has the Confirmed Answer feature enabled on the configuration set form.	Instruct user to dial a digit after the dial tone.
User enters a digit after hearing dial tone, but is not cut through to the caller.	User is entering the digit too quickly.	Some cellular providers need almost a second to cut through a voice path after answer. Instruct user to pause between answering the phone and pressing the digit.
User dials the Self Administration for EC500 FAC and receives intercept tone.	The user is misdialing extension or security code. The user is not entering a number that is routable through ARS.	Instruct user in proper sequence for entering information for the feature.
User reports that after setting number using Self Administration for EC500, calls are delivered properly to the cell phone, but there is no office caller ID and he cannot use FNEs.	A dialing prefix or country code was entered as part of the phone number.	Instruct user to separate entry of dialing prefix, country code, and phone number by an asterisk.
User reports some people he calls see an office caller ID and others see the cell phone number.	There are multiple PBXs. Only calls to the PBX where the user is located can see the office caller ID.	Administer SIP signaling groups connecting the PBXs and administer the Mapping Subscriptions form to shared the mappings among the PBXs.

Users cannot receive Extension to Cellular calls on their cell phones

If Extension to Cellular users cannot receive calls on their cell phones, follow these procedures in the suggested order to isolate and fix the problem. After each step, verify if the problem was fixed. Make a call to the mapped cell phone through the office telephone number.

1. Verify that you can call the cell phone from the switch.

   This call also verifies that the service contract with the cellular service provider (CSP) is active, and that the user gets good coverage in that area.

   Make the direct call to the published number of the cell phone. When making this test call, wait until the call rings the cell phone which verifies that there is coverage. Or, wait until the call goes to the cellular voice mail. This coverage verifies that the service is provided but there might not be good coverage.

2. In a SAT session, type **`status station`**. Click **Enter**.

   The system displays the **Status Station** screen. Verify the office number that the Extension to Cellular telephone is mapped to. Verify that SAC or Call Forwarding has not been activated on the principal extension.

3. For the Extension to Cellular extension, type **`status station <extension>`**. Click **Enter**.

   The system displays the **Status Station** screen for that extension.

   Check the following states:

   - The service state is “in service/idle.” If not, type **`release <extension>`**. Click **Enter** to put the extension back in the active state.
   - The Extension to Cellular state is enabled on the Status Station screen. If Extension to Cellular is disabled, ask the user to enable Extension to Cellular for the principal office number.

4. On the Stations with Off-PBX Telephone Integration screen (Figure 221: Stations with Off-PBX Telephone Integration screen, page 2 on page 965), verify that the entries in the following fields are correct:

   - **Mobility Trunk Group**
   - **Dial Prefix**
   - **Calls Allowed**
   - **Cell Phone Number**

5. Check the **ARS Analysis** table and ensure that there is an entry to route the cell phone number over an ISDN trunk on the switch.

6. If the Mobility Trunk Group is **ars** or **aar**, verify that no FAC number is included in the cell phone number field.

7. Type **`list ars route-chosen`** ***`1234567890`*** where ***`1234567890`*** is a 10-digit cell phone number, to verify the type of routing used to route the call.
8. Check ARS digit conversion to verify that no unwanted characters are added to the dial string.

If the problem cannot be corrected by following this procedure, escalate the issue to Avaya Remote Technical Services (RTS). In addition to the preceding checks, verify with the technician that the Extension to Cellular station is not restricted from receiving incoming calls.

Facility and Non-Facility Associated Signaling

Use Facility Associated Signaling (FAS) to allow an ISDN-PRI T1/E1 interface D-channel to carry signaling information for all the bearer (B) channels on its associated spans.

Use Non-Facility Associated Signaling (NFAS) to allow an ISDN-PRI T1/E1 interface D-channel to carry signaling information for as many as 300 bearer (B) channels on its associated spans.

Detailed description of Facility and Non-Facility Associated Signaling

This section provides a detailed description of the Facility and Non-Facility Associated Signaling feature.

Facility Associated Signaling (FAS) allows an ISDN-PRI T1/E1 interface D-channel to carry signaling information for all the bearer (B) channels on its associated spans.

Non-Facility Associated Signaling (NFAS) allows an ISDN-PRI T1/E1 interface D-channel to carry signaling information for up to 300 bearer (B) channels on its associated spans. In other words, a single D-channel can carry signaling information for numerous B-channels that are located on different DS1 circuit packs.

Note:

NFAS is valid for T1/E1 Country Protocol 1 only. Digital T1 service is also sometimes called DS1 to distinguish the service from analog T1 service.

ISDN-BRI trunks do not support NFAS. For more information, see ISDN Service on page 1089.

D-channel backup with NFAS

With NFAS, you can administer a backup D-channel to improve reliability. The system switches to the backup D-channel, if a signaling link failure occurs on the primary D-channel span.

You administer one D-channel as the primary D-channel, and another D-channel as the secondary D-channel. These assignments ensure that both D-channels are in the same state at the same time, and that neither channel can be used to carry B-channel traffic at any time. The primary D-channel has precedence over the secondary D-channel.

When D-channel backup is activated, the system preserves all calls that are answered. However, some call-related information can be lost. Calls that are not answered when D-channels are switched, can also lose call-related information.

Figure 252: ISDN-PRI configuration on page 1018 shows a possible configuration that involves three **ISDN**-**PRI**s between a DEFINITY Server and another DEFINITY Server or the public network.

Figure 252: ISDN-PRI configuration

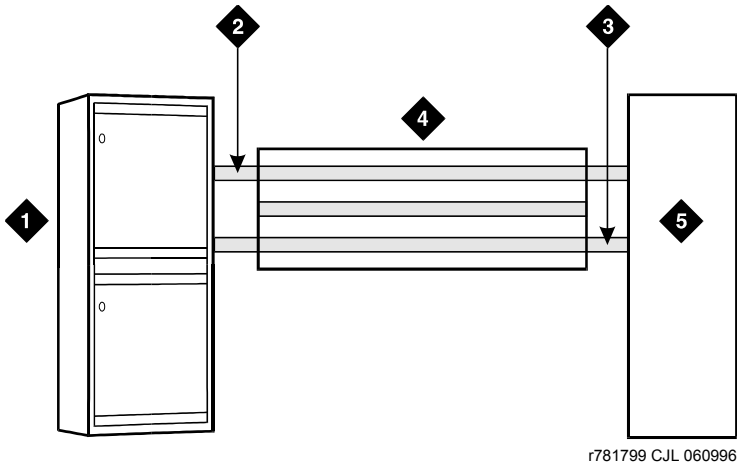


Figure notes:

1. Avaya S8*XXX* Server
2. Secondary D-channel
3. Primary D-channel
4. ISDN-PRI controlled by D-channel
5. Network far-end DEFINITY server

With T1 (24-channel) interfaces, two of the ISDN-PRIs contain a D-channel and 23 B-channels. The other ISDN-PRI contains 24 B-channels. One of the D-channels is the primary D-channel, and the other is the secondary D-channel. Together, this pair of D-channels signals for all 70 (23+24+23) B-channels in the three Primary Rate Interfaces.

Since the D-channels carry signaling for more than one ISDN-PRI facility, D-channel backup requires the use of NFAS. At any given time, one of the two D-channels is carrying Layer 3 signaling messages, while the other D-channel is active at layer 2, but in standby mode only. Any layer 3 messages received over the standby D-channel are ignored. Since only one of the D-channels can be active at a time, load sharing between the two D-channels is not possible. The two D-channels can provide signaling for only a predefined set of B-channels and cannot dynamically back up other D-channels on other interfaces.

D-channel backup activation

- D-channel Failure

  If the signaling link fails on the active D-channel, D1, or the hardware that carries the D1 channel fails, the system sends a message over the standby D-channel, D2. D2 then becomes the active D-channel and carries all subsequent signaling messages. When the signaling link or the hardware on D1 recovers from the failure, D1 becomes the standby D-channel.

- System Technician

  If a system technician sends a command to a switch over a D-channel, the system tears down the signaling link on D1. Then, the system sends a message on D2 to request that D2 become the active D-channel. D2 then becomes the active D-channel, and the switchover is complete.

Administering Facility and Non-Facility Associated Signaling

The following steps are part of the administration process for the Facility and Non-Facility Associated Signaling feature:

- Reviewing the guidelines for FAS and NFAS
- Implementing FAS and NFAS

This section describes:

- Any prerequisites for administering the Facility and Non-Facility Associated Signaling feature
- The screens that you use to administer the Facility and Non-Facility Associated Signaling feature
- Administration procedures for the Facility and Non-Facility Associated Signaling feature

Prerequisites for administering Facility and Non-Facility Associated Signaling

You must complete the following actions before you can administer the Facility and Non-Facility Associated Signaling feature:

- None

Screens for administering Facility and Non-Facility Associated Signaling

Screen name	Purpose	Fields
DS1 Circuit Pack	Define the signaling mode.	**Signaling Mode**
Interface Links	Create an association between the D-channel on a DS1 circuit pack and the port on the TN765 Processor interface that is used for this link.	All
Processor Channel	Assign processor channels to the link that is administered on the Interface Links screen.	All
Signaling Group	Define the signaling group.	All
Trunk Group	Add trunk ports to the trunk group, and to the signaling group.	• **Port** • **Sig Grp**

Reviewing the guidelines for FAS and NFAS

To review the guidelines for Facility Associated Signaling (FAS) and Non-Facility Associated Signalling (NFAS):

1. Decide which T1/E1 facilities use FAS.
2. Decide which of the remaining T1/E1 facilities carry D-channel signaling information on the sixteenth (E1) or the twenty-fourth (T1) channel. For those channels that have a D-channel backup, D-channel pairs must be allocated.
3. Define Signaling Groups. A Signaling Group is a group of B-channels for which a given D-channel, or D-channel pair, carries the signaling information. Each Signaling Group must be designated as either a FAS or an NFAS Signaling Group.
   - A FAS Signaling Group must contain all the ISDN B-channels on the T1/E1 interface that are associated with the D-channel of the group. An FAS signaling group cannot contain
     B-channels from any other DS1 circuit pack. For 24-channel DS1 boards, some of the DS1 ports can use in-band, robbed-bit, signaling and be members in a tie trunk group instead of an ISDN trunk group. These tie trunks cannot be members of a Signaling Group.

- No restriction exists on which T1/E1 ports can belong to an NFAS Signaling Group. Normally, an NFAS Signaling Group consists of one or two D-channels, and several complete T1/E1 interfaces.
- If a Signaling Group contains only a subset of the B-channels of a T1/E1 interface (ports 1 to 12, for example), the group is considered to be an NFAS Signaling Group, not an FAS Signaling Group. The remaining B-channels on the T1/E1 interface are then assigned as members of another NFAS Signaling Group.

4. You must assign an Interface ID to each T1/E1 facility in an NFAS Signaling Group. For example, if the B-channels in a Signaling Group span three T1/E1 facilities, you must assign a unique Interface ID to each of the three facilities. This designation is required to uniquely identify the same B-channel (port) number on each of the T1/E1 facilities in the Signaling Group. Therefore, this interface must be agreed upon by both sides of the interface, and administered before initialization.
5. Primary and secondary D-channel backup must be agreed by both sides of the interface, and administered before initialization. If the IDs do not match, the signaling group comes up, but calls fail.

Implementing FAS and NFAS

To implement FAS and NFAS, you must administer the following screens, in the order listed:

1. Administer the DS1 Circuit Pack screen.
2. Administer the Interface Link screen and associated screens.

   You can administer the Interface Link screen and associated screens any time after you administer the DS1 Circuit Pack screens, with the following restrictions:

   - You cannot assign a D-channel on a Signaling Group screen, unless the associated link is disabled.
   - You cannot assign a trunk member until you administer the associated Signaling Group.
3. Administer the ISDN-PRI Trunk Group, Signaling Group, and Trunk Group screens.

The screens in this administration section show the DS1 interface configuration for NFAS.

Administering the DS1 Circuit Pack screen

To administer the DS1 Circuit Pack screen:

1. You must specify the **Signaling Mode** field for each DS1 circuit pack.

   In this example, the **Signaling Mode** field set to **isdn-ext**. In this mode, either inband robbed-bit signaling, or a D-channel on another DS1 circuit pack. is used to signal all trunks on this circuit pack.

Figure 253: DS1 Circuit Pack screen

```
                    DS1 CIRCUIT PACK
            Location: 1B17                          Name: _______________
            Bit Rate: 2.048                            Line Coding: hdb3
     Signaling Mode: isdn-ext
Interface Companding: 5law
           Idle Code: 11111111
         MAINTENANCE PARAMETERS
      Slip Detection? n                    Remote Loop-Around Test? n
```

Administering the Interface Links and Processor Channels screens

To administer the Interface Links and Processor Channels screens:

1. Complete Steps a and b to administer the Interface Links and Processor Channels screens for the **ISDN**-**PRI** interface on DEFINITY SI configurations, if the D-channel is switched through the TN765 Processor Interface (PI) circuit pack:
   a. Use the Interface Links screen to create an association between the D-channel on a **DSI** circuit pack, and the port on a TN765 Processor Interface circuit pack that is used for this link.
   b. Use the Processor Channels screen to assign processor channels to the link that you administered on the Interface Links screen.

Administering the ISDN-PRI Trunk Group, Signaling Group, and Trunk Group Members screens

To administer the ISDN-PRI Trunk Group, Signaling Group, and Trunk Group Members screens:

1. Note the following details shown in the Signaling Group screen (Figure 254: Signaling Group screen (Group 1) - D-channel backup, three DS1 interfaces on page 1023, Figure 255: Signaling Group screen (Group 2) - no D-channel backup, two DS1 interfaces on page 1023, and Figure 256: Signaling Group screen (Group 3) - FAS on page 1024):
   - Signaling Group 1 B-channels on **DS**1 boards B0 and B1 are signaled by D-channel pair B1524 (see the **Primary D-Channel** field) and B1624 (see the **Secondary D-Channel** field).
   - Signaling Group 2 B-channels on board B1 are signaled by D-channel B1824.
   - Board B0 has no D-channel. The B-channels on board B0 can be signaled by either D-channel pair B1524/B1624 (Signaling Group 1) or D-channel B1824 (Signaling Group 2).

- The **DS**1 interface on board B19 (Signaling Group 3) is a Facility Associated Signaling situation. Note that the system does not display the **Secondary D-channel** and **Trunk Board/Interface ID** fields when the **Associated Signaling** field is set to **y**.

Figure 254: Signaling Group screen (Group 1) - D-channel backup, three DS1 interfaces

```
                          SIGNALING GROUP

Group Number : 1     Associated Signaling? n          Max number of NCA TSC: 0
                        Primary D-Channel: 1B1524     Max number of CA TSC: 0
                      Secondary D-Channel: 1B1624  Trunk Group for NCA TSC: __
        Trunk Group for Channel Selection: _____
    Trunk Brd    Interface ID        Trunk Brd    Interface ID
  1:   1B15          0             11:   ____          __
  2:   1B16          1             12:   ____          __
  3:   1B17          2             13:   ____          __
  4:   ____          __            14:   ____          __
  5:   ____          __            15:   ____          __
```

Figure 255: Signaling Group screen (Group 2) - no D-channel backup, two DS1 interfaces

```
                          SIGNALING GROUP

Group Number : 2    Associated Signaling? n          Max number of NCA TSC: 0
                       Primary D-Channel: 1B1824     Max number of CA TSC: 0
                     Secondary D-Channel: ______  Trunk Group for NCA TSC: __
       Trunk Group for Channel Selection: _____
    Trunk Brd    Interface ID        Trunk Brd    Interface ID
  1:   1B17          0             11:   ____          __
  2:   1B18          1             12:   ____          __
  3:   ____          __            13:   ____          __
  4:   ____          __            14:   ____          __
  5:   ____          __            15:   ____          __
```

Figure 256: Signaling Group screen (Group 3) - FAS

```
                              SIGNALING GROUP

Group Number : 3     Associated Signaling? y       Max number of NCA TSC: 0
                        Primary D-Channel: 1B1924   Max number of CA TSC: 0
                                                  Trunk Group for NCA TSC: __
        Trunk Group for Channel Selection: _____
```

2. In the **Sig Grp** column on the Signaling Group Screen (Figure 257: ISDN-PRI Trunk Group screen - Trunk Members with Required Signaling Group on page 1024) perform the following actions:
   - If a **DS**1 interface appears in one, and only one, Signaling Group, leave the **Sig Grp** field blank. The system automatically populates the field with the correct Signaling Group.
   - If a **DS**1 circuit pack appears in more than one Signaling Group, type the Signaling Group numbers in the appropriate fields.
3. Press **Enter** to save your changes.

Figure 257: ISDN-PRI Trunk Group screen - Trunk Members with Required Signaling Group

```
Page Y of X
                              TRUNK GROUP

                 Administered Members (min/max): xxx/yyy
                     Total Administered Members: xxx
GROUP MEMBER ASSIGNMENTS
    Port          Code   Sfx    Name               Night        Sig Grp
 1: 1B1501___                  ____________       _________      _
 2: 1B1523___                  ____________       _________      _
 3: 1B1601___                  ____________       _________      _
 4: 1B1623___                  ____________       _________      _
 5: 1B1701___                  ____________       _________      1
 6: 1B1709___                  ____________       _________      1
 7: 1B1716___                  ____________       _________      2
 8: 1B1724___                  ____________       _________      2
 9: 1B1801___                  ____________       _________      _
10: 1B1823___                  ____________       _________      _
11: 1B1901___                  ____________       _________      _
12: 1B1923___                  ____________       _________      _
13: _________                  ____________       _________      _
14: _________                  ____________       _________      _
15: _________                  ____________       _________      _
```

Facility Restriction Levels

Use the Facility Restriction Levels (FRL) feature to restrict some types of calls to specific users. For example, you can use FRL to allow some users to place international calls, but allow other users to place only local calls.

Facility Restriction Levels supports the following capabilities:

- Alternate Facility Restriction Levels (AFRL)

  Use AFRL to assign a second set of FRLs within a route pattern or to lines and trunks. For example, you can use an AFRL to disable the ability to place long distance calls when the office is closed.

- Traveling Class Mark (TCM)

  TCM allows the system to pass the FRL of a caller from one server to another server. The server that receives the FRL uses the FRL to determine the calling privileges that are assigned to the user.

Detailed description of Facility Restriction Levels

This section provides a detailed description of the Facility Restriction Levels (FRL) feature.

The FRL controls the privileges of the call originator. The system compares the FRL of the call originator with the FRL of the call termination point. The system allows the call to continue if the FRL of the call originator is equal to or greater than the FRL of the:

- Trunk group that is the terminating point of a call that is not an Automatic Alternate Routing (AAR) or an automatic route selection (ARS) call
- Route pattern that is assigned to the trunk that is the terminating point of an AAR or an ARS call

AAR and ARS calls

Originators of AAR and ARS calls

An originator of an AAR or an ARS call can be:

- An attendant

- A telephone user
- A remote access user
- A data terminal with a keyboard
- An incoming tie trunk group from a subtending location
- An incoming intertandem tie-trunk group, at a server or a switch
- An incoming access tie trunk group that links a remote main server or a switch to a tandem server or a switch

When the system determines the FRL of the call originator, the system uses the FRL that is assigned to the COR of:

- A telephone user
- All incoming tie trunk groups
- An attendant group for attendant-extended calls
- The individual attendant, if Individual Attendant Access is assigned
- The data module that is associated with a data terminal
- The barrier code that a user dials for a remote access call

  If the remote access call does not require a barrier code, no FRL exists.

Call termination points for AAR and ARS calls

A termination point for an AAR or an ARS call can be:

- A tie trunk
  - A tie trunk termination point for an AAR and ARS call can include a common-control switching arrangement (CCSA) access trunk and an enhanced private switched communications services (EPSCS) access trunk.
  - A tie trunk termination point for an AAR and ARS call does not include a release-line trunk (RLT).
- A Wide Area Telecommunications Services (WATS) trunk
- A central office (CO) trunk
- A foreign exchange (FX) trunk
- An integrated services digital network-primary rate interface (ISDN-PRI) trunk

Each of these outgoing trunk groups has a COR that contains an FRL. However, for AAR and ARS calls, the system uses the FRL that you assigned to the route pattern of the trunk group.

AFRL

Use the Alternate Facility Restriction Levels (AFRL) capability to define a second set of facility restriction levels within a route pattern, or for lines or trunks. Attendants and system administrators can activate the AFRLs and change user access to lines and trunks. For example, you can use AFRL to disable the ability to place a long distance call when the office is closed.

AFRL alters the route patterns for originating telephones, originating trunks, and dialed authorization codes. If AFRL is active:

- Traveling Class Mark (TCM) is set to a new FRL value
- The TCM information that the system records in the Call Detail Recording (CDR) records is the value of the AFRL, not the original TCM.

CAUTION:
AFRL has an impact on both AAR and ARS call routing because AFRL can change routing preferences. The use of AFRL on tandem and tie-trunk applications can affect entire networks. The system can block calls that are part of a cross-country private network that need to be routed further.

Alt-frl feature button

You can assign an **alt-frl** button to any attendant console and to any user telephone. The attendant or the user presses the **alt-frl** button to activate and deactivate the AFRL. The use of the **alt-frl** button can affect the status of other buttons.

When AFRL is active, the user might notice a change in calling privileges. Consider notifying users of the changes in calling privileges, and prepare your telecommunications department to respond to user inquiries.

Authorization codes

Authorization codes prevent unauthorized access to some system facilities. When a user dials an authorization code, the system checks the code. If the code is invalid, the system generates the intercept tone. If the code is valid, the system uses the COR and the FRL that is associated with the authorization code for further call processing. However, if AFRL is activated, the system uses the AFRL for further call processing.

If the system uses an intertandem tie trunk group for a call, the system outpulses a TCM as the last digit of the number. If the FRL of the intertandem tie-trunk is equal to or greater than the terminating FRL, the system proceeds with call processing. If the FRL of the originator is less than the FRL of the termination point, the system compares the TCM with the FRL of the tie trunk. If the TCM is greater than or equal to the FRL of the tie trunk, the system proceeds with call processing.

Administering Facility Restriction Levels

This section describes the screens that you use for administering the Facility Restriction Levels (FRL) feature.

Screens for administering Facility Restriction Levels

Screen name	Purpose	Fields
AAR Digit Analysis Table	Associate a dialed string with a route pattern, and thus to an FRL.	**Route Pattern**
ARS Digit Analysis Table	Associate a dialed string with a route pattern, and thus to an FRL.	**Route Pattern**
Attendant Console	Assign an **alt-frl** button for the attendant so that the attendant can activate the AFRL capability.	Any available button field in the **Feature Button Assignments** area
	Assign a COR for the attendant to associate an FRL with the attendant.	**COR**
Class of Restriction	Assign an FRL to the Class of Restriction (COR).	**FRL**
Console Parameters	Assign a COR for the attendant group to associate an FRL with the attendant group.	**COR**
Data Module	Assign a COR for the data module to associate an FRL with the data module.	**COR**
Remote Access	Assign a COR to the barrier code to associate an FRL with the barrier code.	**COR**
Route Pattern	Assign an FRL to the trunk group.	**FRL**

Screen name	Purpose	Fields
Station	Assign an **alt-frl** button for a user so that the user can activate the AFRL capability.	Any available button field in the **Button Assignments** area
	Assign a COR for the user to associate an FRL with the user.	**COR**
Trunk Group	Require that a user enter an authorization code, if the user wants to tandem a call through an Automatic Alternate Routing (AAR) or an Automatic Route Selection (ARS) route pattern.	**Auth Code**
	Assign a COR for the trunk group to associate an FRL with the trunk group.	**COR**

End-user procedures for Facility Restriction Levels

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Facility Restriction Levels (FRL):

- Using the Alternate Facility Restriction Levels (AFRL) capability

To use the AFRL capability:

- To activate AFRL, press the **alt-frl** button.
- To deactivate AFRL, press the **alt-frl** button.

Reports for Facility Restriction Levels

The following reports provide information about the Facility Restriction Levels feature:

- None

Considerations for Facility Restriction Levels

This section provides information about how the Facility Restriction Levels (FRL) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Facility Restriction Levels under all conditions. The following considerations apply to Facility Restriction Levels:

- Trunk groups
  - Use the Route Pattern screen to assign the FRL to a trunk group.
  - You can use the same trunk group in more than one route pattern.
  - The same trunk group can have a different FRL in a different pattern.
  - You can assign the same FRL to more than one trunk group.
- General access

  Be consistent in FRL assignments. Always use FRL 0 or FRL 1 for a trunk group that everyone can access.
- Route patterns

  If you use a range of 0 through 5 in one route pattern, use the same range in another pattern, if all users can access the first-choice route.

  Assign a Class of Restriction (COR) with an FRL of 0 to a group of users to restrict the users to local calls. Use any other number for the FRL on your first-choice route pattern.
- Remote access barrier codes

  You assign FRLs for remote access users through the remote-access barrier codes. The simplest way to assign these FRLs is to duplicate the on-premises FRLs, and then relate the appropriate barrier code to users who use remote access. For more information, see Remote Access on page 1415.

Interactions for Facility Restriction Levels

This section provides information about how the Facility Restriction Levels feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Facility Restriction Levels in any feature configuration.

- Call Detail Recording (CDR)

  If your system uses a 15-digit CDR account, the system overwrites the **FRL** field in the **CDR** record with the account code.

Facility Test Calls

Use the Facility Test Calls feature to make test calls to access specific trunks, dual-tone multifrequency (DTMF) receivers, time slots, and system tones.

Detailed description of Facility Test Calls

This section provides a detailed description of the Facility Test Calls feature.

With the Facility Test Calls feature, you can make test calls to access specific trunks, dual-tone multifrequency (DTMF) receivers, time slots, and system tones.

You can make test calls from any telephone to test specific trunks. Avaya maintenance personnel can make test calls from remote locations.

The system supports four types of facility test calls.

- Trunk test for specific tie trunks or central office (CO) trunks.

  You cannot test direct inward dialing (DID) trunks with this feature. Your Class of Restriction (COR) must allow you to use the Facility Access Trunk Test function.
- DTMF receiver test for DTMD receivers that are located on a tone detector or a call classifier/tone detection circuit pack.
- Time slot test for a specific time slot on the time division multiplex (TDM) buses, or the out-of-service time slots.
- System tone test for a specific system tone.

For more information, see the *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

You can create a Feature Access Code (FAC) for administrators and users to access the Facility Test Calls feature. You can also assign a feature button for a user to access the feature from the user telephone.

Security

SECURITY ALERT:
Proper administration of Facility Test Calls minimizes the ability of unauthorized persons to gain access to your system. However, you are responsible to properly implement the feature, evaluate and administer the various restriction levels, protect access codes, and distribute the codes only to individuals who are aware of the sensitive nature of the access information. Instruct each authorized user to properly use access codes.

In rare instances, unauthorized individuals use Facility Test Calls to connect to the public network. Applicable tariffs require that you pay all network charges for such calls. Avaya Inc. cannot be responsible for charges incurred by such calls, and will not make any allowance or give any credit for charges that result from unauthorized access.

To help secure the Facility Test Calls feature from unauthorized use:

- Remove the access code when the access code is not in use.
- Change the access code from the default value that is set when you receive your system.
- Secure records of the access code.
- Use COR to restrict the number of users who can use the access code.

You can set Logoff Notification to notify you when you log off the system that the Facility Test Calls feature is still enabled. This notification can alert you that an unauthorized activation of the feature has occurred.

Administering Facility Test Calls

This section describes the screens that you use for administering the Facility Test Calls feature.

Screens for administering Facility Test Calls

Screen name	Purpose	Fields
Class of Restriction	Assign an FRL to the Class of Restriction (COR).	**FRL**
Feature Access Code (FAC)	Specify a Feature Access Code (FAC) for Facility Test Calls	**Facility Test Calls Access Code**
Station (multiappearance)	Assign a **trk-ac-alm** facility test lamp alarm button for a user.	Any available button field in the **Button Assignments** area

Considerations for Facility Test Calls

This section provides information about how the Facility Test Calls feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Facility Test Calls under all conditions. The following considerations apply to Facility Restriction Levels:

- You must use a digital telephone that resides on the local server to make test calls.

Interactions for Facility Test Calls

This section provides information about how the Facility Test Calls feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Facility Test Calls in any feature configuration.

- Service Observing

  You cannot use Facility Test Calls for Service Observing.

Feature Access Codes

Use Feature Access Codes (FAC) to provide users with quick access to certain features of the telephone system. When you assign a FAC to a feature, users do not have to program a button on the telephone to use this feature. Instead, users just dial the FAC.

Detailed description of Feature Access Codes

This section provides a detailed description of Feature Access Codes.

Feature Access Codes can contain from one to four characters. These characters can be all digits, or a combination of digits and either an asterisk (*) or a pound sign (#). If you use an asterisk (*) or a pound sign (#), these characters must appear in the first position of the FAC. Before you define a FAC that includes an asterisk or a pound sign, consider that users with analog rotary dial telephones cannot dial these codes.

The asterisk (*) and pound sign (#) are often used in pairs. Use one character plus digits to activate a feature, and the other character plus the same digits to deactivate that feature. For example, say that you use the asterisk (*) and then the digits 2 and 9 to activate the Posted Messages feature. You might then use the pound sign and the same digits 2 and 9 to deactivate the Posted Messages feature.

FACs are divided into four types:

- Access FACs

  An access FAC gives a user access to a feature.

- Activate or deactivate FACs

  An activate and a deactivate pair of FACs allows a user to activate or deactivate a specific feature.

- Send or Cancel FACs

  A send and a cancel pair of FACs allows a user to send or cancel a message.

- Lock or unlock FACs

  A lock and an unlock pair of FACs allows a user to lock or unlock the message retrieval capability of a telephone.

Many features already have default FACs assigned. You can use these default FACs, or you can change the default FACs to codes that make more sense to you.

Each FAC must conform to your dial plan, and each FAC must be unique. If you try to define a FAC that is already assigned to another feature, the system warns you of the duplicate FAC. You cannot continue until you change one of the FACs.

Administering Feature Access Codes

The following steps are part of the administration process for the Feature Access Codes feature:

- Assigning Feature Access Codes
- Changing or deleting Feature Access Codes

This section describes:

- Any prerequisites for administering Feature Access Codes
- The screens that you use to administer Feature Access Codes
- Complete administration procedures for Feature Access Codes

Prerequisites for administering Feature Access Codes

You must complete the following actions before you can administer Feature Access Codes:

- Ensure that Feature Access Codes are set up in your dial plan. You must have a FAC or Deactivation Access Code (DAC) entry on the dial plan screen for the digit range that you intend to use for you Feature Access Codes. For a description of how to set up your dial plan, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Feature Access Codes

Screen name	Purpose	Fields
Feature Access Code (FAC)	Assign FACs to specified telephone features.	All

Assigning Feature Access Codes

To assign a FAC for a specific feature:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 258: Feature Access Code (FAC) screen on page 1037).

Figure 258: Feature Access Code (FAC) screen

```
change feature-access-codes                                  Page 1 of 8

                              FEATURE ACCESS CODE (FAC)

         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
                      Announcement Access Code: ____
                       Answer Back Access Code: ____
                         Attendant Access Code: ____
      Auto Alternate Routing (AAR) Access Code: ____
    Auto Route Selection (ARS) - Access Code 1: ____     Access Code 2: ____
                 Automatic Callback Activation: ____      Deactivation: ____
Call Forwarding Activation Busy/DA: ____   All: ____      Deactivation: ____
                        Call Park Access Code: ____
                      Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                  CDR Account Code Access Code: ____
                        Change COR Access Code: ____
                   Change Coverage Access Code: ____
                   Contact Closure   Open Code: ____       Close Code: ____
                   Contact Closure  Pulse Code: ____
```

2. In the field next to the specific feature to which you want to assign the FAC, type a FAC that conforms to your dial plan. You might have to scroll through several pages of the Feature Access Code (FAC) screen to find the telephone feature that you want.

   Some features require more than one FAC. Type a FAC in each required field. For example, type a separate FAC in the **Call Forwarding Activation Busy/DA** field, the **All** field, and the **Deactivation** field.

3. Press **Enter** to save your changes.
4. Ensure that you notify all users about the assigned FACs.

Changing or deleting Feature Access Codes

To change or delete a FAC for a specific feature:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 259: Feature Access Code (FAC) screen on page 1038).

Figure 259: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 1 of 8

                              FEATURE ACCESS CODE (FAC)

         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
                      Announcement Access Code: ____
                       Answer Back Access Code: ____
                         Attendant Access Code: ____
      Auto Alternate Routing (AAR) Access Code: ____
    Auto Route Selection (ARS) - Access Code 1: ____     Access Code 2: ____
                Automatic Callback Activation: ____      Deactivation: ____
Call Forwarding Activation Busy/DA: ____   All: ____     Deactivation: ____
                         Call Park Access Code: ____
                       Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                  CDR Account Code Access Code: ____
                        Change COR Access Code: ____
                   Change Coverage Access Code: ____
                   Contact Closure   Open Code: ____       Close Code: ____
                   Contact Closure  Pulse Code: ____
```

2. In the field next to the feature that you want to change, type a new FAC that conforms to your dial plan over the existing FAC. You might have to scroll through several pages of the Feature Access Code (FAC) screen to find the telephone feature that you want.

   Some features require more than one FAC. Type a FAC in each required field. For example, type a separate FAC in the **Call Forwarding Activation Busy/DA** field, the **All** field, and the **Deactivation** field.

3. To remove a FAC, delete the existing FAC and leave the field blank.
4. Press **Enter** to save your changes.
5. Ensure that you notify all users about the changed FACs.

Troubleshooting Feature Access Codes

This section lists the known or common problems that users might experience with Feature Access Codes:

Problem	Possible cause	Action
The user experiences delays when the user attempts to use a FAC.	You might have a FAC and an extension with the same digits on your dial plan.	Check your dial plan to see if you have a FAC and an extension with the same digits. For more information, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Group Paging

Use the Group Paging feature to make an announcement over a group of digital speakerphones.

- You can create up to 32 paging groups on one media server.
- Each group can consist of up to 32 extensions.
- You can assign the same extension to different groups.

Detailed Description of Group Paging

With the Group Paging feature, you can create a page group, and assign extensions as members of the group. You assign an identifying extension to each page group, which users dial to page the group. When a user dials the extension of the paging group, Communication Manager activates the speakers on all the telephones in the group. Speakerphone paging is one-way communication: Group members hear the person place the page, but cannot respond directly.

Restrictions

Pages are not always heard on every telephone in a group. An extension does not transmit a group page if the extension has an active or a ringing call, or if the extension is off-hook. Listeners can drop a page if the listeners disconnect. Pages cannot be heard when the Send All Calls or Do Not Disturb features are activated.

When a group member does not hear the announcement for any of these reasons, the caller is not notified. Therefore, the originator of an important page might want to check with the group members to ensure that all members heard the page.

Controlling access to paging groups

Each paging group is assigned a class of restriction (COR). Thus you can provide or deny access to different classes of users by setting calling permissions appropriately. Note that you can administer CORs so that remote callers can make speakerphone pages. If you do not want to allow remote users to page, you can use the Class of Restriction screen to set calling permissions for vector directory numbers (VDNs) and trunk groups so that neither can initiate pages. For more information on CORs, see Class of Restriction on page 715.

Administering Group Paging

The following steps are part of the administration process for the Group Paging feature:

- Creating a paging group
- Changing a paging group
- Viewing all paging groups

This section describes:

- Any prerequisites for administering the Group Paging feature
- The screens that are required to administer the Group Paging feature
- Complete administration procedures for the Group Paging feature

Screens for administering Group Paging

Screen Name	Purpose	Fields
Group Paging Using Speakerphones	Create or change a paging group, and add or delete group members.	All
Speakerphone Page Groups	View a list of all existing paging groups.	All

Creating a paging group

To create a new paging group:

1. Type **`add group-page n`**, where ***n*** is a number between **1** and **32**, or type **`add group-page next`** for the next available group number. Press **Enter**.

   The system displays the Group Paging Using Speakerphone screen (Figure 260: Group Paging Using Speakerphone screen on page 1043).

Figure 260: Group Paging Using Speakerphone screen

```
                    GROUP PAGING USING SPEAKERPHONE

   Group Number: 1                          Group Extension: 3210
     Group Name: Sales staff                            COR: 5
GROUP MEMBER ASSIGNMENTS
    Ext     Name                             Ext      Name
 1: 2009    B. Smith                   17:
 2: 2010    R. Munoz                   18:
 3: 2011    Y. Lu                      19:
 4: 2012    A. Sullivan                20:
 5:                                    21:
 6:                                    22:
 7:                                    23:
 8:                                    24:
 9:                                    25:
10:                                    26:
11:                                    27:
12:                                    28:
13:                                    29:
14:                                    30:
15:                                    31:
16:                                    32:
```

2. In the **Group Extension** field, type the extension that users dial to page the members of this group. In this example, the Group Extension is **3210**.
3. In the **Group Name** field, type the name that you want to assign to this paging group. This name appears on the telephone display of a caller when paging the group. In this example, the Group name is **Sales staff**.
4. In the **COR** field, type the Class of Restriction (COR) that you want to assign to this group. In this example, any user who wants to page this group must have permission to call COR 5.
5. In the **Ext** field in row 1, type the extension of the first member of the paging group. In this example, the extension is **2009**.
6. Type the remaining extensions of the other members of this group. When you save your changes, the software automatically completes the **Name** fields with the names that are associated with the extensions on the Station screen.
7. Press **Enter** to save your changes.

   Paging is now active on the system.

Changing a paging group

You can add or delete members of a paging group, or modify the other attributes of the group, such as the group name, group extension, or COR.

To change a paging group:

1. Type **change group-page *n***, where ***n*** is the number of the paging group that you want to change. Press **Enter**.

   The system displays the Group Paging Using Speakerphone screen (Figure 260: Group Paging Using Speakerphone screen on page 1043.

2. In the **Ext** field, type the extension of a member that you want to add, or delete the extension of a member that you want to remove from the group.
3. Make any changes to the **Group Name**, **Group Extension**, or **COR** fields.
4. Press **Enter** to save your changes.

Viewing all paging groups

To view a list of existing paging groups:

1. Type **list group-page**. Press **Enter**.

   The system displays the Speakerphone Page Groups screen (Figure 261: Speakerphone Page Groups screen on page 1044).

Figure 261: Speakerphone Page Groups screen

```
list group-page

                          SPEAKERPHONE PAGE GROUPS
  Group     Group                                                  No. of
  Number    Extension        Group Name                COR       MEMBERS
  11:       696147           AUTO H-grp-page1          15        6
  12:       696148           AUTO H-grp-page1          15        2
  13:       696149           Test Group 1              1         4
  14:       694056           Test Group 2              1         2
```

Considerations for Group Paging

This section provides information about how the Group Paging feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Group Paging feature under all conditions.

- The person making the group call should wait until after hearing the zip tone before starting to speak.

Interactions for Group Paging

This section provides information about how the Group Paging feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the Group Paging feature in any feature configuration.

- Attendant Intrusion

  Attendants cannot intrude on group pages. If the attendant tries to intrude on the originator of the page, the intrusion attempt succeeds. However, all group page members can hear both the paging originator and the attendant.

- Auto Exclusion and Manual Exclusion

  Bridged appearances are not allowed on the page. Therefore, the Auto Exclusion and the Manual Exclusion features are disabled. Auto Exclusion is not activated because there are no bridged appearances to alert when the page terminates.

- Auto Hold

  Auto Hold does not put a group page on hold. The page is dropped, and the incoming call is answered.

- Automatic Callback

  Automatic Callback is disabled when a user calls an active page group.

- Bridging

  Bridging is disabled on this feature. A bridged appearance of a group member does not receive any indication of a call when the page arrives. The bridged appearance cannot bridge onto the page.

- Call Coverage

  Pages do not follow the coverage paths of the group members. A page group cannot be a coverage point.

- Call Park

  Group members who receive a page cannot park the call.

- Call Pickup and Direct Call Pickup

  Other extensions cannot pick up a group page.

- Call Forwarding

  Group pages cannot be forwarded.

- Conference

  Neither group members who receive a page, nor the originator of the page, can conference the page to other extensions.

- Distributed Communications System (DCS)

  Page groups cannot be administered across DCS servers or switches. DCS is not supported.

- Do Not Disturb

  If a member of a page group activates Do Not Disturb, that member does not receive pages.

- Go to Cover

  The Go to Cover feature is ignored because group pages do not follow coverage.

- Hold

  The originator of a group page can put the page on hold, but group members cannot.

- Leave Word Calling

  Leave Word Calling (LWC) is disabled. A page group cannot receive messages.

- Manual Signaling

  The Manual Signaling feature cannot be assigned to a page group.

- Send All Calls (SAC)

  If a member of a page group activates SAC, that member does not receive pages.

- Service Observing

  Group page members and page originators cannot be observed while active on a page.

- Transfer

  Group members cannot transfer a page.

- Trunks

  Trunks cannot be added to a page group.

- Vectoring

  Paging groups cannot be explicitly added to a vector path.

Troubleshooting Group Paging

This section lists the known or common problems that users might experience with the Group Paging feature.

Problem	Possible cause	Action
A user gets a busy signal when the user tries to page.	All telephones in the group are busy or off-hook.	Wait a few minutes and try again.
	Send All Calls or Do Not Disturb is activated for all telephones in the group.	Group members must deactivate these features to hear a page.
Some group members do not hear a page.	Send All Calls or Do Not Disturb is activated for the telephones of these group members.	Group members must deactivate these features in order to hear a page.

Hold

Use the Hold feature to temporarily disconnect from a call, use the telephone for another call, and then return to the original call.

Hold supports the following capabilities:

- Automatic Hold

  When an attendant or a multifunction telephone user selects a second call, the system automatically puts the active call on hold, and makes the second call active.

Detailed description of Hold

This section provides a detailed description of the Hold feature.

Multiappearance telephone users can use a Hold button to activate Hold. With Automatic Hold, a user can also press a second call appearance to put an active call on hold. The system holds the call at the call appearance that is used for the call. Multiappearance telephone users can hold a call on each call appearance.

Single-line telephone users can use two types of Hold, Soft Hold and Hard Hold.

Soft Hold

Use Soft Hold to conference or transfer a call that includes the held call. With Soft Hold, the user can put a call on hold, consult with another party, activate or deactivate a feature, and then return to the soft-held call.

Hard Hold

Use Hard Hold to perform operations that do not include the held call. The user can put a call on hold and call another party. The user can then answer a waiting call, transfer or conference the waiting call, or activate or deactivate features.

Automatic Hold

With Automatic Hold, attendants and multifunction telephone can alternate easily between two or more calls. For example, when an attendant or a multifunction telephone user selects a second call, the system automatically puts the active call on hold, and makes the second call active. Automatic Hold is a system-wide capability. If you do not enable Automatic Hold for your system, the system drops the current active call when an attendant or a user selects a second call. A call that is placed in Automatic Hold is in Hard Hold.

To put an active call on hold, without pressing the Hold button, the user presses a second call-appearance button. The second call appearance becomes active. A user can place more than one call on hold. However, the user must keep one call appearance available for other calls.

The controlling telephone can have only one auto-held call on soft hold at a time. A soft hold is the state of a line after the user presses a conference button or a transfer button, but before either process is complete. The controlling telephone is guaranteed the ability to reenter any auto-held call later, unless the auto-held parties disconnect, or the auto-held tone exceeds the auto-held tone time limit.

Administering Hold

The following steps are part of the administration process for the Hold feature:

- Enabling Automatic Hold
- Assigning a FAC for CAS remote hold and answer

This section describes:

- Any prerequisites for administering the Hold feature
- The screens that you use to administer the Hold feature
- Complete administration procedures for the Hold feature

Prerequisites for administering Hold

You must complete the following actions before you can administer the Hold feature:

- None

Screens for administering Hold

Screen name	Purpose	Fields
Feature Access Code (FAC)	Define the Feature Access Code (FAC) for centralized attendant services (CAS) attendant remote hold and answer.	**CAS Remote Hold/ Answer Hold-Unhold**
Feature-Related System Parameters	Enable the Automatic Hold capability for your system.	**Auto Hold**

Enabling Automatic Hold

To enable Automatic Hold for your system:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Auto Hold** field (Figure 262: Feature-Related System Parameters screen on page 1052).

Figure 262: Feature-Related System Parameters screen

```
change system-parameters features                                  page 5

                          FEATURE-RELATED SYSTEM PARAMETERS

       Public Network Trunks on Conference Call: 5              Auto Start? n
   Conference Parties with Public Network Trunks: 6              Auto Hold? y
 Conference Parties without Public Network Trunks: 6         Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180        Bridging Tone? n
                  Short Interdigit Timer (seconds): 3        Conference Tone? n
               Unanswered DID Call Timer (seconds): ____      Intrusion Tone? n
               Line Intercept Tone Timer (seconds): 30     Special Dial Tone? n
                  Long Hold Recall Timer (seconds):      Mode Code Interface? n
                       Reset Shift Timer (seconds): 0
     Station Call Transfer Recall Timer (seconds): 0
                               DID Busy Treatment: tone
       Invalid Number Dialed Intercept Treatment: Announcement _____
              Allow AAR/ARS Access from DID/DIOD? _
                Allow ANI Restriction on AAR/ARS? _
     Use Trunk COR for Outgoing Trunk Disconnect? _
                  7405ND Numeric Terminal Display? n            7434ND? n
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                         Attendant Originated Calls:
   DTMF Tone Feedback Signal to VRU - Connection: _    Disconnection: _
```

3. In the **Auto Hold** field, perform one of the following actions:
   - If you want the Automatic Hold capability available to all users on your system, type **y**.
   - If you do not want the Automatic Hold capability available to any users on your system, type **n**.
4. Press **Enter** to save your changes.

Assigning a FAC for CAS remote hold and answer

To assign a Feature Access Code (FAC) for Centralized Attendant Service (CAS) remote hold and answer for your system:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen, (Figure 263: Feature Access Code (FAC) screen on page 1053).

Figure 263: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 1 of 7

                              FEATURE ACCESS CODE (FAC)

Abbreviated Dialing List1 Access Code: ____
            Abbreviated Dialing List2 Access Code: ____
            Abbreviated Dialing List3 Access Code: ____
   Abbreviated Dial - Prgm Group List Access Code: ____
                         Announcement Access Code: ____
                          Answer Back Access Code: ____
                            Attendant Access Code: ____
         Auto Alternate Routing (AAR) Access Code: ____
          Auto Route Selection (ARS) Access Code1: ____  Access Code 2: ____
                    Automatic Callback Activation: ____   Deactivation: ____
   Call Forwarding Activation Busy/DA: ____   All: ____   Deactivation: ____
                            Call Park Access Code: ____
                          Call Pickup Access Code: ____
   CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                      CDR Account Code Access Code: ____
                            Change COR Access Code: ____
                       Change Coverage Access Code: ____

                      Data Origination Access Code: ____
                          Data Privacy Access Code: ____
                  Directed Call Pickup Access Code: ____
```

2. In the **CAS Remote Hold/Answer Hold-Unhold Access Code** field, type the FAC that a CAS attendant can use to:
   - Place calls on hold
   - Answer calls that are held at a remote server that is running Communication Manager.
3. Press **Enter** to save your changes.

Reports for Hold

The following reports provide information about the Hold feature:

- None

Considerations for Hold

This section provides information about how the Hold feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Hold under all conditions. The following considerations apply to Hold:

- To drop a call that is dialed from a single-line telephone within the first 10 seconds after you complete dialing the call, flash the switch hook.
- A single-line telephone user cannot hold a call that involves an attendant. A multiappearance telephone user can hold a call that involves an attendant, unless the user attempts to conference or transfer the call.
- When only Automatic Hold is involved, and the attendant on an active loop presses a second loop, the system places the active call on Hard Hold.
- The Held Call Timed Reminder does not apply to conference calls, and is not started when a conference is placed on hold.
- Automatic Hold operates in conjunction with the START key or the Automatic Start feature of an attendant console. The START key and the Automatic Start operation have precedence over Automatic Hold, and place an active loop call on soft hold.

Interactions for Hold

This section provides information about how the Hold feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Hold in any feature configuration.

- Automatic Callback

  A single-line telephone user cannot receive an Automatic Callback call while a call is on hold.

- Bridged Call Appearance

  Any user, who is active on a bridged call, can place the call on hold. If no other users with a bridged call appearance of the same extension are connected to the call, the status lamp at the Bridged Appearance button indicates that the call is on hold. If the primary extension or another bridged appearance is connected to the call, the status lamp at all bridged appearances indicates an active status for the call.

- Centralized Attendant Service (CAS)

  Automatic Hold does not affect the operation of **CAS.**

- Distributed Communications System (DCS)

  Automatic Hold does not affect the operation of DCS, and is administered separately for each node in a **DCS** network.

- **Leave Word Calling (LWC)**

  A multiappearance telephone user who is on hold can activate **LWC** toward the holding user.

  A single-line telephone user cannot activate **LWC** toward another user while a call is on Soft Hold.

- Music-on-Hold

  Only one party on hold can hear music.

- Personal Central Office Line (PCOL)

  When a user, who is active on a **PCOL** call, puts the call on Hold, the lamp flutters or winks. The status lamp that is associated with the **PCOL** button lamp does not track the busy or idle status of the **PCOL**.

- Priority Calling

  Users can receive priority ringing and have a call on soft hold.

Hot Line Service

Use the Hot Line Service feature to assign a specific destination to which the user of a single-line telephone automatically connects to a destination when the user goes off-hook.

Detailed description of Hot Line Service

This section provides a detailed description of the Hot Line Service feature.

With the Hot Line Service, the user of a single-line telephone can automatically connect to a preassigned destination when the user goes off-hook. You can assign the following numbers as a Hot Line Service destination:

- An attendant
- An extension
- A Feature Access Code (FAC)
- A public telephone number
- A private telephone number

The Hot Line Service destination number must be stored in an Abbreviated Dialing list. When the user goes off-hook, the system automatically routes the call to the stored number, and completes the call as if the user dialed the call.

If an attendant number is the Hot Line Service destination number, the system automatically routes the telephone user to the attendant.

If the appropriate FAC is stored with the number in the Abbreviated Dialing list, the system uses Automatic Alternate Routing (AAR), automatic route selection (ARS), Data Privacy, or Priority Calling.

If the Public Network Access code or the Private Network Access code is the number stored in the Abbreviated Dialing list, the system connects the user to the outside number.

A Direct Department Calling (DDC), a Uniform Call Distribution (UCD), a Terminating Extension Group (TEG) extension, or any individual extension within such a group, can be a Hot Line Service destination.

Hot Line Service does not change the way that a user receives calls. Calls to a user with Hot Line Service are controlled by the Class of Restriction (COR) that you assign to the user extension. Hot Line Service does not affect the recipient of the call.

Administering Hot Line Service

This section describes the screens that you use to administer the Hot Line Service feature

Screens for administering Hot Line Service

Screen name	Purpose	Fields
Abbreviated Dialing List • System List • Group List • Personal List	Store the number that you want the system to use when the user enters the dial code.	**Dial Code**
Data Modules • Data Line Module • MPD/MTDM • Netcon Data Module • Processor Interface Data Module • System Port Data Module • Packet Gateway (PGATE) • Netcon Data Module	Specify Hot Line Service information for the data module.	• **Special Dialing Option** • **Hot Line Destination**
Station - single-line	Specify Hot Line Service information for the user.	• **Hot Line Destination - Abbreviated Dialing List Number** • **Hot Line Destination - Dial Code** • **Special Dialing Code**

Reports for Hot Line Service

The following reports provide information about the Hot Line Service feature:

- None

Considerations for Hot Line Service

This section provides information about how the Hot Line Service feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Hot Line Service under all conditions. The following considerations apply to Hot Line Service:

- Specify the attendant as the Hot Line Service destination when you want the attendant to screen call originations.
- You can assign Hot Line Service to any number of telephones, with the same or different destinations. The number of users who can use Hot Line Service is limited by the number of entries that you can store in the Abbreviated Dialing lists.
- A Hot Line Service user can activate any feature, but only if the FAC is stored in the Abbreviated Dialing List.

Interactions for Hot Line Service

This section provides information about how the Hot Line Service feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Hot Line Service in any feature configuration.

- Night Service

  When Night Service is active, the system redirects the Hot Line Service call.

- Bridged Call Appearance - Single-Line Voice Terminal

  A bridged call appearance of a telephone that is administered for Hot Line Service, also places a hot line call automatically when a user goes off-hook on that bridged appearance.

- Loudspeaker Paging Access

  You can use Loudspeaker Paging Access with Hot Line Service to provide automatic access to paging equipment.

- Ringback Queuing

  If a Hot Line Service call accesses a trunk group with Ringback Queuing, the call can queue, unless the telephone is Termination Restricted by the Class of Service (**COR)**. Queuing, when applicable, is automatic on single-line telephones.

Hunt Groups

Use the Hunt Groups feature to set up a group of extensions that can handle multiple calls to a single telephone number. You can choose the call distribution method to route calls. For each call to the number, the system hunts for an available extension in the hunt group, and connects the call to that extension.

A hunt group is especially useful when you expect a high number of calls to a particular telephone number. A hunt group might consist of people who are trained to handle calls on specific topics. For example, the group might be a:

- Benefits department within your company
- Service department for products that you sell
- Travel reservations service
- Pool of attendants

A hunt group might also consist of a group of shared telecommunications facilities. For example, the group might be a:

- Modem pool
- Group of data-line circuit ports
- Group of data modules

Detailed description of Hunt Groups

This section provides a detailed description of the Hunt Groups feature.

The Hunt Groups feature supports the following capabilities:

- Announcements for hunt groups
- Call Coverage for hunt groups
- Call Distribution methods for hunt group types
- Hunt group extension unavailability
- Queues for hunt groups
- TTY hunt groups

Announcements for hunt groups

When an extension is not immediately available, the system plays a recorded announcement to the caller. You can record and assign one delay announcement to each hunt group queue. An announcement can be shared among hunt groups. Usually, a hunt group announcement asks the caller to wait, and says that the call will be answered in the order in which the call was received.

A call that connects to a delay announcement remains in a queue while the system plays the announcement. If the call is not answered by the time that the announcement completes, the caller hears music, if music is administered. If music is not administered, the caller hears silence. When the call starts ringing at the telephone of a hunt group member, the caller hears ringing.

Delay announcement intervals for hunt groups

You can define a delay announcement interval for each hunt group. This interval of 0 to 99 seconds specifies how long a call remains in the queue before the system connects the call to a recorded announcement. When a call enters the queue, the interval starts. If Call Coverage is administered, the Don't Answer interval of 1 to 99 ringing cycles also starts when the call enters the queue. After these intervals start, one of the following processes also starts:

- If the Don't Answer interval expires before the delay announcement interval expires, the system redirects the call to coverage.
- If no coverage point is available, the call remains in the queue. The system connects the call to the delay announcement when the delay announcement interval expires.
- If the delay announcement interval expires before the Don't Answer interval, the system connects the call to a delay announcement. If the announcement is already in use, the system resets the delay announcement interval.

This process continues as above until the call is answered, goes to coverage, connects to an announcement, or ends because the caller hangs up.

If you set the delay announcement interval to 0 seconds, the system automatically connects a call to the announcement. This announcement is called a *forced first announcement*. In this case, the system does not connect the call to a hunt group member until after the announcement. The caller does not hear music.

If the system uses call coverage to redirect a call to another hunt group, the caller does not hear the forced first announcement of either hunt group. However, the caller might hear the first or the second announcement of the covering hunt group.

Analog, aux-trunk, or integrated delay announcements for hunt groups

Delay announcements can be analog, aux-trunk, or digitally integrated. For an analog or aux-trunk announcement, a caller who enters the queue hears the associated announcement the next time that the system plays the announcement. A caller who enters the queue after the announcement starts does not hear the announcement until the announcement starts again. For an integrated announcement, multiple callers can be connected to the same announcement at different times, depending on the available ports.

Example

Assume that a hunt group has the following parameters:

- The queue length is 10 calls.
- The queue warning level is 5 calls.
- The recorded announcement delay is 20 seconds.

All hunt group members are busy. A call enters the queue as the fifth call, which causes the queue warning-level lamp to light. Hunt group members see the lamp, and try to quickly complete their current calls. Meanwhile, the call waits in the queue for 20 seconds, and the system plays the recorded announcement. When a hunt group member becomes available, the first call in the queue connects to that group member. The queue warning-level lamp turns off when the number of calls in the queue falls to four.

Call Coverage for hunt groups

You can set up call coverage for a hunt group. Then if a hunt group queue is full, the system sends new calls to the coverage point.

You can specify one of the following methods to determine how the system distributes calls to members of the hunt group:

- Direct Department Dialing (DDD)
- Uniform Call Distribution (UCD)
- Circular
- Automatic Call Distribution (ACD)
- Expert Agent Selection (EAS)

If a call goes into a hunt group queue, the call stays in the queue for the Don't Answer interval. The system then redirects the call to the coverage point. A call coverage point can be another hunt group.

For more information on setting up call coverage, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Call Distribution methods for hunt group types

The system can use different types of station hunting methods to distribute calls to hunt groups. You specify the call distribution method in the **Group Type** field on the Hunt Group screen. The available values for the **Group Type** field depend on how your system is configured.

You have more call distribution options if your company acquires Automatic Call Distribution (ACD) or Expert Agent Selection (EAS). These options are available if the **ACD** and **Expert Agent Selection (EAS)** fields on the Optional Features screen are enabled. ACD and EAS distribute calls according to the workloads and the skill levels of the agents in each hunt group. You can use this type of call distribution to track call handling and monitor the efficiency of agents. When you assign ACD to a hunt group, the group is called a *split*. When you assign EAS to a hunt group, the group is called a *skill*.

For more information on EAS, see the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780. For more information on ACD and multiple call handling, see the *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*.

The following table lists the different hunt group types and how each type handles incoming calls.

Group type	Hunting method	Extra software needed
circ (Circular)	The system routes calls in a "round-robin" order. The order in which participating extensions are administered is the order in which calls are directed. The system tracks the last extension in the hunt group to which a call was connected. The next call to the hunt group is directed to the next extension on the list, regardless of idle time.	None
ddc (Direct Department Calling)	Direct Department Calling (DDC) is also known as "hot seat" distribution. The system starts with the first extension in the hunt group, and hunts for an available extension. If the first extension is busy, the system checks the second extension. If the second extension is busy, the system checks the third extension, and so on. When an extension is available, the system rings that extension to connect the call. This type of hunting provides the most equitable distribution of calls. Also, this type of hunting is required for a modem pool, data-line circuit ports, and data modules. When the group is administered as a skill, DDC is unavailable.	None

Group type	Hunting method	Extra software needed
ead-loa (Expert Agent Distribution - Least Occupied Agent)	The system hunts for the available agent who has the highest skill level, and the lowest percentage of work time since the agent logged in.	EAS and Business Advocate
ead-mia (Expert Agent Distribution - Most Idle Agent)	The system hunts for the available agent who has the highest skill level, and the longest idle time since the last call.	EAS
pad (Percent Allocation Distribution)	The system selects from a group of available agents based on a comparison of work time in the skill, and the target allocation for the skill.	
slm (Service Level Maximizer)	The system compares the current skill level for each administered skill to a user-defined call service level target. The system selects only those agents whose other skills have the least need for the service of the agent at the current time.	
ucd-loa (Uniform Call Distribution - Least Occupied Agent)	The system hunts for the agent with the lowest percentage of work time since the agent logged in.	ACD, EAS, and Avaya Business Advocate
ucd-mia (Uniform Call Distribution - Most Idle Agent)	The system hunts for the agent who has been idle the longest since the last call.	None

Hunt group extension unavailability

An extension in a hunt group is unavailable to receive calls if the hunt group member is already handling another call. The extension is unavailable even if the call is not a hunt group call, and even if the telephone is a multi-appearance telephone.

An extension also becomes unavailable if the member presses one of the following buttons:

- Hunt Group Busy, or if the member enters the Feature Access Code (FAC) for Hunt Group Busy Activate.
- Send All Calls
- Call Forwarding All Calls

Hunt Group Busy option

A hunt group member can dial the Hunt Group Busy code and then the hunt group number to make the extension of the member unavailable for calls. The extension remains unavailable until the group member dials the Hunt Group Busy deactivation code.

If the last available member of a hunt group tries to activate the Hunt Group Busy option, the following events occur:

- New calls to the hunt group receive a busy tone or go to coverage.
- The system continues to route calls that are already in the queue to the last available extension.
- When the queue is empty, the system activates Hunt Group Busy. At the last available extension, if a status lamp is associated with the **Aux Work** button, the lamp flashes until the queue is empty. When no more calls remain in the queue, Hunt Group Busy activates and if a status lamp is provided, the lamp lights steadily, but does not flash.

If an agent is an ACD split and a hunt group member, the agent in the split usually has an **AUX-work** button that also activates/deactivates Hunt Group Busy. If an agent is the last available member and pushes **AUX-work**, the lamp on the button flashes until the queue is empty. The flashing light means that the agent is still available. When the queue is empty, the lamp lights but does not flash, and Hunt Group Busy takes effect.

Using Send All Calls with hunt groups

If a station activates Send All Calls with the **Send All Calls** button, hunt group calls go in the queue, if a queue is administered. If a queue is not administered, callers get a busy treatment if Send All Calls is activated for all the agents.

If an extension is an agent in an ACD split and a hunt group member, the split agent usually has an **AUX-work** button that also activates and deactivates Hunt Group Busy. If an agent presses the **Send All Calls** button, the agent becomes unavailable for hunt group calls. The agent becomes available for hunt group calls again when the agent presses the **Send All Calls** button again.

Using Call Forwarding All Calls with hunt groups

With Call Forwarding All Calls active, an extension within a hunt group is unavailable for hunt group calls. If a forced first announcement is administered for the hunt group, callers hear the forced first announcement before the system forwards the call.

Queues for hunt groups

You can set up a queue for a hunt group. When all extensions in the group are busy, calls wait in the queue for the next available extension. You set the length of the queue to determine how many calls can wait in the queue.

If all hunt group members are unavailable or the queue is full, the system treats the call in one of the following ways:

- If the call is internal or is carried on a DID (Direct Inward Dialing), DS1 (Digital Signal Level 1), or tie trunk, the caller hears a busy tone.
- If the call is on a central office (CO) trunk, the caller hears ringing, but gets no answer.
- If the hunt group has call coverage, the system sends the call to a coverage point.

You can set up a queue warning level and an associated queue warning indicator lamp. When the queue reaches this level, the lamp lights and remains lit until the queue drops below this level. You can have one lamp for each hunt group queue. Install the lamp so that all members of the hunt group can see the lamp.

TTY hunt groups

Several laws require that "reasonable accommodation" be provided for people with disabilities. For this reason, your company might offer support for callers who use teletypewriters (TTYs).

To accommodate TTY callers, you can create a hunt group that includes agents who are equipped with a TTY. Many TTYs can connect directly to the telephone network by means of analog RJ-11 jacks. However, Avaya recommends that agents be equipped with TTYs that include an acoustic coupler that can accommodate a standard telephone handset. One reason for this recommendation is that a large proportion of TTY users are hearing impaired, but speak clearly. These people often prefer to receive calls on the TTY, and then speak in response. The call center agent must alternate between listening on the telephone and typing on the TTY. This process is easier with an acoustically coupled configuration.

Although TTY-emulation software packages are available for personal computers, few of these software packages can mix voice and TTY on the same call.

For a TTY hunt group, you can record TTY announcements and use announcements for the hunt group queue. To record announcements for TTY, follow the same procedure that you use for voice recordings from your telephone. However, instead of speaking into your telephone to record, type the announcement with the TTY.

As an alternative to creating a TTY hunt group, you can use vectors to process TTY calls. With vectors, you can allow TTY callers and voice callers to use the same telephone number. In this case, you can also record a single announcement that contains both TTY signaling and a voice recording.

Administering Hunt Groups

The following steps are part of the administration process for the Hunt Groups feature:

- Setting up hunt groups
- Changing hunt groups
- Setting up queues for hunt groups
- Adding hunt group announcements
- Setting up night service for hunt groups

This section describes:

- Any prerequisites for administering the Hunt Groups feature
- The screens that are used to administer the Hunt Groups feature
- Complete administration procedures for the Hunt Groups feature

Screens for administering Hunt Groups

Screen Name	Purpose	Fields
Announcements/ Audio Sources	Record announcements for hunt groups.	As needed
Class of Service	Change the Class of Service (COS) from the default of 1.	As needed
Coverage Paths	Set up coverage paths for hunt groups.	• **Ext** • **Type** • **COR** • **TN** • **Name** • Others as needed
Hunt Group	Add or change hunt groups.	As needed
Call Center Optional Features	To use these call distribution methods for hunt groups, ensure that **ACD** and **Expert Agent Selection (EAS)** are set to **y** .	• **ACD** • **Expert Agent Selection (EAS)**
Trunk Groups	Set up night service for hunt groups.	**Night Service Incoming Destination**

Setting up hunt groups

To set up a hunt group, you need the following information:

- The telephone number for the hunt group
- The number of people answering calls
- The call distribution method for the hunt group

To set up a hunt group:

1. Type **add hunt-group next**. Press **Enter**.

   The system displays the Hunt Group screen. The **Group Number** field is automatically filled in with the next available hunt group number.
2. In the **Group Name** field, type the name of the group.
3. In the **Group Extension** field, type the hunt group extension.
4. In the **Group Type** field, type the code for the call distribution method that you choose.
5. Press **Enter** to save your changes.

   The COS (Class of Service) default for all hunt groups is **1**. Therefore, any changes to COS 1 on the Class of Service screen changes the COS for all hunt groups. A **COS** field does not appear on the Hunt Group screen.
6. Click **Next** until you see the Group Member Assignments page of the Hunt Group screen.
7. In the **Ext** field, type the extensions of the agents that you want in the hunt group.
8. Press **Enter** to save your changes.

For more information about the other fields on the Hunt Group screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Changing hunt groups

To change a hunt group:

1. Type **change hunt-group *n***, where ***n*** is the number of the hunt group. Press **Enter**.

   The system displays the Hunt Group screen.
2. Change the necessary fields.
3. Press **Enter** to save your changes.

Setting up queues for hunt groups

You can configure Communication Manager to place hunt group calls that cannot be answered immediately in a queue.

You can administer the number of calls that can wait in the queue. You can also administer the system to provide a warning when the number of calls in the queue exceeds a certain value, and when a call waits in the queue longer than a specified number of seconds.

To set up a hunt group queue:

1. Type **change hunt-group *n***, where ***n*** is the number of the hunt group to change. Press **Enter**.

   The system displays the Hunt Group screen.

2. In the **Queue** field, type **y**.
3. In the **Queue Length** field, type the maximum number of calls that you want to wait in the queue.
4. In the **Calls Waiting Threshold** field, type the number of calls that can be in the queue before the queue status lamps flash.
5. In the **Time Warning Threshold** field, type the number of seconds for a call to wait in the queue before the queue status lamps flash.
6. Press **Enter** to save your changes.

Adding hunt group announcements

You can add recorded announcements to a hunt group queue. Use announcements to encourage callers to stay on the line, or to provide callers with information. You can define how long a call remains in the queue before the caller hears an announcement.

You assign the recorded announcements to an extension. You can type **display announcements** to find the extensions of recorded announcements that are already assigned to extensions. You can use the same announcement for more than one hunt group.

For more information on recording announcements, see the "Announcements" feature description.

To add an announcement to a hunt group queue:

1. Type **change hunt-group *n***, where ***n*** is the number of the hunt group to which you want to add the announcement. Press **Enter**.

   The system displays the Hunt Group screen.

2. In the **First Announcement Extension** field, type the extension of the announcement that you want callers to hear.

3. In the **First Announcement Delay (sec)** field, type the number of seconds that you want the caller to wait before the caller hears the first announcement. If you set the delay announcement interval to **0**, callers automatically hear the announcement immediately. This is called a forced first announcement.
4. Press **Enter** to save your changes.

Setting up night service for hunt groups

You can administer hunt group night service if you want to direct hunt group calls to a night service destination. The destination you administer can be:

- An extension
- A recorded announcement extension
- A vector directory number (VDN)
- Another hunt group extension
- An attendant

To administer night service for a hunt group:

1. Type **change hunt-group *n***, where ***n*** is the number of the hunt group for which you want to administer night service. Press **Enter**.

   The system displays the Hunt Group screen.
2. In the **Night Service Destination** field, type the night service extension to which the system routs calls.
3. Press **Enter** to save your changes.
4. Program a night service button so that members of the hunt group can activate and deactivate night service. For more information on how to program feature buttons, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Considerations for Hunt Groups

This section provides information about how the Hunt Groups feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Hunt Groups feature under all conditions.

- Members assigned to multiple hunt groups

  An extension can be a member of more than one hunt group. However, a telephone, even a multiappearance telephone, can receive only one hunt group call at a time. On a multiappearance telephone, all appearances must be idle to receive a hunt group call.

  You can assign a Coverage Incoming Call Indicator (ICI) button to a multiappearance telephone or an attendant console. When a member receives a call for the hunt group that is associated with the ICI button, the status lamp lights.

- Automatic Call Distribution (ACD) agents as hunt group members

  Do not include agents in an ACD split in non-ACD hunt groups if the agents also receive ACD split calls. The system distributes all ACD calls to agents in a split before the system distributes hunt group calls.

  When you change an ACD split to a non-ACD hunt group, each agent in the split must dial the Hunt Group Busy deactivation code to receive calls for that hunt group. If the agent has an AUX-work button, the status lamp lights when you make the change. The agent can then press the button to become available for hunt group calls.

- Hunt group for communications devices

  Members of a hunt group that is used for shared data communications must be of the same type. Thus, you can put data modules or analog modems in a hunt group, but not both. Option settings must be the same for all group members.

  A caller can still use the Data Extension button to access the associated data module, even if the module is in a hunt group. Individual data modules or modems can originate and receive calls.

- Access restrictions

  You can use Class of Restrictions (COR) to restrict an extension from receiving calls other than those calls to the hunt group to which the extension is assigned. You can also restrict extensions on Communication Manager from calling the extension of the hunt group.

- System limits

  The size of your system determines how many hunt groups you can set up, and how many extensions you can assign to each group.

- Trunk signaling

  A hunt group always has its own extension. Therefore, a caller with a telephone on Communication Manager can dial that extension to call the hunt group. If a trunk group can pass digits from the central office (CO) to Communication Manager, for example, over a DS1 trunk group, a caller can also dial a 7-digit number. The 7-digit number consists of a specified prefix and the extension of the hunt group.

  If a trunk group cannot pass digits from the CO to Communication Manager, the system can connect incoming calls to a hunt group only if the trunk group has the hunt group extension as the primary destination. This requirement includes trunk groups for incoming listed directory number (LDN) calls, international exchange calls, 800 service calls, and automatic tie-trunk calls.

Interactions for Hunt Groups

This section provides information about how the Hunt Groups feature interacts with other features in the system. Use this information to ensure that you receive the maximum benefits of the Hunt Groups feature in any feature configuration.

- Attendant Call Waiting

  Attendant Call Waiting does not work for calls that the attendant sends to a hunt group. Attendant Call Waiting does work for calls to individual hunt group members.

- Attendant Return Call

  Attendant Return Call does not work for calls that the attendant sends to a hunt group.

- Automatic Callback

  Automatic Callback does not work on calls to a hunt group.

- Automatic Call Distribution (ACD)

  ACD does not work with circular station hunting.

- Call Detail Recording (CDR)

  For each call, the system can record the associated hunt group extension or the member extension that answers.

- Internal Automatic Answer (IAA)

  Internal calls to a hunt group member are eligible for Internal Automatic Answer (IAA).

- Leave Word Calling (LWC)

  A hunt group can receive and store LWC messages. The following entities can retrieve LWC messages:

  — One member of the hunt group

  — A covering user of the group

  — A system-wide message retriever

  The message retriever must have a telephone display, and proper authorization. If the message retriever is a member of the hunt group, you can assign a remote Automatic Message Waiting lamp to the retriever. The lamp indicates when the hunt group has an LWC message.

- Night Service

  When the Night Service destination for a hunt group is another hunt group, callers hear the forced announcement of the first hunt group, if a forced first announcement is administered. The system then redirects the call to the night service hunt group.

- Priority Calling

  The system treats a priority call to a hunt group the same as a nonpriority call, except that the extension receives a distinctive three-burst ring.

- Queuing

  Queuing does not work with circular station hunting.

- Terminating Extension Group (TEG)

  A TEG cannot be a member of a hunt group.

- Vectoring

  Call vectoring does not work with circular station hunting.

Individual Attendant Access

Use the Individual Attendant Access feature to allow users to call a specific attendant console. If you have more than one attendant console, you can assign an extension to each console. Users can then dial the assigned extension to call an attendant directly.

Detailed description of Individual Attendant Access

This section provides a detailed description of the Individual Attendant Access feature.

With individual attendant extensions, you can also allow attendants to use features that an attendant group cannot use. For example, you can assign individual attendant extensions to hunt groups.

Administering Individual Attendant Access

The following steps are part of the administration process for the Individual Attendant Access feature:

- Assigning an extension to an attendant console

This section describes:

- Any prerequisites for administering the Individual Attendant Access feature
- The screens that you use to administer the Individual Attendant Access feature
- Complete administration procedures for the Individual Attendant Access feature

Prerequisites for administering Individual Attendant Access

You must complete the following actions before you can administer the Individual Attendant Access feature:

- Set up an attendant console. For information on how to set up an attendant console, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Individual Attendant Access

Screen name	Purpose	Fields
Attendant Console	Assign an extension to an attendant console.	**Extension**

Assigning an extension to an attendant console

To assign an extension to an attendant console:

1. Type **add attendant *n***, where ***n*** is a number between 1 and 28 that you want to assign to the attendant console. Press **Enter**.

   The system displays the Attendant Console screen (Figure 264: Attendant Console screen on page 1076).

Figure 264: Attendant Console screen

```
add attendant console                                          Page 1 of 4

                          ATTENDANT CONSOLE 2

        Type:                Name: operator
   Extension:               Group: 1             Auto Answer: none
Console Type:                  TN: 1             Data Module? n
        Port:                 COR: 1       Disp Client Redir? n
                              COS: 1        Display Language: english

DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS (Trunk Access Codes)
    Local Remote            Local Remote              Local Remote
 1:                      5:                        9:
 2:                      6:                       10:
 3:                      7:                       11:
 4:                      8:                       12:

HUNDREDS SELECT BUTTON ASSIGNMENTS
 1:           5:            9:           13:           17:
 2:           6:           10:           14:           18:
 3:           7:           11:           15:           19:
 4:           8:           12:           16:           20:
```

2. In the **Extension** field, type a valid extension that conforms to your dial plan.
3. Press **Enter** to save your changes.

Intercom

Use the Intercom feature to administer a button that calls a predefined extension when the button is pressed. You can also use Intercom feature to allow one user to call another user in a predefined group just by pressing a couple of buttons.

Detailed description of Intercom

This section provides a detailed description of the Intercom feature.

To control which telephones can make intercom calls to each other, you put the telephones in groups called "intercom groups." Once you add a set of telephones to the group, users can make intercom calls by administering one or both of the following feature buttons on their telephones:

- Automatic Intercom

  Users use this button to call one predefined telephone in the same intercom group. You specify the destination extension for this button.

- Dial Intercom

  Users in an intercom group use this button to call anyone else in the same group. The user lifts the handset, presses the Dial Intercom button, and then dials a 1digit or a 2 digit code for the extension.

Telephones with both of these capabilities can belong to the same intercom group.

Intercom groups

- You can create up to 32 intercom groups on one server that runs Communication Manager.
- Each group can contain up to 32 extensions in it.
- You can assign the same extension to different groups.
- Intercom calls are possible only between extensions in the same group.
- Any group member with a feature button for Dial Intercom can make an intercom call to any other member in the group.

Telephones

- You can assign any type of telephone to an intercom group. However, only multiappearance telephones can make and receive intercom calls. Single-line telephones can only receive intercom calls. Multiappearance telephones must have at least one open or available call appearance to receive intercom calls.
- An intercom call makes a unique alerting sound. If the telephone has an intercom button with a status lamp, the lamp also flashes.
- An automatic intercom connection between two telephones, even if the Class of Restriction (COR) does not allow other calls between them.

Administering Intercom

For more information, see Using Telephones as Intercoms in *Administering Avaya Aura™ Communication Manager*, 03-300509.

Interactions for Intercom

This section provides information about how the Intercom feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Intercom in any feature configuration.

- Bridged Appearances

  Bridged appearances cannot receive Intercom calls.

- Call Coverage

  Intercom calls do not follow a coverage path, unless the caller activates Go To Cover.

- Call Forwarding

  Intercom calls cannot be forwarded to a destination that is off the network.

- Call Pickup and Directed Call Pickup

  Intercom calls are not included in the call pickup alerting count.

- Data Privacy and Data Restriction

  Extensions with either of these features active cannot originate Intercom calls.

Internal Automatic Answer

Use the Internal Automatic Answer (IAA) feature to provide a convenient, hands-free way to answer internal calls to users who have multifunction stations with a speakerphone or a headphone.

Detailed description of Internal Automatic Answer

This section provides a detailed description of the Internal Automatic Answer (IAA) feature.

A user can answer an eligible call automatically if the user activates IAA at the answering telephone, and the telephone can accept an incoming call. A telephone cannot accept an incoming call if the telephone is off-hook, in the process of dialing digits, or has a call on hold.

You assign a single programmable feature button to telephones. When the user presses the IAA feature button, the button lamp lights, and the system activates IAA. When the user presses the same button again, the system deactivates IAA, and turns off the status lamp. Pressing the feature button has no effect on a an active call or a ringing call. The IAA button can be toggled on or off at any time, regardless of the state of the telephone. Using the speakerphone to place calls does not affect the state of IAA.

When IAA answers a call, the calling telephone receives a tone. The called telephone answered automatically by a telephone with IAA. The called telephone receives a tone in the form of a ring ping. The called phone then goes off-hook to automatically answer an IAA-eligible call. The system turns on the answering telephone's speaker and the microphone of the called phone.

If a user has IAA active and is currently busy on a call, or in the process of dialing digits, subsequent incoming calls are treated as if IAA were not activated.

The following internal calls are eligible for IAA:

- Station-to-station voice calls, with both telephones on the same server. These calls include redirected intraswitch calls. To use IAA for these calls, you must set the **Internal Auto-Answer of Attd-Extended/Transferred Calls** field on the Feature-Related System Parameters screen to **transferred** or **both**.
- Internal call from another node in a Distributed Communications System (DCS) configuration.These calls are from an internal, non attendant telephone on that node and includes redirected inter-DCS calls. To use IAA for these calls, you must set the **Internal Auto-Answer of Attd-Extended/Transferred Calls** field on the Feature-Related System Parameters screen to **transferred** or **both**.

- Attendant-extended external calls. You must set the **Internal Auto-Answer of Attd-Extended/Transferred Calls** field on the Feature-Related System Parameters screen to **attd-extended** or **both**.

The following calls are ineligible for IAA:

- Calls from public network trunks, including Private Central Office Line (PCOL)
- Calls from non-DCS tie trunks
- Automatic Callback calls
- Automatic Circuit Assurance calls
- Data calls
- Attendant-extended external calls if you set the **Internal Auto-Answer for Attd Extended/Transferred Calls** field on the Feature-Related System Parameters screen to **transferred** or **none**.
- Calls that the system redirects because of an overflow of Emergency Access to the Attendant calls in the queue.
- Calls when you set the **Active Station Ringing** field of the receiving telephone on the Feature-Related System Parameters screen to **continuous**.

Administering Internal Automatic Answer

This section describes the screens that you use to administer the Internal Automatic Answer (IAA) feature.

Screens for administering Internal Automatic Answer

Screen name	Purpose	Fields
Feature-Related System Parameters	Set up IAA at a system level.	**Internal Auto-Answer of Attd-Extended/Transferred Calls**

Reports for Internal Automatic Answer

The following reports provide information about the Internal Automatic Answer (IAA) feature:

- None

Considerations for Internal Automatic Answer

This section provides information about how the Internal Automatic Answer (IAA) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Internal Automatic Answer under all conditions. The following considerations apply to Internal Automatic Answer:

- Users must always deactivate IAA when the users leave the work area. If users do not deactivate IAA, the unattended station might unintentionally answer incoming calls, instead of sending all the calls.
- A 602A terminal is off-hook when the headset or the speakerphone is connected. Therefore, IAA answers a call if all other call appearances are idle.

Interactions for Internal Automatic Answer

This section provides information about how the Internal Automatic Answer (IAA) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Internal Automatic Answer in any feature configuration.

- Attendant Console

  IAA is unavailable with Attendant Console.

- Automatic Answer

  You cannot administer both IAA and Automatic Answer simultaneously on the same telephone.

- Automatic Call Distribution (ACD)

  Calls that are directed to an ACD split are eligible for IAA.

- Automatic Callback

  Callback calls by way of Automatic Callback are not answered automatically by IAA.

- Automatic Circuit Assurance (ACA)

  Calls that are generated by ACA are ineligible for IAA.

- Bridged Call Appearance - Multiappearance Telephone

  Calls that terminate on a bridged call appearance are ineligible for IAA at the bridged station, even if the bridged station has IAA active. However, IAA can be used by the principal station to answer the call.

- Bridged Call Appearance - Single-Line Telephone

  Calls that terminate to a bridged call appearance are ineligible for IAA at the bridged station, even if the bridged station has IAA active.

- Call Coverage

  If an internal call is redirected to another telephone by Call Coverage redirection criteria, that call is eligible for IAA at the redirected telephone.

  IAA does not apply to calls to the original called extension when:

  — The called telephone has Send All Calls active.

  — The calling telephone selects Go to Cover before placing the call

  Calls that are directed to a coverage answering group are ineligible for IAA.

  Note:
  If you set the coverage path for a telephone to All Calls, and that telephone activates IAA, the first coverage point hears a ring. Then the principal station automatically answers, and the coverage-simulated bridge is dropped. The coverage station rings, but is unable to answer the call, because the coverage-simulated bridge was dropped.

- Call Forwarding

  Calls to a telephone with IAA and Call Forwarding active are forwarded, and are unanswered by the station dialed.

  Note:
  If the forwarded-to telephone is internal and has IAA active, the forwarded-to telephone automatically answers the redirected call.

- Call Park

  If you are using Deluxe Paging and Call Park times out, the call returns to the originating telephone that parked the call, and is eligible for IAA.

- Call Pickup

  IAA can answer internal calls to a telephone in a Call Pickup group. If the called extension in a Call Pickup group has IAA-active, the call is automatically answered. A telephone with IAA active is not able to automatically answer calls to other telephones in its Call Pickup group.

- Conference

  IAA can answer internal conference calls.If more than one party has joins a conference call through automatic answer, the parties remain connected until the parties disconnect, or the controlling party drops the call.

- Data Call Setup

  Data calls are not eligible for IAA.

- Direct Department Calling (DDC) and Uniform Call Distribution (UCD)

  Internal calls to a member of a DDC or a member of a UCD group member are eligible for IAA.

- Distributed Communications System (DCS)

  If a call is from an internal telephone on another server or switch in a DCS configuration, that call is considered internal and is eligible for automatic answer.

- Do Not Disturb

  Do Not Disturb preempts IAA at the called telephone.

- Go to Cover

  IAA does not apply to calls to the original called extension when the calling telephone selects Go to Cover before placing a call.

- ISDN-BRI

  IAA is unavailable with ISDN-BRI telephones.

- Loudspeaker Paging - Deluxe Paging

  If Call Park times out when you are using Deluxe Paging, the call returns to the originating telephone that parked the call. Such calls are eligible for IAA.

- Ringback Queuing

  Automatic calls that are generated by Ringback Queuing are ineligible for IAA.

- Send All Calls

  IAA does not apply to calls to extensions with Send All Calls is active.

- Terminating Extension Group (TEG)

  Calls to a TEG extension are ineligible for IAA. However, calls to an individual extension are eligible.

Inter-PBX Attendant Service

Use the Inter-PBX Attendant Service (IAS) feature to allow attendants who support multiple locations, to work at a single location.

Detailed description of Inter-PBX Attendant Service

This section provides a detailed description of the Inter-PBX Attendant Service (IAS) feature.

With IAS, attendants can work at one location while the attendants support users at other locations. The system routes any incoming trunk calls that are to a user location, and any attendant-seeking calls, over tie trunks to the attendant location.

Administering Inter-PBX Attendant Service

This section contains prerequisites and the screens for administering the Inter-PBX Attendant Service (IAS) feature. The following steps are part of the administration process for the Inter-PBX Attendant Service feature:

- Enabling Inter-PBX Attendant Service

This section describes:

- Any prerequisites for administering the Inter-PBX Attendant Service
- The screens that you use to administer the Inter-PBX Attendant Service
- Complete administration procedures for the Inter-PBX Attendant Service

Prerequisites for administering Inter-PBX Attendant Service

You must complete the following actions before you can administer the Inter-PBX Attendant Service feature:

- Set up an attendant console. For information on how to set up an attendant console, see the *Administering Avaya Aura™ Communication Manager*, 03-300509.

- View the Optional Features screen, and ensure that the **Centralized Attendant** field is set to **n**. If the **Centralized Attendant** field is set to **y**, your system is not enabled for the Inter-PBX Attendant Service feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Inter-PBX Attendant Service

Screen name	Purpose	Fields
Console Parameters	Enable IAS.	• **IAS Att. Access Code** • **IAS (Branch)?** • **IAS Tie Trunk Group No.**

Enabling Inter-PBX Attendant Service

To enable Inter-PBX Attendant Service:

1. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 265: Console Parameters on page 1086).

Figure 265: Console Parameters

```
change console-parameters                                    Page   1 of 4
                            CONSOLE PARAMETERS
         Attendant Group Name: OPERATOR
                          COS: 0                                   COR: 0
       Calls in Queue Warning: 5                      Attendant Lockout? y
        Ext Alert Port (TAAS):
                          CAS: none
                                                Night Service Act. Ext.:
                IAS (Branch)? y                 IAS Tie Trunk Group No.:
          IAS Att. Access Code:                   Alternate FRL Station:
               Backup Alerting? n          DID-LDN Only to LDN Night Ext? n
      Attendant Vectoring VDN:
```

2. In the **IAS Att. Access Code** field, type the extension of the attendant group at the main server that runs Communication Manager.

Note:
You must type **y** in this field if the **IAS (Branch)?** field is set to **y**.

The system displays the **IAS Att. Access Code** field only if the **Centralized Attendant** field on the **Optional** Features screen is set to **n**.

3. In the **IAS (Branch)?** field, type **y**.

   The system displays this field only if the **Centralized Attendant** field on the **Optional** Features screen is set to **n**.

4. In the **IAS Tie Trunk Group No.** field, type the number of the tie trunk group to the main IAS location. Valid entries for the DEFINITY R, CSE, and SI are **1** through **666**. Valid entries for the S8300 Server, IP-PNC, and S8700 Multi-Connect are **1** through **2000**.

   Note:
   You must complete this field if the **IAS (Branch)?** field is set to **y**.

   The system displays this field only if the **Centralized Attendant** field on the **Optional** Features screen is set to **n**.

5. Press **Enter** to save your changes.

Reports for Inter-PBX Attendant Service

The following reports provide information about the Inter-PBX Attendant Service (IAS) feature:

- None

Considerations for Inter-PBX Attendant Service

This section provides information about how the Inter-PBX Attendant Service (IAS) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Inter-PBX Attendant Service under all conditions. The following considerations apply to Inter-PBX Attendant Service:

- None

Interactions for Inter-PBX Attendant Service

This section provides information about how the Inter-PBX Attendant Service (IAS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Inter-PBX Attendant Service in any feature configuration.

- Centralized Attendant Service

  IAS does not work with Centralized Attendant Service

ISDN Service

Use the Integrated Services Digital Network (ISDN) Service feature to provide a message-oriented signaling method that allows information to be sent along with a call. The ISDN Service feature also gives you access to a variety of public and private network services and facilities.

The ISDN standard consists of Layers 1, 2, and 3 of the Open System Interconnect (OSI) model. Communication Manager can be connected to an ISDN by way of the standard frame formats: Basic Rate Interface (BRI) and the Primary Rate Interface (PRI).

Detailed description of ISDN Service

This section provides a detailed description of the Integrated Services Digital Network (ISDN) Service feature.

The ISDN Service feature provides end-to-end digital connections and uses a high-speed interface that provides service-independent access to switched services. Through internationally accepted standard interfaces, an ISDN provides circuit or packet-switched connections within a network, and can link to other ISDN-supported interfaces to provide national and international digital connections.

Note:
This feature description does not contain procedures for working with ISDN trunk groups. Due to the complexity of ISDN technology and the potential consequences of errors, ask your Avaya representative to help you in planning, installing, and administering ISDN trunks.

ISDN supports the following features:

- Call-by-Call Service Selection (CBC)
- Distributed Communications System (DCS). (Only ISDN-PRI supports DCS+ and DCS with Rerouting)
- Electronic Tandem Networks (ETN)
- Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS), but only with ISDN-PRI.
- Generalized Route Selection (GRS)
- Call Identification Display - Calling Party Number (CPN) and Billing Number (BN)
- Administered Connections and Access Endpoints

- Interworking, or the mixture of ISDN and non-ISDN trunks and stations
- Wideband Switching (H0, H11, H12, and NxDS0, but only with ISDN-PRI.
- QSIG Multivendor Connectivity
- Lookahead Interflow
- Lookahead Routing
- Usage Allocation

Transmission rate and protocols

In ISDN-PRI, the transmission standard for Layer 1 (the physical layer) is either DS1 T1 or E1. The DS1 T1 (used in North America and Japan) is a digital-transmission standard that carries traffic at the rate of 1.544 Mbps, and the E1 (used in Europe) carries traffic at a rate of 2.048 Mbps. The "D" (data) channel multiplexes signaling messages for the "B" (bearer) channels carrying voice or data. In a T1, when a D-channel is present, it occupies Channel 24. In an E1, when a D-channel is present, it occupies channel 16.

Communication Manager offers several administrable protocols, each of which provides a different set of ISDN services. The following combination of services, including but not limited to Basic Call, Basic Supplementary Services, Supplementary Services with Rerouting, Display, and QSIG Networking are supported on the ISDN-PRI interface. Available services outside the United States vary from country to country.

With ISDN, Communication Manager interfaces with a wide range of other products including servers, network switches, and host computers. These products include earlier releases of servers running Communication Manager, public network switches (for example, AT&T 4ESS, Lucent 5ESS, and Northern Telecom DMS250), and other products adhering to the ISDN signaling protocol.

Figure 266: ISDN network configuration on page 1091 shows an example of how ISDN is used in private and public network configurations.For example, ISDN can be used to connect a switch to a public-switched network, to other switches, and to computers.

Figure 266: ISDN network configuration

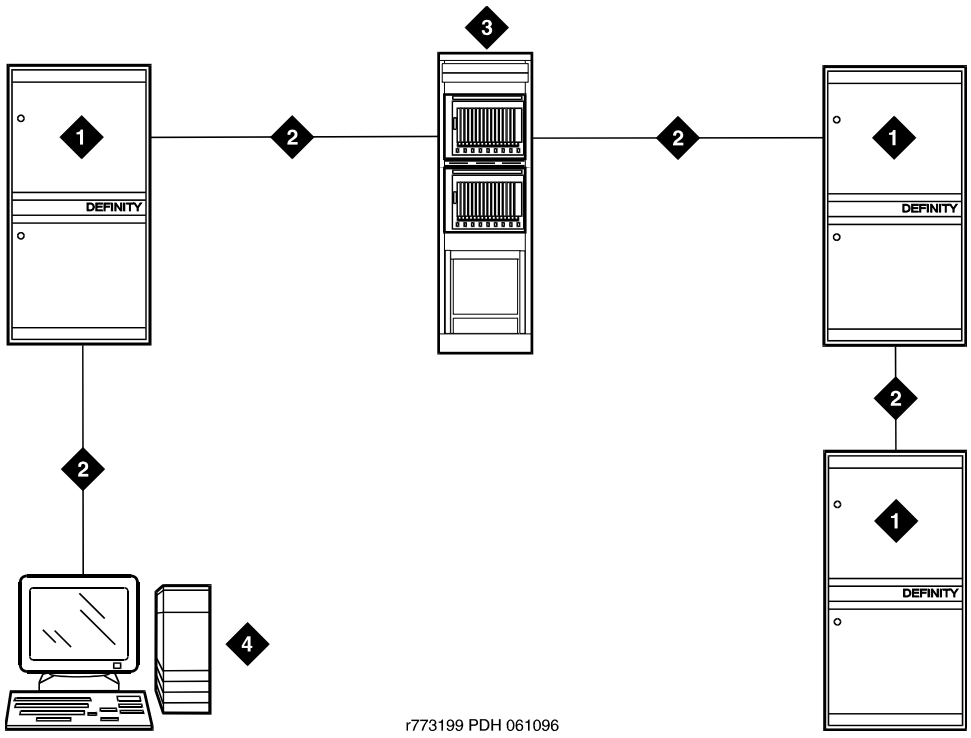


Figure notes:

1. Avaya Server
2. ISDN trunk
3. Public switched network
4. Host computer

AT&T Switched Network protocol

Communication Manager supports the AT&T Switched Network Protocol described in the TR41449 (for 4ESS to common carrier) and TR41459 (for 5ESS to CO) ISDN protocol standards as defined by AT&T. This protocol is used when the DS1 circuit pack is administered for Country Code 1, Protocol Version a. The AT&T Switched Network provides you with the following services.

Access to AT&T Switched Network Services

ISDN provides access to AT&T Switched Network Services. The definition of the **Service Type** field on the ISDN Trunk Group screen includes a table that outlines these switched-network services. An ISDN trunk group may be dedicated to a particular feature. Alternately, an ISDN call-by-call trunk group may provide access to several features.

Call Identification Display

ISDN Call Identification Display provides a transparent name and number display for all display-equipped telephones within an ISDN network. The feature is transparent in that the same information can be provided at all ISDN facilities. Telephones using this feature should be digital telephones with a 40-character alphanumeric display. The Merlin hybrid sets with 32-character displays (7315H and 7317H) also support this feature.

ISDN Call Identification Display is provided in addition to the normal Telephone Display and Attendant Display features when the network supports end-to-end ISDN connectivity. When both ISDN and DCS display information are received, either the DCS or ISDN call identification information can be displayed. If only ISDN display information is received, information displays in ISDN format.

The display fields that may be used for ISDN are **Name**, **Number**, **Miscellaneous Call Identification**, and **Reason for Call Redirection**. The display information varies, depending on the type of call, how the call is handled (for example, whether it is redirected or not), and the information is available on the call.

CPN/BN to Host Call Identification

The CPN/BN to Host Call Identification enables CPN and BN information to be passed from Communication Manager to the ISDN Gateway, so that the ISDN Gateway can forward the information to a host for data-screen delivery to agents in an ACD split.

By delivering call-identification information such as CPN/BN and additional Communication Manager information such as the answering-agent's extension to an adjunct network (ISDN Gateway), the adjunct automatically delivers data screens to agents for new calls and call transfers.

Figure 267: CPN- and BN-to-host configuration on page 1093 shows a simplified diagram of a CPN- and BN-to-host arrangement. The ISDN Gateway is a UNIX or MS-DOS computer connected to Communication Manager on one side and to a host computer on the other side. The media server connection is over a synchronous interface with BX.25 protocol.

Figure 267: CPN- and BN-to-host configuration

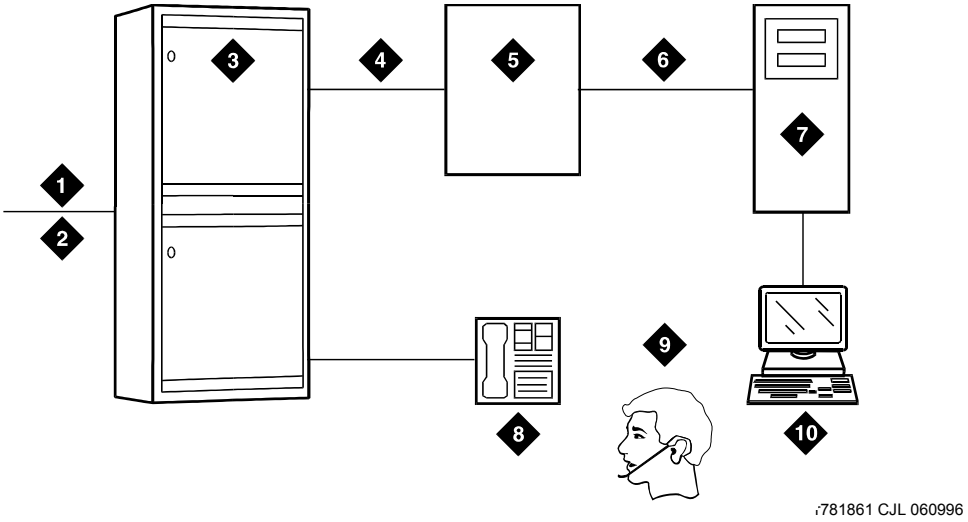


Figure notes:

1. ISDN trunk
2. SID/ANI
3. Avaya Server
4. BX.25
5. ISDN Gateway
6. Existing interface
7. Host computer
8. Telephone
9. ACD agent position
10. Data terminal

Private network services

In addition to providing access to switched-public networks, ISDN provides private-network services by connecting Communication Manager in an ETN, DCS, or QSIG Network. This gives you more efficient private networks that support new integrated voice and data services. ETN, DCS, and QSIG networking services are provided as follows.

ETN services

Avaya S8*XXX* Servers that function as tandem nodes in an ETN can be interconnected using DS1 trunking facilities with ISDN. All signaling between the tandem switches is done with ISDN D-channel and normal ISDN protocol. The ISDN can also be used to connect ETN tandem and main servers or switches. In this case, the main server or switch collects all of the address digits from local users as well as users at other satellite and tributary switches, and originates a call over ISDN to the tandem server or switch.

Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) are used with ISDN and DS1 trunking facilities to access ETN facilities. AAR and ARS are used to collect the dialing information for the call that is originated from the main server or switch.

DCS services

ISDN-PRI facilities can be used in a DCS arrangement whenever tie trunks are used to connect the DCS nodes. Most DCS features are not affected by ISDN-PRI. However, there is a minor impact on a few of the DCS features, as far as the functions that the local and remote media servers or switches perform.

QSIG services

QSIG networking provides compliance to the International Organization for Standardization (ISO) ISDN private-networking specifications. The QSIG Networking platform is supported over the ISDN Basic Call setup protocol. Communication Manager supports QSIG Supplementary Services.

Wideband Switching (ISDN-PRI only)

Wideband Switching provides support for services that require large bandwidth, such as high-speed video conferencing. Wideband also supports multiple channel calls end-to-end. These services have traditionally been handled by dedicated facilities. With Wideband Switching, dedicated facilities are no longer a requirement for these large bandwidth services.

Call-by-Call Service Selection

Call-by-Call Service Selection allows the same ISDN trunk group to carry calls to a variety of services or facilities. Embodied in this feature is the ability to allocate usage. It provides significant flexibility for creating user-defined incoming and outgoing services and is used on any ISDN trunk group.

Access to Software Defined Data Network

With ISDN, the SDDN service may be accessed. SDDN provides virtual private-line connectivity by way of the switched public network. The services provided by SDDN include voice, data, and video applications. SDDN services complement the ISDN voice services.

Access to Switched Digital International

Switched Digital International (SDI) provides 64 kbps of unrestricted connectivity to international locations by way of the AT&T Switched Network. It is also the backbone for the AT&T International ISDN network. SDI complements the ACCUNET digital service already available to United States locations. This service can be accessed using Call-by-Call Service Selection. SDI provides economical high-speed data transfer to international locations.

National ISDN-2 services

Communication Manager supports National ISDN-2 (NI-2), which offers many of the same services as the AT&T Switched Network protocol. The NI-2 protocol is used when the DS1 circuit pack is administered for Country Code 1, Protocol Version b.

NI-2 provides users with the following services:

- Calling Line Identification
- Non-Facility Associated Signaling (ISDN-PRI only)
- D-Channel Backup, but with ISDN-PRI only
- Wideband Switching, but with ISDN-PRI only
- Call-by-Call Service Selection

Calling Line Identification

Calling Line Identification for NI-2 is essentially CPN identification, as previously described.

Non-Facility Associated Signaling (ISDN-PRI only)

Non-Facility Associated Signaling (NFAS) allows an ISDN-PRI T1 or E1 Interface D-channel (signaling channel) to convey signaling information for B-channels (voice and data) on ISDN-PRI T1 or E1 facilities other than the facility that contains the D-channel.

D-Channel Backup (ISDN-PRI only)

D-Channel Backup is provided to improve reliability in the event of a signaling-link failure.

Wideband Switching (ISDN-PRI only)

Wideband Switching for NI-2 is essentially the same as that of the AT&T Switched Network ISDN-PRI protocol.

Call-by-Call Service Selection

Call-by-Call Service Selection for NI-2 is essentially the same as that for the AT&T Switched Network ISDN-PRI protocol.

ISDN interworking

ISDN interworking allows calls to use a combination of both ISDN and non-ISDN trunking and station facilities. A non-ISDN trunking facility is any trunk facility supported by the system that does not use the ITU-T recommended Q.931 message set for signaling. Non-ISDN trunking facilities include facilities such as analog trunks, AVD DS1 trunks, and DS1 trunks with bit-oriented signaling (robbed-bit or common channel).

Communication Manager supports the conversion of ISDN signaling to non-ISDN in-band signaling and the conversion of non-ISDN in-band signaling to ISDN signaling for interworking purposes.

A mixture of ISDN and non-ISDN signaling is required in order to provide end-to-end signaling when using different types of trunk or station facilities on a call. Figure 268: ISDN and non-ISDN interworking on page 1096 shows an example of interworking.

Figure 268: ISDN and non-ISDN interworking

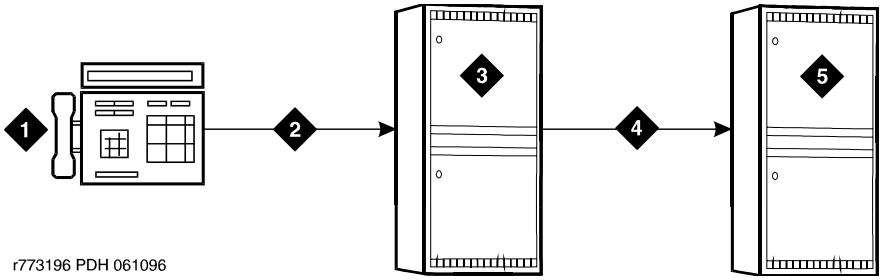


Figure notes:

1. Call from network to system B
2. ISDN trunk
3. System A
4. Non-ISDN trunk
5. System B

In this example, a call for someone at Switch B comes into Switch A. Interworking allows the ISDN signaling of the call to be converted at Switch A to non-ISDN in-band signaling before the call forwards to Switch B. Even though the call comes into Switch A on an ISDN trunk, Switch A can send the call to Switch B over a non-ISDN trunk by converting the signaling information.

The system provides accurate CDR billing information on calls that are not interworked. Accuracy of CDR billing information on interworked calls is equivalent to the accuracy provided by the public network.

Communication Manager supports sending a non-ISDN trunk name as the connected name. Therefore, a non-ISDN trunk name can be sent as the connected name even when a call starts out as an ISDN call but is interworked over non-ISDN trunks.

Call Identification Display

Two types of identification numbers are provided with ISDN and may be used in the various types of displays used with ISDN. The two types of identification numbers are as follows:

- Calling Party Number (CPN): A 0-15 digit DDD number associated with a specific station. When a system user makes a call that uses ISDN, that user's CPN is provided by the system for ISDN. ISDN public-unknown numbering or ISDN private numbering screens are administered to create a 0-15 digit CPN from a local station number.
- Billing Number (BN): The calling party's billing number, which is provided to an inter-exchange network by way of Equal Access or CAMA. This number is stored at either a local or network switch. If a customer is connected directly to the AT&T Switched Network, the BN is the customer's billing number stored in that network. If the CPN is not provided on an incoming ISDN call, the network uses the BN for the station identification number.

The following types of display information are provided with ISDN:

- Calling party's number

  The calling party's number appears on the called party's display. This number is provided only if the outgoing ISDN trunk group is administered to send the CPN, and if ISDN public-unknown numbering or ISDN private numbering screens are administered to create a CPN. On calls incoming to a system, the network may provide either the CPN or BN as the calling party's number. Extensions and 12-digit international numbers display without dashes. Dashes are only used for 7-digit and 10-digit numbers when North American Area Code is enabled on the Dial Plan screen.

- Calling party's name

  The calling party's name appears on the called party's display. On calls generated from a DEFINITY server, the caller's name is provided if the ISDN trunk group is administered to send the name to the network. On calls incoming to a DEFINITY server, the (public or private) network may provide the caller's name. If the caller's name is not available, the called party's display shows "CALL FROM" instead, followed by the calling party's number (if available).

- Connected party's number

  The connected party's number appears on the caller's display. On calls generated from a DEFINITY server, callers' displays may show the digits dialed as the call is made. If the (public or private) ISDN network provides the connected party's number, the calling party's display is updated to show the connected party's number. The format of the connected party's number is the same as that of the calling party's number described previously on calls incoming to a DEFINITY server. The 0-15 digit number of the party who answers the call is provided to the ISDN network only if the incoming ISDN trunk group is administered to send connected number to the network and ISDN public-unknown numbering or ISDN private numbering screens are administered to create a CPN.

Note:
The connected party may be the party actually called, in the event the call is transferred before the connected party answers the call.

- Connected party's name

  The connected party's name appears on the calling party's display. On calls generated from a DEFINITY server, the (public or private) ISDN network may provide the connected party's name to the Communication Manager, when the call is answered. If the connected party's name is not available, the calling party's display shows ANSWERED BY, followed by the connected party's number (if available).

  On calls incoming to a DEFINITY server, the connected party's name is provided if the incoming ISDN trunk group is administered to send the name to the network.

Depending on how the media servers or switches that are involved in a call are configured, parties may see none, some, or all the information described above.

Displays for redirected calls

Features such as Call Coverage, Call Forwarding All Calls, Bridged Call Appearance, or Call Pickup redirect calls from the called party's extension to some other destination. Once the redirected call has been connected at its new destination, the displays for the calling, called, and connected parties are as follows:

- Calling party display

  a= CONNECTED NAME CONNECTED NUM MISCID

- Called party display

  This is the display of the party the caller originally dialed. If this party bridges onto the redirected call after it has been answered, they see:

  a= CONFERENCE 2

  In this situation, the connected party's display (see below) shows the same information. The calling party's display is also updated if the calling and called parties are on the same server running Communication Manager.

- Connected party display

  The connected party is the party who answers the redirected call.

  a= CALLING ID to CALLED ID R

  The R indicates the reason for redirection. The CALLING ID and the CALLED ID may be the name or the number, depending on the information received from the far end.

Displays for conference calls

Both terminal and attendant conference calls are identified as calls with "n" number of conferees. This display information generates locally and does not change the display shown by another server. If the conference call eventually drops back to a two-party call, the original display information is restored. However, when two DCS and/or ISDN calls (or any possible combination of each) are conferenced and revert to a two-party call, the trunk group of the remaining call displays.

Displays for calls to hunt groups

On ISDN calls to a hunt group extension, the caller's display identifies either the name of the hunt group or the name of the group member who answers the call, depending on hunt group administration.

Displays for calls to Terminating Extension Groups

On ISDN calls to a Terminating Extension Group (TEG), the caller's display identifies either the group or the group member who answers the call, depending on administration.

Caller Information Forwarding

With CINFO you can use a vector *collect digits* step to retrieve caller entered digits (ced) and customer database-provided digits (cdpd) supplied by the network in an incoming call's ISDN SET UP message. ISDN is required if the CINFO comes from the network.

Facilities restriction level and traveling class mark

The traveling class mark (TCM) used to pass on the originating facilities's restriction level (FRL) is sent by ISDN facilities in the SETUP message only if the trunk services type is tandem.

Information Indicator Digits (II-digits)

With II-digits you can make vector-routing decisions based on the type of the originating line. II-digits are provided for an incoming call by ISDN-PRI. It is a generally available ISDN AT&T Network service.

Malicious Call Trace

ISDN calling number identification is sent when Malicious Call Trace (MCT) notification is activated on an ISDN trunk.

Multiple Subscriber Number - Limited

The ISDN standard Multiple Subscriber Number (MSN) feature lets you assign multiple extensions to a single BRI endpoint. A side effect of supporting the NT interface is the MSN feature works with BRI endpoints allowing the Channel ID IE to be encoded as "preferred." The endpoint must be administered as the far end of an NT-side ISDN-BRI trunk group. Also, you must use the Uniform Dial Plan (UDP) feature to assign the desired extensions to the "node" at the far end of the trunk group.

Overlap Sending

You can administer overlap sending on AAR and ARS calls routed over ISDN trunk groups. This allows you to send and receive digits one digit at a time instead of enbloc. (With enbloc, digits are not sent until the entire group of digits is received).

Interworking between TGU/TGE trunks and ISDN (Italy)

This modifies ISDN messaging operations in systems that use TGE/TGU trunks to network satellite servers or switches. Messaging from Communication Manager provides appropriate ringback or busy tone to the calling party.

Administering ISDN Service

This section describes the screens that you use to administer the ISDN Service feature.

Screens for administering ISDN Service

Screen name	Purpose	Fields
Access Endpoint	Administer ISDN Service.	• **Access Endpoints** • **Wideband Access Endpoint**
Trunk Groups	Administer incoming calls and trunk groups usage and allocation.	All

Screen name	Purpose	Fields
ISDN Numbering - Private	Administer private numbering plans.	All
ISDN Numbering - Public/ Unknown	Administer ISDN call identification displays.	All

Interactions for ISDN Service

This section provides information about how the ISDN Service feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of ISDN Service in any feature configuration.

- Australia Malicious Call Trace (MCT)

  Communication Manager with a BRI connection to the Australian public network can notify the network if a user in a private network invokes the MCT feature. This service works on Australian national connections.

- Direct Inward Dialing (DID)

  Some public network operators may not offer full DID service on BRI trunks, but instead may offer the BRI equivalent, which typically is called MSN. This is the case if the public network treats the BRI as an endpoint interface rather than a trunk group interface. In such a case, the network only routes up to 10 public numbers to a particular pair of BRI trunks. The network may not let calls overflow from one BRI trunk to another.

- D-Channel Backup

  D-Channel Backup is not supported on BRI connections.

- Distributed Communications System

  If both DCS and ISDN features are provided over the same facility with a DEFINITY server, DCS displays generally override ISDN displays. However, with Communication Manager, the ISDN connected name and number can override the DCS called name and number if the **Display Connected Name/Number for ISDN DCS Calls** field is **y** on the Feature-Related System Parameters screen.

  BRI trunks support DCS if using a BX.25 link to transport the DCS messages. DCS+, also known as DCS Over ISDN D-Channel, according to the AT&T protocol, is not supported on BRI trunks.

- Facility Test Calls

  Neither BRI or PRI trunks support Facility Test Calls.

- France VN4 Protocol

  The France national VN4 protocol is supported on BRI trunks as ETSI.

- Generalized Route Selection

  BRI trunks are capable of carrying 56Kbps or 64Kbps data calls. The link coding that restricts certain PRI trunks to 56Kbps only does not apply to BRI trunks.

- German 1TR6 Protocol

  The German national 1TR6 protocol is not supported over BRI trunks.

- Message Sequence Tracer

  ISDN-BRI trunks support Message Sequence Tracer. However, certain filtering capabilities available for PRI trunks are not available. Specifically, it is not possible to filter BRI trunk messages based on incoming/outgoing calling/called number.

- Network Access - Public (LEC/AT&T/Other Carriers)

  Public network access using BRI trunks is available but only in those countries that support point-to-point BRI connections. In the U.S., BRI access is offered only by the Local Exchange Carriers and not by Interexchange Carriers.

- Network Access - Private Premises Based

  Full support for private-network connections using BRI trunks is available.

- Non-Facility Associated Signaling

  Non-Facility Associated Signaling is not supported on BRI connections.

- Temporary Signaling Connections

  Communication Manager does not support Temporary Signaling Connections according to the AT&T protocol on BRI trunk interfaces. Only the QSIG NCA TSC protocol is supported on these interfaces

- Wideband Switching (NxDS0)

  Communication Manager does not support wideband switching on BRI connections.

Last Number Dialed

Use the Last Number Dialed feature to automatically redial the last telephone number that was dialed from the telephone, or from a bridged appearance of the telephone.

Detailed description of Last Number Dialed

This section provides a detailed description of the Last Number Dialed feature.

With the Last Number Dialed feature, users can to automatically redial the last telephone number that was dialed from the telephone, or from a bridged appearance of the telephone.

The system saves the first 24 digits of the last telephone number that was dialed. The system saves the digits for calls that the user places with either manual dialing or Abbreviated Dialing. When a user presses the Last Number Dialed button, or dials the Feature Access Code (FAC) for Last Number Dialed, the system places the call again.

Administering Last Number Dialed

This section provides the screens that you need to administer the Last Number Dialed feature:

Screens for administering Last Number Dialed

Screen name	Purpose	Fields
Attendant Console	Assign the **last-numb** feature button to an attendant console.	Any available button field in the **Feature Button Assignments** area
Feature Access Code (FAC)	Assign a FAC for Last Number Dialed.	**Last Number Dialed Access Code**
Station - multiappearance	Assign the **last-numb** feature button for a user.	Any available button field in the **Button Assignments** area

Considerations for Last Number Dialed

This section provides information about how the Last Number Dialed feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Last Number Dialed under all conditions. The following considerations apply to Last Number Dialed:

- When the user presses the last number dialed button, the system outpulses any special characters that are stored in the Abbreviated Dialing button that was used to place the previous call. Such characters include Pause, Wait, Mark, and Suppress.
- Any delays that a user might encounter when the user dials the call manually, are not repeated when the user uses the Last Number Dialed feature.
- The system does not save Last Number Dialed information to disk, tape, or flash card. The system never saves manually dialed end-to-end, signaling digits.
- A user can enter a partial number, hang up, and use Last Number Dialed, and manually enter the remaining digits. If the user calls from a display telephone, the system does not display the digits that the user enters manually. However, the system completes the call.

Interactions for Last Number Dialed

This section provides information about how the Last Number Dialed feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Last Number Dialed in any feature configuration.

- Abbreviated Dialing

  If the previously called number is in an Abbreviated Dialing privileged list, and the Class of Restriction (COR) of the user prevents the user from dialing the number, the system uses Intercept Treatment when the user presses Last Number Dialed. To redial the number, the user must again use the Abbreviated Dialing privileged list.

- Automatic Callback

  Users can use Automatic Callback after the users use Last Number Dialed on a call to an internal telephone.

- Bridged Call Appearance

  Last Number Dialed causes the last number that was dialed from a telephone, or a bridged appearance of the telephone, to be redialed.

- Centralized Attendant Service (CAS)

  If a CAS attendant attempts to extend a call with Last Number Dialed, the system does not complete the call.

Leave Word Calling

Use the Leave Word Calling (LWC) feature to allow internal system users to leave a short pre-programmed message for other internal users. When the message is stored, the Automatic Message Waiting lamp lights on the called telephone. Users can retrieve LWC messages on a telephone display, Voice Messaging Retrieval, or the AUDIX system. Messages can be retrieved in English, French, Italian, Spanish, or a user-defined language.

Detailed description of Leave Word Calling

This section provides a detailed description of the Leave Word Calling (LWC) feature.

LWC electronically stores a standard message. For example:

CARTER, ANN 2/7 10:45a 2 CALL 3124

This message means that Ann Carter called two times, the last time on the morning of February 7 at 10:45 a.m. She wants a return call to extension 3124.

When the system receives identical messages, the system updates only the date and the time, and number of messages. If nine or more identical messages accumulate, the count remains at nine, and the system updates only the date and time.

Messages can be stored by calling users, called users, and covering users as follows:

A caller who leaves a LWC message can cancel that message, if the message was not already retrieved. To cancel the message, the calling user lifts the handset, presses LWC Cancel or dials the access code, and then dials the extension of the called party.

The system can indicate that one telephone received a LWC message on a second telephone. The system lights a remote Automatic Message Waiting lamp at the remote telephone and the Automatic Message Waiting lamp lights at the called voice terminal. The Remote Automatic Message Waiting lamp is a status lamp associated with a button assigned for this purpose.Thus, the lamp on an assistant’s telephone can light when an executive receives a LWC message. If the executive calls to retrieve messages, the assistant knows at a glance if any messages were left.

Users without Voice Terminal Display can have their messages retrieved by a system-wide message retriever or by covering users in their Call Coverage path. They can also use Voice Message Retrieval.

The system restricts unauthorized users from displaying, canceling, or deleting messages. The Lock capability restricts a voice terminal and the Unlock function releases the restriction. To activate Lock, the users dial a system-wide access code. They cancel Lock by first dialing a system-wide access code and then an Unlock security code unique to the voice terminal. These functions apply only to the voice terminal where the function is active. You can assign a status lamp to show the lock status of the voice terminal.

Voice synthesis

Avaya solutions can also provide voice synthesis for LWC, depending on which voice-synthesis circuit pack is installed. This voice synthesis can be either in English or Italian.

Users without telephone display can have their messages retrieved by a system-wide message retriever or by covering users in their Call Coverage path. They can also use Voice Message Retrieval.

With the Leave Word Calling Log External Calls capability, the system can monitor when an external call is not answered. The server keeps a record of as many as 15 calls, provided that the caller identification is available, and the message lamp on the telephone lights. The displays on the telephone shows the names and numbers of unsuccessful callers.

End-user procedures for Leave Word Calling

Calling user

1. Press the **LWC** button or dial the LWC access code.
2. Dial the desired number.
3. Before the call is answered, if you are a multiappearance voice-terminal user, press **LWC**. If you are a single-line voice-terminal user, press Recall and dial the access code.
4. After the call is answered, press **LWC** or **Recall** and dial the access code.

Called user

1. The user answers the call.
2. The called user presses LWC to leave a message for the calling user to return the call.
3. A called user can store an LWC message by dialing the LWC access code only if the called user has an analog voice terminal.

Covering user

A covering user can be through Call Coverage, Call Pickup, or Call Forwarding All Calls.

1. The covering user answers the call.
2. The covering user presses Coverage Callback to store a message for the called user that tells them to return a call the calling user.
3. After answering the call, the covering user presses **LWC** to leave a call-me message for the originally called user.

In addition, a user that was placed on hold can activate LWC and leave a message for the holding user to place a return call.

Considerations for Leave Word Calling

This section provides information about how the Leave Word Calling (LWC) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Leave Word Calling feature under all conditions. The following considerations apply to the Leave Word Calling feature:

- You can administer up to 10 telephones, or nine telephones and the attendant console group as system-wide message retrievers.
- If the stored-message level reaches 95% of capacity, the status lamps that are associated with all Coverage Message Retrieval buttons in the system flash. These lamps continue to flash until the stored-message level falls below 85%. Authorized retrievers can selectively delete messages to gain storage space. The system does not automatically purge old messages.
- LWC messages cannot be stored, canceled, or retrieved for Vector Directory Number extensions.

Interactions for Leave Word Calling

This section provides information about how the Leave Word Calling (LWC) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Leave Word Calling in any feature configuration.

- AUDIX Interface

  LWC Cancel cannot be used to cancel an AUDIX message.

- Bridged Call Appearance

  A LWC message that is left by a user on a bridged call appearance leaves a message for the called party to call the primary extension for the bridged call appearance. When a user calls a primary extension and activates LWC, the message is left for the primary extension, even if the call was answered at a bridged call appearance.

- Call Coverage

  You can use LWC with or without Call Coverage. However, the two features complement each other. LWC provides the Coverage Callback option. Also, a caller can activate LWC for the called party even if the call was answered by a covering user.

- Centralized Attendant Service (CAS)

  LWC Message Retrieval does not work with CAS.

- Conference

  A member of a conference call cannot activate LWC because the user cannot be uniquely identified. After LWC is activated for a party on a conference or transfer, the origination of the conference or the transfer cannot press Conference/Transfer a second time to return to the original call. The originator must select the call appearance button to return to the previously held call.

- Distributed Communications System (DCS)

  LWC works with DCS, but only for 4- digit and 5-digit extension dial plans. LWC works with QSIG for all dial plans of 3- through 7-digits.

- Expert Agent Selection (EAS)

  When an EAS agent is logged into a telephone, the agent can only retrieve LWC messages that are left for the login ID of the agent. To retrieve LWC messages that are left for that telephone, the agent must log out.

  When an EAS agent is logged into a telephone, the Message lamp of the telephone defaults to tracking the status of LWC messages waiting for the telephone. However, you can assign the Message lamp to track the status of LWC messages waiting for the login ID of the agent.

- Message Waiting Indicator (MWI)

  As QSIG does not specify a standard way to light the MWI lamp upon receipt of an LWC message, Avaya's implementation requires systems running Communication Manager in order to work properly.

- Vector Directory Number (VDN)

  LWC messages cannot be stored, cancelled, or retrieved through VDN extensions.

Line Lockout

Use the Line Lockout feature to remove a user with a single-line telephone from service when the user does not hang up after the user receives dial tone or intercept tone.

Detailed description of Line Lockout

This section provides a detailed description of the Line Lockout feature.

Lockout occurs when:

- A user does not hang up after the other party on a call disconnects.
  - The user receives the dial tone for 10 seconds, and then receives the intercept tone for the interval that you administer.
  - You can administer the system to play a special howler tone before the system takes the telephone out of service.
  - If the handset remains off-hook, the system takes the telephone out of service.
- A user pauses for 10 seconds between digits when the user dials numbers.
  - The user receives intercept tone for 30 seconds.
  - If the handset remains off-hook, the system takes the telephone out of service.

The telephone remains out of service until the user hangs up.

Administering Line Lockout

This section describes the screens that you use to administer Line Lockout.

Screens for administering Line Lockout

Screen name	Purpose	Fields
Feature-Related System Parameters	Specify the number of seconds that the system waits before the system removes the telephone of the user from service, after the system generates the warning tone.	**Line Intercept Tone Timer**
	Specify the tone that the system generates for the last user on a call, until the user hangs up or the system generates the tone for 45 seconds.	**Station Tone Forward Disconnect**
	Specify the number of seconds that the system allows a telephone with an Off-Hook Class of Service (COS) to remain off-hook before the system sends an emergency call to the attendant.	**Time Before Off-hook Alert**
System Parameters Country-Options	Enable the system to disconnect calls that are unanswered	**Disconnect on No Answer by Call Type**
	Enable the system to generate howler tone for users, before the system removes the telephone of the user from service.	**Howler Tone After Busy**

Reports for Line Lockout

The following reports provide information about the Line Lockout feature:

- None

Considerations for Line Lockout

This section provides information about how the Line Lockout feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Line Lockout under all conditions. The following considerations apply to Line Lockout:

- The out-of-service condition that Line Lockout provides does not tie up switching facilities.
- Line Lockout does not apply to multiappearance telephones.

Listed Directory Number

Use the Listed Directory Numbers (LDN) feature to allow outside callers to access your attendant group.

Listed Directory Number supports the following capabilities:

- Attendant group access through incoming Direct Inward Dialing (DID) trunks
- Attendant group access through incoming central office (CO) and foreign exchange (FX) trunks

Detailed description of Listed Directory Number

This section provides a detailed description of the Listed Directory Number (LDN) feature.

The system routes both incoming Direct Inward Dialing (DID) calls and incoming foreign exchange (FX) and central office (CO) calls to an attendant group, based on how you administer the trunks.

Incoming DID trunk calls to the attendant group

incoming DID calls only to an extension. The LDN feature allows you to assign one or more extensions to an attendant group. The system uses the LDN extension, or extensions, to route DID calls to an attendant group.

Incoming FX and CO trunk calls to the attendant group

Incoming FX and CO trunks calls can terminate at an attendant group. You can also administer your system to terminate an incoming FX or CO trunk to an:

- Attendant group

  If you decide to terminate the call at an attendant group, the system processes the call as an LDN call.

- Extension

  The extension can be a vector directory number (VDN), an Automatic Call Distribution (ACD) split, a Direct Department Calling (DDC) group, a Uniform Call Distribution (UCD) group, a remote access extension, or any system extension.

Administering Listed Directory Number

The following steps are part of the administration process for the Listed Directory Number (LDN) feature:

- Assigning listed directory numbers
- Assigning an incoming destination to a trunk

This section describes:

- Any prerequisites for administering the Listed Directory Number feature
- The screens that you use to administer the Listed Directory Number feature
- Complete administration procedures for the Listed Directory Number feature

Prerequisites for administering Listed Directory Number

You must complete the following actions before you can administer the Listed Directory Number feature:

- None

Screens for administering Listed Directory Number

Screen name	Purpose	Fields
Listed Directory Numbers	Assign listed directory numbers and an optional, night-service destination.	All
Trunk Group	Assign an incoming destination to a trunk.	**Incoming Destination**

Assigning listed directory numbers

To assign a listed directory number:

1. Type **change listed-directory-number**. Press **Enter**.

The system displays the Listed Directory Numbers screen (Figure 269: Listed Directory Numbers screen on page 1115).

Figure 269: Listed Directory Numbers screen

```
change listed-directory-number                                Page   1 of   2

                          LISTED DIRECTORY NUMBERS

                           Night Destination:

          Ext      Name                            TN
      1:
      2:                                           1
      3:                                           1
      4:                                           1
      5:                                           1
      6:                                           1
      7:                                           1
      8:                                           1
```

2. In the **Night Destination** field, type a night destination extension that consists of 1 to 8 digits. The extension must be comprised of the numbers **0** through **9**. The night destination extension receives the calls to the extensions that you type in the **Ext** field, when the Night Service feature is active.

   For DEFINITY® CSI, SI, and IP-PNC, you can type a night service extension, a recorded announcement extension, a Vector Directory Number (VDN), an individual attendant extension, or a hunt group extension.

3. In the **Ext** field, type the number of the extension that you want to use for the LDN feature. The extension number can consist of 1 to 9 digits.
4. In the **Name** field, type the name that you use to identify the listed directory number. The name can consist of 1 to 27 alphanumeric characters.
5. In the **TN** field, type the Tenant Partition number.
6. Repeat Steps 3 through 5 for each extension to which you want to assign a listed directory number.
7. Press **Enter** to save your changes.

Assigning an incoming destination to a trunk

To assign an incoming destination to a trunk:

1. Type **change trunk-group *n***, where ***n*** is the number of the trunk group to which you want to assign an incoming destination.

   The system displays the Trunk Group screen.

2. In the **Incoming Destination** field, perform one of the following actions:

   - If the **Trunk Type** field on the Trunk Group screen is not set to **auto**, leave the field blank.
   - Type the extension for the incoming calls.

     You can type any extension. However, the extension is usually for a VDN, a voice response unit, or a voice messaging system. The Night Service feature overrides the extension that you type in the **Incoming Destination** field.

     CAUTION:
     When you assign a Multi-Location Dial Plan shortened extension in a field that is designed for announcement extensions, certain administration end validations that are usually performed on announcement extensions are not performed, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Ensure that you administer the correct type of announcement for the application when you assign shortened extensions.

   - If you want the system to route the calls to the attendant, type **attd**.

     The system records the calls as LDN calls on the call detail recording records.

   The system displays the **Incoming Destination** field on the CO Trunk screen, when the **Direction** field on the **Trunk Group** screen is set to **incoming** or **two-way**.

   Use the **Incoming Destination** field to set the destination for all incoming calls on trunk groups such as central office (CO), foreign exchange (FX), and Wide Area Telecommunications Service (WATS), that must terminate at a single destination. This field can be set to a station so all incoming calls will ring at this station. If this destination station is busy, the caller will hear a ringback tone instead of a busy tone. The destination that you type in the **Incoming Destination** field is also the default night service destination, unless you enter a different destination in the **Night Service** field.

3. Press **Enter** to save your changes.

Reports for Listed Directory Number

The following reports provide information about the Listed Directory Number feature:

- None

Considerations for Listed Directory Number

This section provides information about how the Listed Directory Number (LDN) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Listed Directory Number under all conditions. The following considerations apply to Listed Directory Number:

- The number of listed directory numbers that you can assign depends on the configuration of your system.

Interactions for Listed Directory Number

This section provides information about how the Listed Directory Number (LDN) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Listed Directory Number in any feature configuration.

- Night Service

  If you activate the Night Service capability, and a night console is not assigned or is not operational, the system routes:

  - Incoming Direct Inward Dialing (DID) LDN calls route to a designated DID LDN night extension. If no DID LDN night extension is designated, the system routes DID LDN calls to the attendant
  - Incoming central office (CO) or foreign exchange (FX) trunk calls to the night destination that is specified for the trunk group. If no night destination is specified for the trunk group, the system routes the calls to the normal incoming destination for that trunk group.
  - Internal calls and coverage calls to the attendant to the DID LDN night extension during night service.

Locally Sourced Announcements and Music

Use the Locally Sourced Announcements and Music feature to access announcement and music audio sources from a local port network or media gateway.

Locally sourced audio can help:

- Improve the quality of audio
- Reduce resource usage, such as VoIP resources
- Provide a backup mechanism for announcement and music sources

Detailed description of Locally Sourced Announcements and Music

This section provides a detailed description of the Locally Sourced Announcements and Music feature. This feature is available with Communication Manager Release 3.0.

The Locally Sourced Announcement and Music feature differs from the Announcement feature and the Music-on-Hold feature. The Announcement and Music-on-Hold features are single-sourced audio while the Locally Sourced feature is group-sourced audio. Locally Sourced Announcement and Music is based on groups of audio sources. Audio sources are assigned either to an audio group or a music-on-hold group.

Audio groups are made up of multiple sources of the same announcement or music. These audio sources can be located on any or all of the Voice Announcement with LAN (VAL) TN2501AP boards or on virtual VALs (vVAL) in a media gateway. The VAL or vVAL boards are assigned to an audio group. The audio group is then assigned to an announcement or audio extension as a group sourced location.

Announcement or music recordings are saved as wav file types. Each recording must be saved manually onto the VAL or vVAL boards the same way as single-sourced announcements using an FTP program or VAL Manager. Each recording has the same file name within an audio group. The audio group can contain announcements and music.

A music-on-hold group is a collection of externally connected and continuously playing music sources. An example of a music-on-hold source is a radio station connected to a media gateway using an analog station port. Multiple music-on-hold sources can be used in the same system.

As with the Music-on-Hold feature, only one music source is defined for a system or for a tenant partition. However, you can define a music source as a group of music-on-hold sources. Therefore, both non-tenant and tenant systems can use the group concept to distribute music-on-hold sources throughout a system.

When an incoming call requires an announcement or music-on-hold, the audio source that is closest to the incoming call trunk plays. An algorithm selects the most local source of audio to play for a call.

The most local source means that it is local to the trunk or user in the same Media Gateway or in the same group of Port Network Gateways, in the same network region, in the interconnected network region, or is interconnected through an Inter-Gateway Alternate Routing (IGAR). An announcement file extension can be administered for queuing. Under queuing, if the audio source selected to play has no available playback ports, the request to play that audio is held in queue until a port on the source is available. If the queuing option is not administered for the audio file, the search for a local source continues as above.

Accessing audio locally minimizes audio distortion because the audio is located within or close to the same port network or gateway as the caller. Therefore, the Locally Sourced feature improves the quality of announcements and music-on-hold. This feature also reduces resource usage, such as VoIP resources, because the nearest available audio source of an announcement or music is played. Locally Sourced Announcements and Music also provides a backup for audio sources because multiple copies of the audio files are stored in multiple locations.

You can use an announcement or audio source extension with an assigned audio group anywhere that a single sourced announcement or audio source extension can be used. See the Announcements feature or the Music-on-Hold feature for information on single sourced audio.

Note:
For more information on Inter-Gateway Alternate Routing (IGAR), see *Administering Network Connectivity on Avaya Aura™ Communication Manager,* 555-233-504.

Administering Locally Sourced Announcements and Music

The following steps are part of the administration process for the Locally Sourced Announcements and Music feature:

- Adding an audio group
- Listing all audio groups
- Changing audio group extensions
- Listing audio group extensions

- Adding a music-on-hold group
- Listing music-on-hold groups
- Changing music-on-hold source type
- Adding music sources to a tenant partition
- Displaying VAL board or vVAL group descriptions
- Displaying system capacities

This section describes:

- The prerequisites for administering the Locally Sourced Announcements and Music feature
- The screens that you use to administer the Locally Sourced Announcements and Music feature
- Complete administration procedures for the Locally Sourced Announcements and Music feature

Screens for administering Locally Sourced Announcements and Music

Screen name	Purpose	Fields
Audio Groups	List audio group features and announcement extensions.	All
Audio Group	Add, change, or delete audio source locations in an audio group.	All
Announcements/Audio Sources	Display and change individual announcements and music-on-hold extensions. Determine properties of audio sources.	All
MOH Group	Add, change, display, delete music-on-hold groups.	All
Music-on-Hold Groups	List all of the music-on-hold groups in the system.	All
Feature-Related System Parameters	Change music-on-hold group source type.	Music/Tone On Hold Type
Tenant	Display the music source for a tenant partition.	Music Source

Screen name	Purpose	Fields
Music Sources	Add, change, display, delete music sources.	All
Announcement Group Board Usage	Display group identification.	All
System Capacity	Display available extension source combinations capacity.	Extension-Source Combinations

Adding an audio group

To add an audio group:

1. Type **add audio-group *number*** where ***number*** is the group number. Press **Enter**.

   The system displays the Audio Group screen (Audio Group screen on page 1122).

Figure 270: Audio Group screen

```
add audio-group 1                                                Page 1 of 4

                                   AUDIO GROUP 1

                     Group Name: Relaxation Music__

AUDIO SOURCE LOCATION

1: ____01A09    16: _________ 31: _________ 46: _________ 61: _________
2: ___ 019v9    17: _________ 32: _________ 47: _________ 62: _________
3: _________    18: _________ 33: _________ 48: _________ 63: _________
4: _________    19: _________ 34: _________ 49: _________ 64: _________
5: _________    20: _________ 35: _________ 50: _________ 65: _________
6: _________    21: _________ 36: _________ 51: _________ 66: _________
7: _________    22: _________ 37: _________ 52: _________ 67: _________
8: _________    23: _________ 38: _________ 53: _________ 68: _________
9: _________    24: _________ 39: _________ 54: _________ 69: _________
10:_________    25: _________ 40: _________ 55: _________ 70: _________
```

2. In the **Group Name** field, type an identifier name for the group.
3. In the **Audio Source Location** fields, type in the VAL boards or vVAL location designators for each audio source in the audio group.
4. Press **Enter** to save your changes.

Listing all audio groups

To list all audio groups in a system:

1. Type **list audio-group**. Press **Enter**.

   The system displays the Audio Groups screen (Audio Groups screen on page 1123).

Figure 271: Audio Groups screen

```
list audio-group

                          AUDIO GROUPS

Group       Name                      Number of Sources

1           Relaxation Music               2
12          Forgive the wait              20
23          Best deals for today          30


At End of Member List
```

2. View your settings and exit the screen.

Changing audio group extensions

To change audio group extensions for announcements and music, see the Adding/changing/displaying or removing announcement extensions on page 183.

Listing audio group extensions

To list all of the announcement extensions that refer to a specific audio group:

1. Type **list usage audio-group *number*** where ***number*** is the audio group number. Press **Enter**.

   The system displays the Announcements/Audio Sources screen (Announcements/Audio Sources screen on page 1124).

Figure 272: Announcements/Audio Sources screen

```
list usage audio-group 1

                              ANNOUNCEMENTS/AUDIO SOURCES

Used By
  Extension 27116__________      Name  audio_group_voa
  Extension 27117                Name  audio_group_collect_digits
  Extension 27118                Name  audio_group_wait
  Extension 27121                Name  audio_group_repeater
  Extension 27122                Name  audio_group_musicA
```

2. View your settings and exit the screen.

Adding a music-on-hold group

To add a music-on-hold group:

1. Type **add moh-analog-group *number*** where ***number*** is the music-on-hold group number. Press **Enter**.

   The system displays the MOH Group screen (MOH Group screen on page 1125).

Figure 273: MOH Group **screen**

```
add moh-analog-group 1                                          Page 1 of 4

                                  MOH GROUP 1

                             Group Name: Relaxation Music__

MOH SOURCE LOCATION

1: __01A0905   16: _________ 31: _________ 46: _________ 61: _________
2: __019v401   17: _________ 32: _________ 47: _________ 62: _________
3: _________   18: _________ 33: _________ 48: _________ 63: _________
4: _________   19: _________ 34: _________ 49: _________ 64: _________
5: _________   20: _________ 35: _________ 50: _________ 65: _________
6: _________   21: _________ 36: _________ 51: _________ 66: _________
7: _________   22: _________ 37: _________ 52: _________ 67: _________
8: _________   23: _________ 38: _________ 53: _________ 68: _________
9: _________   24: _________ 39: _________ 54: _________ 69: _________
10:_________   25: _________ 40: _________ 55: _________ 70: _________
11: _________  26: _________ 41: _________ 56: _________ 71: _________
12: _________  27: _________ 42: _________ 57: _________ 72: _________
13: _________  28: _________ 43: _________ 58: _________ 73: _________
14: _________  29: _________ 44: _________ 59: _________ 74: _________
```

2. In the **Group Name** field, type in an identifier name for the music-on-hold group.
3. In the **MOH Source Location** numbered fields, type in the music-on-hold VAL or vVAL source locations.
4. Press **Enter** to save your changes.

Listing music-on-hold groups

To list all of the music-on-hold groups in a system:

1. Type **`list moh-analog-group`**. Press **Enter**.

   The system displays the Music-on-Hold **Groups** screen (Music-on-Hold Groups screen on page 1126).

Figure 274: Music-on-Hold Groups screen

```
list moh-analog-group                                              Page 1

                              MUSIC-ON-HOLD GROUPS

Group              Name              Number of Sources

8                Elevator Music           5
10               Latin Renditions        20
11               Polka music             30

At End of Member List
```

2. View your settings and exit the screen.

Changing music-on-hold source type

To change the source type for music-on-hold:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Features-Related System Parameters screen (Feature-Related System Parameters screen on page 1127).

2. In the **Music/Tone on Hold** field, type **music**.

   The **Type** field appears.

   If the **Tenant Partitioning** field on the Optional Features screen is set to **y**, you cannot administer the **Music/Tone on Hold** field. If the **Tenant Partitioning** field on the Optional Features screen set to **y**, you must use the Music Sources screen (Music Sources screen on page 1128) to assign music to a port.

3. Type one of the following values:

   - Type **ext** and the corresponding extension number of the integ-mus announcement/ audio source.
   - Type **group** and the corresponding music-on-hold analog group number.
   - Type **port** and the corresponding location of the music-on-hold analog/aux-trunk source.

4. Press **Enter** to save your changes.

Figure 275: Feature-Related System Parameters screen

```
change system-parameters features                                  page 1
                         FEATURE-RELATED SYSTEM PARAMETERS
                            Self Station Display Enabled? n
                                 Trunk-to-Trunk Transfer? none
 Automatic Callback - No Answer Timeout Interval (rings): 4_
                    Call Park Timeout Interval (minutes): 10
     Off-Premises Tone Detect Timeout Interval (seconds): 20_
                              AAR/ARS Dial Tone Required? y
                        Music/Tone On Hold: music__ Type: Group 1_
           Music (or Silence) On Transferred Trunk Calls: all
                    DID/Tie/ISDN/SIP Intercept Treatment: attd

 Internal Auto-Answer of Attd-Extended/Transferred Calls? y
               Automatic Circuit Assurance (ACA) Enabled? y
                                    ACA Referral Calls: local
                               ACA Referral Destination: ________
            ACA Short Holding Time Originating Extension: ______
             ACA Long Holding Time Originating Extension: ______
          Abbreviated Dial Programming by Assigned Lists:
     Auto Abbreviated/Delayed Transition Interval(rings):
                  Protocol for Caller ID Analog Terminals: Bellcore
 Display Calling Number for Room to Room Caller ID Calls?
```

Adding music sources to a tenant partition

To add music sources to a tenant partition when tenant partitioning is activated:

1. Type **change tenant *number*** where ***number*** is the partition number.

   The system displays the Tenant screen (Tenant screen on page 1128).

Figure 276: Tenant screen

```
change tenant 1

                                TENANT 1

Tenant description: _________________________
Attendant group: 1
Ext Alert Port (TAAS): ______ Ext Alert (TAAS) Extension: ___
Night Destination: _____
Music Source: 1
Attendant Vectoring VDN:
Emergency Number:
```

2. Type **change music-sources**. Press **Enter**.

   The system displays the Music Sources screen (Music Sources screen on page 1128).

Figure 277: Music Sources screen

```
change music-sources

                                MUSIC SOURCES

Source No.      Type       Source                          Description

   1            music      Type: port   01A0904            Country
   2            tone                                       Tone-on-Hold
   3            music      Type: group  49                 Classical
   4            none
   5            none
   6            music      Type: ext    20030              Rock
```

3. In the **Type** field, valid options are **music** and **tone**.
4. In the **Source** field, valid options for the music type are:
   - **ext** - audio source extension for a single or group audio source
   - **group** - a music-on-hold analog group number
   - **port** - an analog or auxiliary trunk source location

5. After a **Source** type is entered, an entry line appears to the right. Type an identifier for the audio source. The identifier is one of the following:
   - audio group extension number,
   - music-on-hold group number, or
   - port location.
6. Type a **Description** for each music source.
7. Repeat steps 3 to 6 to add up to 100 music sources.
8. Press **Enter** to save your changes.

Displaying VAL board or vVAL group descriptions

To identify the group descriptions of specified VAL or vVAL boards:

1. Type **`list usage integ-annc-`*`board location`*** where ***`board location`*** is the 5-character location identification number. Press **Enter**.

   The system displays the Announcement Group Board Usage screen (Announcement Group Board Usage screen on page 1129).

Figure 278: Announcement Group Board Usage **screen**

```
list usage integ-annc-board 01B18                                    Page 1

                        ANNOUNCEMENT GROUP BOARD USAGE

USED BY

Announcement   Announcement   2087   Extension   3005
Audio Group           Group      4      Member   28
Audio Group           Group     23      Member   101
```

Displaying system capacities

The number of audio groups, audio sources per group, audio files per source and extension-source combinations are limited. Extension-source combinations are the total of the single-sourced announcement extensions and the group-sourced announcement sources that are assigned in an audio group to each extension. See the *Avaya Aura™ Communication Manager System Capacities Table* for the current release to see system capacity limits.

To check the used and available capacities within a system:

1. Type **display capacity**. Press **Enter**.

   The system displays the **System Capacity** screen (System Capacity screen on page 1130).

Figure 279: System Capacity **screen**

```
display capacity                                              Page 6 of 12

                                SYSTEM CAPACITY

                                                                      System
                                                  Used   Available  Limit
        RECORDED ANNOUNCEMENTS/MUSIC/AUDIO SOURCES
                                  Analog Queue Slots:    0     1000      1000
                      Extension-Source Combinations:    0     3000      3000
                                  TN2501 VAL Boards:    1        0         1
                         Media Gateway vVAL Sources:    0        0         0
                               TN2602 VoIP Channels:    0        0         0
```

Reports for Locally Sourced Announcements and Music

The following reports provide information about the Locally Sourced Announcements and Music feature:

None.

Considerations for Locally Sourced Announcements and Music

None.

Interactions for Locally Sourced Announcements and Music

This section provides information about how the Locally Sourced Announcements and Music feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Locally Sourced Announcements and Music in any feature configuration.

- Automatic Server Failover Feature

  The operation of local audio and music-on-hold sources might not work as intended in cases where the primary server migrates to a backup server. This interruption occurs because the audio sources might not be available from the backup server due to physical fragmentation of the network. However, the best available local audio source is still chosen by the backup server.

- Multi-Location Dial Plan (MLDP)

  Under the Locally Sourced Announcements and Music feature, an audio source is selected based on where the source is located with respect to the user's location. However, under the MLDP feature, the audio source to be used is predefined and based only on the location of the call's ingress point. Also unlike the locally sourced music-on-hold, the MLDP feature does not support music files.

Loss Plans

Use the Loss Plans feature to determine the amount of loss (quieter) or gain (louder) applied on calls. Usually, your system uses a predefined loss plan that is based on the administered country code. In some circumstances, you can change the loss plan on a per-trunk or a per-telephone basis.

Detailed description of Loss Plans

This section provides a detailed description of the Loss Plans feature.

CAUTION:
The values in the loss plan can significantly affect the quality of service that your users experience. Therefore, in order to change the loss plan you must thoroughly understand loss plans and your particular configuration. Avaya recommends that you seek technical assistance from Avaya before making any modifications to the loss plan.

Use the 2 Party Loss Plan page of the Location Parameters screen to set the decibel gain or loss levels, between two parties on a call. Each row on this screen is considered a different loss group. You can assign a loss group to a particular phone or trunk by administering a value for the **Loss Group** fields on the Station and Trunk Generation screens. This allows you to use different loss plans for different types of phones or different trunk groups.

The Tone Loss Plans page of the Location Parameters screen allows you to set the tone gain or loss levels (in dB) on a conference call, as well as the total gain or loss in a conference based on the number of parties.

Note:
The end-to-end total loss for multi-party conference calls that is administered on the Location Parameters screen is not always applied to a specific call. The loss applied to, for example, a 3-party conference call is calculated by adding the fixed pairwise loss for each pair of ports to the value for 2-party loss shown on the Location Parameters screen. If this total is *less* than the end-to-end total loss value configured for a 3-party conference, calculate the difference, and divide the difference by 2. Add 1 to this figure, and the result is the amount of loss applied to the call.

IP endpoints connected using hairpinning or direct IP-IP are not under the control of the administrable loss plan.

Administering Loss Plans

The following steps are part of the administration process for the Loss Plans feature:

This section describes:

- Any prerequisites for administering the Loss Plans feature
- The screens that you use to administer the Loss Plans feature
- Complete administration procedures for the Loss Plans feature

Prerequisites for administering Loss Plans

You must complete the following actions before you can administer the Loss Plans feature:

- Ensure that the **Digital Loss Plan Modification** field on the Optional Features screen is set to **y** this screen. If the field is not set to **y**, your system is not enabled for the Loss Plans feature.Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- Ensure that the **Customize** field on the Location Parameters screen is set to **y**.

  To view the Location Parameters screen, type **`display location-parameters`**. Press **Enter**.

Guidelines for using loss groups

The following guidelines are provided for using the loss groups:

- Use loss groups 1, 2, 3, 4, 5, and 19 for the following types of stations:
  - 1, 4, and 5 for analog stations
  - 2 for digital stations
  - 3 for BRI stations
  - 19 for IP stations
- Use loss groups 6, 7, and 8 for analog central office (CO) trunks. Analog CO trunks must not use other loss groups.
- Use loss groups 12, 13, and 14 for digital tie trunks.
- Use loss groups 9 and 10 for analog tie trunks.

- Use loss group 15 for tie trunks (analog or digital) where the length of the trunks are less than 100 miles. For example, always select the loss group 15 for tie trunks connecting switches on the same campus.
- Use loss group 11 for digital CO trunks.
- Use loss groups 16 and 17 with the TN439 (2 wire analog tie trunk card) which is only used in Australia.

Screens for administering Loss Plans

Screen name	Purpose	Fields
Optional Features	• Shows whether or not the Loss Plans feature is enabled on your system.	• **Digital Loss Plan Modification**
Location Parameters	• Customize the Loss Plans feature. • Shows the digital loss group number that is used by the virtual IP tie trunks.	• **Customize** • **Inter-location Loss Group**
Station	• Shows the index into the loss plan and the tone plan	• **Loss Group**
Trunk Group	• Shows the index into the loss plan and the tone plan if the call is carried over an analog or a digital signaling port in the trunk group.	• **Analog Loss Group** • **Digital Loss Group**
Personal CO Line Group	• Shows the index into the loss plan and the tone plan if the call is carried over an analog or a digital signaling port in the personal co line group.	• **Analog Loss Group** • **Digital Loss Group**

Loudspeaker Paging

Use the Loudspeaker Paging feature to connect Communication Manager to loudspeaker systems and allow users to page from user telephones.

Detailed description of Loudspeaker Paging

This section provides a detailed description of the Loudspeaker Paging feature.

You can administer up to nine separate zones, or sets of loudspeakers on Communication Manager. Thus you can make an announcement to one group or location without disturbing people who do not need to hear the announcement. Auxiliary trunks connect the speakers in each zone to ports on an auxiliary trunk circuit pack.

Types of Paging

Communication Manager offers two types of loudspeaker paging. You can use each separately, and you can also use both together.

- Voice paging

  With voice paging, users can make announcements over a loudspeaker system from their phones. You can integrate voice paging and Call Park by enabling Deluxe Paging.

- Chime paging

  If frequent voice pages are undesirable, you can assign a unique series of chimes, or a chime code to each extension. The chime code assigned to that extension plays over the speakers when that extension is paged.

  Chime paging is sometimes called Code Calling Access.

Deluxe paging

With standard voice paging, users page by dialing the Trunk Access Code assigned to the zone they want to page. If users have an active call, the users must manually put the call on hold or park the call before they dial the TAC.

When you enable deluxe paging, users can automatically park an active call when they use the voice paging feature.

Users with multiappearance telephones

The following description applies only to systems with deluxe paging. To page and park an active call simultaneously, users with a multiappearance phone press **Transfer**, dial the trunk access code + an extension number where the call will be parked, make the announcement, and press **Transfer** again. The paged party dials the answer back Feature Access Code + the extension number and is connected directly to the parked call. If the paging user presses **Conference** instead of **Transfer**, they are conferenced with the parked caller and both are connected in a three-way conference with the paged user when that user responds. This is called Meet-Me Conferencing.

If the paging user does not want to park the active call, Deluxe Paging also allows "Meet-Me Paging." Paging users can put an active call on hold and make their page, announcing their own extension. When the paged party calls, the paging user can conference the call on hold or transfer it to the paged party.

Users with single-line phones

This description only applies to systems with deluxe paging. To page and park an active call simultaneously, users with a single-line phone press **Recall** or flash the switch hook, dial the trunk access code + an extension where the call will be parked, and press **Recall** again. The paging user is conferenced with the parked caller and both parties are connected in a three-way conference with the paged user when he or she responds. In other words, Meet-Me conferencing is standard operation for users with single-line phones. The paged party dials the answer back Feature Access Code + the extension number and is connected directly to the parked call.

If the paging user does not press **Recall** until the loudspeaker paging time-out interval expires, the user hears a confirmation tone, and the active call is automatically parked on their extension. When the paged party answers the call. The paged party is connected to the paging party. The paging party can then transfer the call to the calling party.

Chime paging

To page a user, dial the TAC for a zone, and then chime the extension of the person that they want to page. The system matches the extension dialed to its assigned code, and plays the code over the loudspeakers. If users have an active call when they start to page, the call is automatically parked on the extension dialed in the page. Paged parties may retrieve the parked call normally.

Auxiliary paging systems

Communication Manager requires a separate port for each paging zone, and supports a maximum of nine zones. If you have more than nine zones or do not want to allot that many ports for paging, Avaya can provide auxiliary paging systems. These systems can support many zones from 1 port. They can also provide additional capabilities such as two-way communication through the loudspeaker system. In this case, the person paged can speak directly to the pager over the loudspeaker.

Restrictions on loudspeaker paging

These restrictions apply to both voice, deluxe voice, and chime paging:

- A paging call cannot be placed on hold, included in a conference call, or transferred.Also, ringback queuing does not work with loudspeaker paging calls either.
- Users with any of the following restrictions cannot page:
  - Controlled restriction
  - Manual originating line service
  - Origination restriction
  - Miscellaneous trunk restriction
- A user with a single-line telephone does not hear a call-waiting tone if the user gets a call while paging.
- Listed Directory Number (LDN) and Direct Inward Dialing (DID) calls cannot access the paging system. However, attendants can park incoming calls and page.
- Remote users (such as remote access users and tie-trunk users) who are paging cannot use # to park calls on their own extensions.

Administering Loudspeaker Paging

The following steps are part of the administration process for the Loudspeaker Paging feature:

- Setting up Voice Paging over loudspeakers
- Setting up Chime Paging over Loudspeakers
- Assigning a chime page code to an individual extension

This section describes:

- Any prerequisites for administering the Loudspeaker Paging feature

- The screens that you use to administer the Loudspeaker Paging feature
- Complete administration procedures for the Loudspeaker Paging feature

Prerequisites for administering Loudspeaker Paging

You must complete the following actions before you can administer the Loudspeaker Paging feature:

- The server that runs Communication Manager must have one or more auxiliary trunk circuit packs with enough available ports to support the number of paging zones that you define. Each paging zone requires one port.

  For information on specific circuit packs, see the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

- To set up deluxe paging, view the Feature-Related System Parameters screen. Ensure that the **Deluxe Paging and Call Park Timeout to Originator** field is set to **y**.

  To view the Feature-Related System Parameters screen, type **`change system-parameters features`**. Press **Enter**.

Screens for administering Loudspeaker Paging

Screen name	Purpose	Fields
Feature-Related System Parameters	Set up deluxe paging.	**Deluxe Paging and Call Park Timeout to Originator**
Loudspeaker Paging	Set up voice paging over loudspeakers.	• **Voice Paging Timeout** • **Port** • **Voice Paging - COR** • **Voice Paging - TAC** • **Location**
	Set up chime paging over loudspeakers	• **Code Calling Playing Cycles** • **Port** • **Voice Paging - TAC** • **Voice Paging - COR** • **Location** • **Code Calling - TAC**
Code Calling Ids	Set up chime paging over loudspeakers	• **Ext** • **Id**

Setting up Voice Paging over loudspeakers

To set up voice paging over loudspeakers:

1. Type **change paging loudspeaker**. Press **Enter**.

   The system displays the Loudspeaker Paging screen (Figure 280: Loudspeaker Paging screen on page 1141).

   In this example, you set up voice paging for an office with five zones. You allow users to page all five zones at once, and you assign a Class of Restriction (COR) of 1 to all zones.

Figure 280: Loudspeaker Paging screen

```
                              LOUDSPEAKER PAGING

                                    CDR? y
                  Voice Paging Timeout (sec): 30
                 Code Calling Playing Cycles:

PAGING PORT ASSIGNMENTS
                      Voice Paging     Code Calling
 Zone  Port       TAC  COR  TN     TAC  COR  TN     Location:
   1:  01C0501    301   1   1                1      Reception area
   2:  01C0502    302   1   1                1      Shipping & receiving
   3:  01C0503    303   1   1                1      Staff offices
   4:  01C0504    304   1   1                1      Management suite
   5:  01C0601    305   1   1                1      Breakroom
   6:                       1                1
   7:                       1                1
   8:                       1                1
   9:                       1                1
 ALL:             310   1   1                1
```

2. In the **Voice Paging Timeout** field, type the maximum number of seconds that a page can last.

   In this example, the paging party is disconnected after **30** seconds.

3. In the **Port** field for Zone 1, type the port number that is assigned to the auxiliary trunk circuit pack to this zone**.**

   In this example, the port number is **01C0501**.

4. In the **Voice Paging - TAC** field, type the value the for Trunk Access Code (TAC) that users dial to page this zone.

   In this example, the value is **301**.

5. In the **Voice Paging - COR** field, type the class of restriction (COR) for this zone. You can assign different CORs to different zones.

   In this example, the COR is **1**.

6. In the **Location** field on the Zone 1 row, type a descriptive name for the zone. Use this name to help you remember the corresponding physical location.

   In this example, the zone name is **Reception area**.

7. Repeat steps 4 through 6 for each zone.

8. In the **ALL** row of the **Voice Paging- TAC** field in, type **310** and **1** in the **Voice Paging - COR** field.

   When you complete this row, you allow users to page all zones at once. You do not have to assign a port to this row.

9. Press **Enter** to save your changes.

You can integrate loudspeaker voice paging and call parking. This is called "deluxe paging." You enable deluxe paging by entering y in the **Deluxe Paging and Call Park Timeout to Originator** field on the Feature-Related System Parameters screen. To allow paged users the full benefit of deluxe paging, you should also enter a code in the **Answer Back Access Code** field on the Feature Access Code (FAC) screen if you have not done so already. Paged users dial the FAC, plus an extension to retrieve calls parked by deluxe paging.

Note:
To set up paging on an H.248 gateway, connect the paging system to a port on an MM711 and administer the port as an analog station on the Station screen. No entries on the Loudspeaker Paging screen are required.

Setting up Chime Paging over Loudspeakers

To set up chime paging:

1. Type **`change paging loudspeaker.`** Press **Enter**.

   The system displays the Loudspeaker Paging screen (Figure 281: Loudspeaker Paging screen on page 1143).

   In this example, you set up chime paging for a clothing store with three zones. You allow users to page all three zones at once, and you assign a Class of Restriction (COR) of **1** to all zones.

Figure 281: Loudspeaker Paging screen

```
                              LOUDSPEAKER PAGING

                                    CDR? y
            Voice Paging Timeout (sec):
           Code Calling Playing Cycles: 2

PAGING PORT ASSIGNMENTS
                  Voice Paging     Code Calling
 Zone  Port       TAC  COR  TN     TAC  COR  TN     Location:
   1:  01A0301              1      80    1   1      Men's Department
   2:  01A0302              1      81    1   1      Women's Department
   3:  01A0303              1      82    1   1      Children's
   4:                       1                 1
   5:                       1                 1
   6:                       1                 1
   7:                       1                 1
   8:                       1                 1
   9:                       1                 1
 ALL:                       1      89    1   1
```

2. In the **Code Calling Playing Cycles** field, type the number of times that a chime code plays when someone places a page.

   In this example, the number of times is **2**.

3. In the **Port** field for Zone 1, type the port number of the auxiliary trunk circuit pack that is assigned to this zone.

   In this example, the port number is **01A0301**.

4. In the **Code Calling - TAC** field, type the Trunk Access Code (TAC) users dial to page this zone. You cannot assign the same trunk access code to more than one zone.

   In this example, the trunk access code is **80**.

5. In the **Code Calling - COR** field, type the COR number that is assigned to this zone.You can assign different classes of restriction to different zones

   In this example, the COR is **1**.

6. In the Zone 1 row of the **Location** field, type a descriptive name for the zone. Use this name to help you remember the corresponding physical location.

   In this example, the location is **Men's Department**.

7. Repeat steps 4 through 6 for zones 2 and 3.

8. In the **ALL** row of the **Code Calling - TAC** field, type **89** and **1** in the **Code Calling - COR** field.

   When you complete this row, you allow users to page all zones at once. You do not have to assign a port to this row.

9. Press **Enter** to save your changes.

Assigning a chime page code to an individual extension

To assign chime codes to an individual extension:

1. Type **`change paging code-calling-ids`** and press **Enter**.

   The system displays the Code Calling IDs screen (Figure 282: Code Calling IDs screen on page 1144).

Figure 282: Code Calling IDs screen

```
                                CODE CALLING IDs
ID ASSIGNMENTS
   Id   Ext        Id   Ext     Id   Ext     Id   Ext     Id   Ext
   111: 2130       141: _______ 221: _______ 251: _______ 331: _______
   112: 2131       142: _______ 222: _______ 252: _______ 332: _______
   113: 2149       143: _______ 223: _______ 253: _______ 333: _______
   114: 2150       144: _______ 224: _______ 254: _______ 334: _______
   115: 2152       145: _______ 225: _______ 255: _______ 335: _______
   121: 2153       151: _______ 231: _______ 311: _______ 341: _______
   122: 2160       152: _______ 232: _______ 312: _______ 342: _______
   123: 2167       153: _______ 233: _______ 313: _______ 343: _______
   124: _________  154: _______ 234: _______ 314: _______ 344: _______
   125: _________  155: _______ 235: _______ 315: _______ 345: _______
   131: _________  211: _______ 241: _______ 321: _______ 351: _______
   132: _________  212: _______ 242: _______ 322: _______ 352: _______
   133: _________  213: _______ 243: _______ 323: _______ 353: _______
   134: _________  214: _______ 244: _______ 324: _______ 354: _______
   135: _________  215: _______ 245: _______ 325: _______ 355: _______
```

2. In the **Ext** field, type the first extension for Id **111**.

   In this example, the first extension is **2130**. Each code Id defines a unique series of chimes.

3. To assign chime codes to the remaining extensions type an extension number on the line following each code Id.

   You can assign a different chime code to as many as 125 extensions.

4. Press **Enter** to save your changes.

Interactions for Loudspeaker Paging

This section provides information about how the Loudspeaker Paging feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Loudspeaker Paging in any feature configuration.

- Bridged Call Appearance

  If a parked call includes a shared terminating extension group, a shared Personal Central Office Line (PCOL), or a redirected call with a temporary bridged appearance, the maximum number of off-hook parties on the call is five, instead of six. The sixth position is reserved for the answer-back call.

- Call Coverage

  If a coverage call is parked by deluxe paging, the temporary bridged appearance at the principal extension is maintained as long as the covering user remains off-hook or places the call on hold.

- Call Park

  If a call is parked by deluxe paging and the time-out interval expires, the call usually returns to the paging user. However, with remote access and tie trunk access, the call returns to the attendant. If unanswered, the call follows the coverage path of the paging user.

- Call Pickup

  If you use call pickup or directed call pickup to answer a call and then park it by deluxe paging, a temporary bridged appearance at the principal extension is maintained if you remain off-hook or place the call on hold.

- Conference -Attendant and Terminal

  Paging calls cannot be conferenced.

- Data Call Setup

  If the Data button has been pressed for modem pooling, access to paging is denied.

- Data Privacy

  If a call has Data Privacy activated and you park it by deluxe paging, Data Privacy for that call is automatically deactivated.

- Hunt Groups

  If a hunt-group member parks a call using deluxe paging, the call is parked on the member’s own extension, not the hunt-group extension. You cannot park calls on a group extension by dialing the extension as a call-park destination.

- Night Service

  If a night-station user parks a Night Service call with deluxe paging, the call is parked on the night station’s primary extension.

- Personal Central Office Line (PCOL)

  If a PCOL call is parked by deluxe paging, the temporary bridged appearance of the call is maintained at the PCOL extension until the call is disconnected.

- Terminating Extension Group (TEG)

  If a TEG member parks a call using deluxe paging, the call is parked on the member's extension, not the group extension. You cannot park calls on a group extension by dialing the extension as a call-park destination.

- Transfer

  Paging calls can't be transferred.

Chime paging

The following interactions are specifically for chime paging:

- Abbreviated Dialing

  Don't use special characters in abbreviated dialing lists used with chime paging.

- Conference - Attendant

  A call cannot be conference while the attendant is accessing paging equipment. The attendant can, however, release the call after paging the called party.

- Conference - Terminal

  A call cannot be conferenced while the user is accessing paging equipment.

- Transfer

  A call cannot be transferred while the attendant is accessing paging equipment.

Troubleshooting Loudspeaker Paging

This section lists the known or common problems that users might experience with the Loudspeaker Paging feature.

Problem	Possible cause	Action
Users cannot page.	The attendant has control of the trunk group.	Deactivate attendant control.
Calls to an extension are heard over the loudspeakers.	The extension might have been forwarded to a trunk access code used for paging.	Deactivate call forwarding or change the extension to which calls are forwarded.

Malicious Call Trace

Use the Malicious Call Trace (MCT) feature to track malicious calls. Both users and attendants can track malicious calls, and display information that identifies the source of the call. The user or attendant can share the information with personnel on a tandemed server. The personnel on the tandemed server can continue to trace the call. MCT also supports a voice recorder that records the malicious call.

Detailed description of Malicious Call Trace

This section provides a detailed description of the Malicious Call Trace (MCT) feature.

MCT has three distinct phases:

- Activation
- Control
- Deactivation

Activation

A user or an attendant can use either a feature button (**mct-act**) or a Feature Access Code (FAC) to activate MCT. Either the recipient of the call, or another user or attendant, can activate MCT.

Control

When a user or an attendant activates MCT, the system notifies potential MCT controllers. A potential MCT controller is a user or an attendant who is assigned a feature button (**mct-contr**) that can control MCT. To notify the potential MCT controllers, the system:

- Generates an alerting tone.

  The alerting tone is not a call and does not affect any queues at the telephone.
- Flashes the lamp that is associated with the **mct-contr** button.

The first user or attendant who presses an **mct-contr** button becomes the MCT controller for the call, and the system stops alerting other potential MCT controllers.

MCT begins to trace an incoming call when the controller dials the 3-digit equipment location of the incoming trunk.

While the system generates an alerting tone, the display of the controller shows the message **Malicious Call Trace Request**. While this message is on the display, the display shows no information on incoming calls. When the MCT controller presses the **mct-contr** button again, the system displays information that identifies the called party. As the controller continues to push the button, the system displays the remaining MCT information.

Some of the information that the system displays depends upon the origin of the call:

- If the call originates inside the system, or on the same node within a Distributed Communications System (DCS) network, the software displays the calling number.
- If the call originates outside the system and an Integrated Services Digital Network (ISDN) calling number identification is available on the incoming trunk, the software displays the calling number.
- For all other calls, the software displays the location of the incoming trunk-equipment. In this case, the user must call the connecting server to obtain more information about the malicious call.

For all calls, the software displays the called number, the activating number, whether the call is active, and identification of any other parties who are on the call.

Deactivation

The MCT controller dials the FAC for MCT deactivation to deactivate MCT. Deactivation frees any blocked resources that were involved in the trace. When all parties hang up, the system disconnects the MCT voice recorder.

MCT voice recorder

The MCT voice recorder can be any standard audio cassette player that the Avaya Auxiliary Trunk board can control.

To record a call, manually place the MCT voice recorder in Record MCT mode, and then activate MTC. The activated feature uses the control signal interface of the auxiliary trunk that is connected to the MCT voice recorder to apply power to the recorder.

Note that the system temporarily removes any Bridging, Conference, or Intrusion tones during the time that the MCT voice recorder is connected.

Administering Malicious Call Trace

The following steps are part of the administration process for the Malicious Call Trace feature:

- Assigning an MCT feature button for an attendant
- Assigning an MCT feature button for a user
- Administering MCT for ISDN notification

This section describes:

- Any prerequisites for administering the Malicious Call Trace feature
- The screens that you use to administer the Malicious Call Trace feature
- Complete administration procedures for the Malicious Call Trace feature

Prerequisites for administering Malicious Call Trace

You must complete the following actions before you can administer the Malicious Call Trace feature:

- View the Optional Features screen, and ensure that the **Malicious Call Trace?** field is set to **y**. If the **Malicious Call Trace?** field is set to **n**, your system is not enabled for the MCT feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- Ensure that a Class of Restriction (COR) that enables your users to use the MCT feature exists on your system. The MCT feature requires a COR with the **Access to MCT?** field set to **y**.

  For information about COR administration, see the Class of Restriction feature description.

- Ensure that Feature Access Codes (FACs) to activate and deactivate the MCT feature exist on your system. The MCT feature requires the following FACs:

  — **Malicious Call Trace Activation**

  — **Malicious Call Trace Deactivation**

  For information about FAC administration, see the "Feature Access Code (FAC)" feature description.

Screens for administering Malicious Call Trace

Screen name	Purpose	Fields
Attendant Console	Assign feature buttons for MCT activation and control.	• **mct-act** • **mct-contr**
Class of Restriction	Define a Class of Restriction (COR) that allows MCT.	• **Access to MCT?**
FAC	Specify the Feature Access Codes (FACs) for MCT activation and deactivation.	• **Malicious Call Trace Activation** • **Malicious Call Trace Deactivation**
Malicious Call Trace Control Extensions	Specify the extensions that can use the mct-contr feature button.	All
ISDN-BRI Trunk Circuit Pack	Administer ISDN MCT notification for an ISDN trunk group.	• **Cntry/Peer Protocol** • **Interface**
DS1 Circuit Pack	Administer ISDN MCT notification for an DS1circuit pack.	• **Country Protocol** • **Protocol Version** • **Peer Protocol**
Optional Features	Enable MCT.	**Malicious Call Trace?**
Station	Assign an **Mct-act** and an **Mct-contrl** feature button for a user.	Any available button field in the **Button Assignments** area
Feature-Related System Parameters	Specify that an MCT controller hears a tone when the MCT voice recorder is active.	**Apply MCT Warning Tone?**
	Assign the trunk group for MCT voice recorders.	**MCT Voice Recorder Trunk Group**
	Specify the wait time or a release message.	**Delay Sending Release (seconds)**

Defining Malicious Call Trace on your system

To ensure that an MCT is defined on the Feature-Related System Parameters screen.

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Apply MCT Warning Tone?** field (Figure 283: Feature-Related System Parameters screen on page 1151).

Figure 283: Feature-Related System Parameters screen

```
change system-parameters features                                    page 5
                          FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
               System Printer Endpoint: ____              Lines Per Page: 60
                   EIA Device Bit Rate: 9600

Emergency Extension Forwarding (min): 10

SYSTEM-WIDE PARAMETERS
                          Switch Name: _________________



MALICIOUS CALL TRACE PARAMETERS
                Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group: ___
      Delay Sending Release (seconds)?
SEND ALL CALLS OPTIONS
           Send All Calls Applies to: station
      Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? n
                                            UCID Network Node ID: ___
```

3. In the **Apply MCT Warning Tone?** field, perform one of the following actions:
   - If you want the system to generate a tone at the telephone that controls MCT when the MCT voice recorder is active, type **y**.
   - If you do not want the system to generate a tone at the telephone that controls MCT when the MCT voice recorder is active, type **n**.
4. In the **MCT Voice Recorder Trunk Group** field, type the trunk group for MCT voice recorders.
   - For DEFINITY R, CSI, and S1, valid entries are a number from **1** to **666**.
   - For the IP-PNC servers, valid entries are a number from **1** to **2000**.
5. In the **Delay Sending Release (seconds)** field, type the number of seconds that the server waits to send an ISDN release message, after the server receives an ISDN disconnect message.
   - Valid entries are 0, 10, 20, or 30.

   The system displays this field only if the **Malicious Call Trace?** field on the Optional Features screen is set to **y**.

6. Press **Enter** to save your changes.

Next, you need to ensure that you define the extensions on your system that can use a feature button to control MCT.

To ensure that the extensions on your system that can use a feature button to control MCT:

1. Type **`change mct-group-extensions`**. Press **Enter**.

   The system displays the Malicious Call Trace control extensions screen (Figure 284: Malicious Call Trace Control Extensions screen on page 1152).

Figure 284: Malicious Call Trace Control Extensions screen

```
 change mct-group-extensions
                                                              Page 1 of 1
Extensions Administered to have an MCT-Control Button:
 1: ________ 19: ________ 37: ________ 55: ________ 73: ________  91: ________
 2: ________ 20: ________ 38: ________ 56: ________ 74: ________  92: ________
 3: ________ 21: ________ 39: ________ 57: ________ 75: ________  93: ________
 4: ________ 22: ________ 40: ________ 58: ________ 76: ________  94: ________
 5: ________ 23: ________ 41: ________ 59: ________ 77: ________  95: ________
 6: ________ 24: ________ 42: ________ 60: ________ 78: ________  96: ________
 7: ________ 25: ________ 43: ________ 61: ________ 79: ________  97: ________
 8: ________ 26: ________ 44: ________ 62: ________ 80: ________  98: ________
 9: ________ 27: ________ 45: ________ 63: ________ 81: ________  99: ________
10: ________ 28: ________ 46: ________ 64: ________ 82: ________ 100: ________
11: ________ 29: ________ 47: ________ 65: ________ 83: ________
12: ________ 30: ________ 48: ________ 66: ________ 84: ________
13: ________ 31: ________ 49: ________ 67: ________ 85: ________
14: ________ 32: ________ 50: ________ 68: ________ 86: ________
15: ________ 33: ________ 51: ________ 69: ________ 87: ________
16: ________ 34: ________ 52: ________ 70: ________ 88: ________
17: ________ 35: ________ 53: ________ 71: ________ 89: ________
18: ________ 36: ________ 54: ________ 72: ________ 90: ________
```

2. In any numbered field, type the extension of a user or an attendant console that you want to have an **mct-contr feature** button.

   For every extension and attendant console that you administer, you must assign an **mct-act** and an **mct-contr** feature button. You assign these buttons for the attendant on the Attendant Console screen, and for the user on the Station screen.

3. Press **Enter** to save your changes.

Assigning an MCT feature button for an attendant

To assign an MCT feature button for an attendant:

1. Type **change attendant *n***, where ***n*** is the number of the attendant to which you want to assign an MCT feature button. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 285: Attendant Console screen on page 1153).

Figure 285: Attendant Console screen

```
change attendant 1                                          Page 3 of 4

                                ATTENDANT CONSOLE
FEATURE BUTTON ASSIGNMENTS
  1: split_____                          13: __________
  2: mct-act___                          14: __________
  3: mct-contr_                          15: __________
  4: __________                          16: __________
  5: __________                          17: __________
  6: hold _____ *                        18: __________
  7: __________                          19: forced-rel
  8: aux-work      RC:    Grp:           20: __________
  9: __________                          21: __________
 10: __________                          22: __________
 11: __________                          23: night-serv *
 12: __________                          24: pos-busy__ *
```

3. Type **mct-act** next to the button number that you want the attendant to use to activate MCT.
4. Type **mct-contr** next to the button number that you want the attendant to use to establish control of the malicious call, and to display information about the call.
5. Press **Enter** to save your changes.

Assigning an MCT feature button for a user

To assign an MCT feature button for a user:

1. Type **change station *n***, where ***n*** is the number of the station to which you want to assign an MCT feature button. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 286: Station screen on page 1154).

Figure 286: Station screen

```
change station 20001                                        Page   3 of 4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                      Cord Length: 0
   Building:                                        Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          5: mct-contr
 2: call-appr                          6:
 3: call-appr                          7:
 4: mct-act                            8:
```

3. Type **mct-act** next to the button number that you want the user to use to activate MCT.
4. Type **mct-contr** next to the button number that you want the user to use to establish control of the malicious call, and display information about the call.
5. Press **Enter** to save your changes.

Administering MCT for ISDN notification

To administer MCT for ISDN notification:

1. Type **add ds1 *n***, where ***n*** is the number of the DS1 circuit pack that you want to add. Press **Enter**.

   The system displays the DS1 Circuit Pack screen (Figure 287: DS1 Circuit Pack screen on page 1155).

Figure 287: DS1 Circuit Pack screen

```
add ds1 xxxxxx                                              Page 1 of 2

                              DS1 CIRCUIT PACK

            Location: _____                        Name: ________________
            Bit Rate: _____                  Line Coding: ____
   Line Compensation: _                      Framing Mode: ___
      Signaling Mode: ___________              D-Channel: __
             Connect: _________                Interface: ___________
        Interconnect: ___                   Peer Protocol: ________
   TN-C7 Long Timers? _                  Country Protocol: ____
                                         Protocol Version: _
 Interface Companding: _____                        CRC? _
           Idle Code: ________
                                 DCP/Analog Bearer Capability: ________
                                         T303  Timer(sec):

   MMI Cabling Board: _____  MMI Interface: ESM

MAINTENANCE PARAMETERS

      Slip Detection? _                 Near-end CSU Type: ________
```

2. In the **Country Protocol** field, perform one of the following actions:
   - If the DS1 is connected to a public network in Australia, type **2**.
   - If the DS1 is connected to a public network that supports the ETSI Malicious Call Trace Identification (MCID) service according to EN 300 130, type **etsi**.
   - If the DS1 is connected to a private network of servers that run Communication Manager, type **1**.
3. In the **Peer Protocol** field, type **q-sig**, if the DS1 is connected to a private network of servers that run Communication Manager.

   The system displays the **Peer Protocol** field when the:
   - **Signaling Mode** field is set to **isdn-pri**
   - **Connect** field is set to **pbx**
   - **Interface** field is set to either **peer-master** or **peer-slave**
4. To administer other fields on the DS1 Circuit Pack screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
5. Press **Enter** to save your changes.

6. Type **change bri-trunk-board**. Press **Enter**.

   The system displays the ISDN-BRI Trunk Circuit Pack screen (Figure 288: ISDN-BRI Trunk Circuit Pack screen on page 1156).

Figure 288: ISDN-BRI Trunk Circuit Pack screen

```
change bri-trunk-board                                          Page 1 of 1
                        ISDN-BRI TRUNK CIRCUIT PACK

             Location: 01A09                          Name: _______________
  Interface Companding: a-law_  DCP/Analog Bearer Capability: 3.1kHz
 T3 Timer Length (sec): 15_


Port  Interface  Side  Cntry/Peer TEI  Time  Invert Synch   Layer 1  Detect
                       Protocol       Fill  Bits?  Source? Stable?  Slips?
  1:  user_______        12__     0__  flags   n       n       n       n
  2:  network____        etsi     0__  ones_   y       y       y       y
  3:  user_______        2___     auto flags   y       n       y       n
  4:  peer-slave_  b     QSIG     0__  flags   n       y       y       n
  5:  peer-master  a     QSIG     auto ones_   n       n       n       n
  6:  ___________        ____     0__  ones_   n       n       y       n
  7.  ___________        ____     0__  ones_   n       n       y       n
  8:  ___________        ____     0__  ones_   n       n       y       n
```

7. In the **Cntry/Peer Protocol** field, type **2** if the ISDN-BRI circuit pack is connected to a public network in Australia.
   Type **etsi** if the ISDN-BRI circuit pack is connected to a public network that supports the ETSI Malicious Call Trace Identification (MCID) service according to EN 300 130.
8. In the **Interface** field, type either **peer-master** or **peer-slave**, if the ISDN-BRI circuit pack is connected to a private network of servers that run Communication Manager.
9. To administer other fields on the ISDN-BRI Trunk Circuit Pack screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.
10. Press **Enter** to save your changes.

Note:

You must set the **Supplementary Service Protocol** field on the ISDN Trunk Group screen to **a** for Australia and **c** for ETSI.

End-user procedures for Malicious Call Trace

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Manual Signaling:

- Activating MCT with a feature button when you receive a malicious call
- Activating MCT with a FAC when you are active on a call
- Activating MCT with a FAC when you are not active on a call
- Requesting that an MCT controller on a tandemed server continue the trace
- Displaying MCT information
- Deactivating MCT

Activating MCT with a feature button when you receive a malicious call

To activate MCT with a feature button when you receive a malicious call:

- Press the **mct-act** feature button.

Activating MCT with a FAC when you are active on a call

To activate MCT with a Feature Access Code (FAC) when you are active on a call:

1. Place the call on hold, transfer, or conference.
2. Get a second call appearance.
3. Dial the FAC to activate MCT.
4. When you hear the dial tone, perform one of the following actions:
   - Dial your extension.
   - Press the pound key (#).

     If you press the pound key (#), the system traces the call at your extension.
5. Wait 10 seconds to hear the confirmation tone that the system generates.

Activating MCT with a FAC when you are not active on a call

To activate MCT with a FAC when you are not active on a call:

1. Dial the FAC to activate MCT.
2. Perform one of the following actions:
   - Dial the extension number that received the malicious call.
   - Dial a trunk access code (TAC) and the subsequent member number.

Requesting that an MCT controller on a tandemed server continue the trace

To request that a controller on a tandemed server continue the trace:

1. Contact the controller on the tandemed server.
2. Provide the trunk port ID that you want the controller on the tandemed server to trace
3. The controller on the tandemed server:
   a. Activates MCT
   b. Presses the star key (*)
   c. Dials the trunk port ID

      Dial letters A through E of the port ID as the numbers 1 through 5. For example, to dial the trunk port ID 01C0401 press **0130401**.

Displaying MCT information

To display MCT information on a telephone that has a display panel:

1. Press the **mct-contrl** button.
2. Continue to press the button to display all the information that is available about the malicious call.

Deactivating MCT

To deactivate MCT:

- The MCT controller dials the FAC that deactivates MCT.

  The system generates confirmation tone, extinguishes all lamps that are related to the MCT call, and disconnects the MCT voice recorder, if a voice recorded was used on the call.

Reports for Malicious Call Trace

The following reports provide information about the Malicious Call Trace (MCT) feature:

- The MCT History report provides information about an MCT incident. This information includes the date and time, the controller and the recorder, the parties who were involved on the call, and whether or not the public network was notified about the call.

For detailed information on these reports and the associated commands, see *Avaya Aura™ Communication Manager Reports*, 555-233-505.

Considerations for Malicious Call Trace

This section provides information about how the Malicious Call Trace (MCT) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of MCT under all conditions. The following considerations apply to MCT

- If the originator of the call hangs up, the system discontinues MCT. However, if the recipient of the call hangs up, the system does not discontinue MCT.
- Except for Emergency Access to the Attendant, features that usually display information do not display information on the telephone of the MCT controller, when MCT is activated. Except for the display of information, these features function normally until MCT is deactivated.
- Do not use a Feature Access Code (FAC) to activate MCT because this requires too much time.
- Visually Impaired Attendant Service (VIAS) provides spoken display information for MCT activation, but not for MCT control.
- MCT information on an active malicious call is lost if a server fails while MCT is activated.
- When you request help from a controller on a tandemed server, consider the following possibilities:
  - The malicious caller might hear a warning tone as a result of the intrusion.
  - You can lose continuity on the trace if the person who activates MCT on the tandemed server is not the MCT controller.

- If a malicious call comes in on a non-ISDN trunk, the controller must have the telephone number for the connecting server and a cross-reference of system-trunk port numbers. The controller might also need the DS1 channel number.

Interactions for Malicious Call Trace

This section provides information about how the Malicious Call Trace (MCT) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Malicious Call Trace in any feature configuration.

- Bridged Call Appearance

  The system records the primary extension as the MCT recipient when MCT is activated at a bridged call appearance, or for a bridged call appearance.

- Conference

  A user can use conferencing to place a malicious caller on hold. The user can start a conference, dial the Feature Access Code (FAC) that activates MCT, and then stop conferencing and return to the call appearance of the malicious caller.

  MCT can be activated for a member of a conference. The MCT activation is unaffected by the number of parties on the conference.

- Centralized Attendant Service (CAS)

  The activation, control, and deactivation of MCT for a call must occur on the same server.

- Distributed Communications System (DCS)

  If a telephone in a DCS network is involved in a malicious call, the system records and displays the extension with the MCT information. MCT notification passes over ISDN-PRI DCS trunks, but the activation, control, and deactivation of MCT must be performed by telephones that are on the same DCS node.

- Emergency Access to the Attendant

  Usually, during MCT-Control, no other feature can access the display of the controlling telephone. However, MCT gives up control of the display until an Emergency Access call is completed.

- Make-Busy/Position-Busy/Send All Calls

  The software attempts to activate Make-Busy or Position-Busy for telephones or consoles that activate MCT-Control. If a user has a Send All Calls (SAC) button administered but not active for the primary extension on the phone, SAC activates when the user activates MCT-Control. When the user deactivates MCT, SAC remains active until the user deactivates SAC.

- Music-On-Hold

  If an agent places a malicious call that is being recorded on hold, and the call goes to music-on-hold, the music-on-hold port and the MCT voice recorder port can lock. In this case, the MCT voice recorder continues to record the music-on-hold and is unavailable to record subsequent malicious calls. You must busy out or release the MCT voice recorder port to drop the connection.

- Priority Calling

  The system denies a priority call to an MCT recipient.

- QSIG Global Networking

  MCT notification passes over tandem, tie, access, and DMI-BOS ISDN QSIG trunk groups. QSIG supplementary services name and number ID provide the name and the telephone number of a malicious caller.

- Transfer

  If a user transfers a malicious call, the MCT information that the system displays on the telephone of the MCT controller identifies the party that is transferred as the MCT recipient.

- Trunk Access Code (TAC)

  To activate MCT for a TAC, a user must have an **mct-contr** feature button administered. The user hears a dial tone and enters the trunk-member number for the trunk group that the TAC identified. The user then becomes the MCT controller for a call that involves the identified trunk member. This TAC operation is useful when users must trace a call that tandemed through their server or switch to terminate on another server or switch.

- Trunk Groups

  If a personal central office line (PCOL) is involved in a malicious call trace, the software might hold up the trunk until the MCT deactivates.

Manual Message Waiting

Use the Manual Message Waiting feature to cause the Manual Message Waiting button lamp at another user telephone to light.

Detailed description of Manual Message Waiting

This section provides a detailed description of the Manual Message Waiting feature.

A user presses the designated button to light the Manual Message Waiting button lamp at the telephone of another user telephone. Both the telephones must be multiappearance telephones. To turn the lamp off, either telephone user can press the Manual Message Waiting button.

You can administer Manual Message Waiting for pairs of telephones only. These telephones might be used by two people who share the same job function and often take calls for one another. The Manual Message Waiting feature is also useful in situations where one person usually answers calls for a second person, such as an administrative assistant might do for a manager. The administrative assistant can press a Manual Message Waiting button to signal the manager that a call must be answered. The manager can answer the call or press a Manual Message Waiting button to indicate that the administrative assistant should handle the call

Administering Manual Message Waiting

The following steps are part of the administration process for the Manual Message Waiting feature:

- Assigning the Manual Message Waiting feature button

This section describes:

- Any prerequisites for administering the Message Waiting feature
- The screens that you use to administer the Message Waiting feature
- Complete administration procedures for the Message Waiting feature

Screens for administering Manual Message Waiting

Screen name	Purpose	Fields
Station (multiappearance)	Assign the **man-msg-wt** feature button for a user.	Any available button field in the **Button Assignments** area

Assigning the Manual Message Waiting feature button

To assign a Manual Message Waiting feature button for a user:

1. Type **change station *n***, where ***n*** is the extension of the user to whom you want to assign a Manual Message Waiting feature button. Press **Enter**.

   The system displays the Station screen for the extension that you requested.

2. Click **Next** until you see the **Button Assignments** area (Figure 289: Station screen on page 1164).

Figure 289: Station screen

```
                                   STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:


ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                             7:
 2: call-appr                             8:
 3: call-appr                             9:man-msg-wt
 4:                                      10:dn-dst
 5:                                      11:goto-cover
 6:                                      12:send-calls Ext:
```

3. In the **Button Assignments** area, type **man-msg-wt** next to the button that you want the user to use for Manual Message Waiting.

4. Press **Enter** to save your changes.

Manual Signaling

Use the Manual Signaling feature to signal another user.

Detailed description of Manual Signaling

This section provides a detailed description of the Manual Signaling feature.

With the manual signaling feature, one user can signal another user. When a user presses the manual signaling button, the other user hears a 2-second ring. The status lamp of the user who presses the button lights for two seconds.

If the telephone of the intended recipient of the signal is already alerting, the system:

- Does not generate the 2-second ring
- Causes the manual signaling button lamp of the user who presses the button to flicker briefly

Administering Manual Signaling

The following steps are part of the administration process for the Manual Signaling feature:

- Assigning a manual signaling button for a multiple-call appearance telephone user

This section describes:

- Any prerequisites for administering the Manual Signaling feature
- The screens that you use to administer the Manual Signaling feature
- Complete administration for the Manual Signaling feature

Screens for administering Manual Signaling

Screen name	Purpose	Fields
Station (multiappearance)	Assign a **signal** button to the telephone of a user, and specify the extension that rings when the user presses the button.	Any available button field in the **Button Assignments** area

Assigning a manual signaling button for a multiple-call appearance telephone user

To assign a manual signaling button for a multiple-call appearance telephone user:

1. Type **change station *n*** where ***n*** is the telephone number of the extension to which you want to assign a manual signaling button. Press **Enter**.

   The system displays the Station screen for the extension that you requested.

2. Click **Next** until you see the **Button Assignments** area (Figure 290: Station screen on page 1168).

Figure 290: Station screen

```
change station 32006                                          Page   3 of   4
                                    STATION
 SITE DATA
      Room:                                            Headset? n
      Jack:                                            Speaker? n
     Cable:                                           Mounting: d
     Floor:                                       Cord Length: 0
  Building:                                         Set Color:




ABBREVIATED DIALING
     List1: personal 1         List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                            5: signal     Ext:
 2: call-appr                            6:
 3: call-appr                            7:
 4:                                      8:
```

3. Type **signal** next to the number of the button that you want the user to use for manual signaling.

   When you type **signal** next to the button number, the system displays an **Ext:** field.
4. Type the extension of the recipient of the signal in the **Ext:** field.
5. Press **Enter** to save your changes.

End-user procedures for Manual Signaling

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Manual Signaling:

To use manual signaling:

- Press the manual **signal** button.

Interactions for Manual Signaling

This section provides information about how the Manual Signaling feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Manual Signaling in any feature configuration.

- Data Modules

  If you administer a manual signaling button for a data module, the system denies any attempt to activate the button.
- Vector Directory Number (VDN)

  A manual signaling button cannot point to a VDN.

Meet-me Conference

Use the Meet-me Conference feature to set up a dial-in conference of up to six parties. The Meet-me Conference feature uses Call Vectoring to process the setup of the conference call.

Detailed description of Meet-me Conference

This section provides a detailed description of the Meet-me Conference feature.

With the Meet-me Conference feature, a station user can host a dial-in conference of up to six parties. You can set up the Meet-me Conference extension to require an access code. If you administer an access code, all parties must correctly enter the access code to join the conference. If the extension is one of your Direct Inward Dialing (DID) numbers, any internal or remote access users, or external parties, can dial the Meet-me Conference extension.

When a caller dials into a Meet-me Conference, the system plays an announcement. The announcement tells the caller to enter an access code, if an access code is required. If the caller enters the correct access code, the caller is added to the conference. If no other parties are on the conference, an announcement tells the caller that he is the first caller to join the conference. If other parties are already on the call, an announcement tells the caller that he is joining a conference that is already in progress. All parties who are already on the conference and the newly added party hear an entry tone. When a party drops out of the conference, the remaining parties hear an exit tone.

Administering Meet-me Conference

The following steps are part of the administration process for the Meet-me Conference feature:

- Creating or changing a Meet-me Conference vector
- Creating a Meet-me Conference VDN

This section describes:

- Any prerequisites for administering the Meet-me Conference feature
- The screens that are required to administer the Meet-me Conference feature
- Complete administration procedures for the Meet-me Conference feature

Prerequisites for administering Meet-me Conference

You must complete the following actions before you can administer the Meet-me Conference feature:

- On the Optional Features screen, ensure that the **G3 Version** field is set to **V11** or later. If the **G3 Version** field is not set to **V11** or later, your system is not enabled for the Meet-me Conference feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- On the Optional Features screen, click **Next** until you see the **Enhanced Conferencing** field. Ensure that this field is set to **y**. If the **Enhanced Conferencing** field is set to **n**, your system is not enabled for the Meet-me Conference feature. Contact your Avaya representative before you continue with this procedure.

Screens for administering Meet-me Conference

Screen Name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 1.3 (V11) or greater.	**G3 Version**
	Ensure that Enhanced Conferencing is enabled.	**Enhanced Conferencing**
Call Vector	Create a Meet-me Conference vector.	All
Vector Directory Number	Set up a VDN for Meet-me Conference.	• **Extension** • **Name** • **Vector Number** • **Meet-me Conferencing** • **Conference Access Code** • **Conference Controller**
Meet-me Vector Directory Number	View a list of existing Meet-me Conference VDNs.	All

Creating or changing a Meet-me Conference vector

To create or change a vector for a Meet-me Conference:

1. Type **change vector *n***, where ***n*** is the number of the vector that you want to create or change. Vector numbers must be between 1 and 256. Press **Enter**.

   The system displays the Call Vector screen (Figure 291: Call Vector screen on page 1173).

Figure 291: Call Vector screen

```
 change vector 129                                              Page 1 of 3
                                  CALL VECTOR
   Number: 129              Name: _______________
Multimedia? n     Attendant Vectoring? n     Meet-me Conf? y           Lock? n
     Basic? y  EAS? n   G3V4 Enhanced? y    ANI/II-Digits? y   ASAI Routing? n
 Prompting? y  LAI? n  G3V4 Adv Route? y    CINFO? y   BSR? n      Holidays? n

  01 _____________
  02 _____________
  03 _____________
  04 _____________
  05 _____________
  06 _____________
  07 _____________
  08 _____________
  09 _____________
  10 _____________
  11 _____________
```

2. In the **Meet-me Conf** field, type **y** to designate the vector as a Meet-me Conference vector.
3. Use the numbered fields to create or change a Meet-me Conference vector, as shown in the examples in Figure 291: Call Vector screen on page 1173 and Figure 292: Call Vector screen on page 1174. See Options for creating vector steps on page 1175 and How the vector processes a call on page 1176 for more information on how to create a vector.

Figure 292: Call Vector screen

```
change vector 90                                                Page  1 of 3

                                  CALL VECTOR

    Number: 90                    Name: Enh Conf Vec
                  Attendant Vectoring? n    Meet-me Conf? y           Lock? y
    Basic? y    EAS? n   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? n
Prompting? y    LAI? n  G3V4 Adv Routs? n   CINFO? n   BSR? n   Holidays? n

01 collect       6 digits after announcement 12340
02 goto          step 6 if digits = meet-me-access
03 collect       6 digits after announcement 12341
04 goto          step 6 if digits = meet-me-access
05 disconnect    after announcement 12342
06 goto          step 11 if meet-me-idle
07 goto          step 14 if meet-me-full
08 announcement  12343
09 route-to      meetme
10 stop
11 announcement  12344
```

Figure 293: Call Vector screen

```
 change vector 90                                               Page  2 of 3

                                  CALL VECTOR

    Number: 90                    Name: Enh Conf Vec
                  Attendant Vectoring? n    Meet-me Conf? y           Lock? y
    Basic? y    EAS? n   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? n
Prompting? y    LAI? n  G3V4 Adv Routs? n   CINFO? n   BSR? n   Holidays? n

12 route-to      meetme
13 stop
14 disconnect    after announcement 12345
15 stop
16
17
18
19
20
21
22
```

4. Press **Enter** to submit the vector.

Note:

If a vector allows a new party to join a conference immediately, and the party is an H.323 IP trunk user, the caller might not have a talk path with the other parties in the conference. To prevent this situation, include a short delay in the vector at a point before a new party joins the Meet-me Conference. This delay can be a step to collect digits, a 1-second delay, or an announcement. Since Meet-me vectors are always configured with announcements and digit collections, this situation is rarely an issue.

Options for creating vector steps

- **collect**

  When the **Meet-me Conf** field is enabled, the **collect** vector step collects the next six digits. The vector step then uses those digits as the access code for a Meet-me Conference call. See vector steps 1 and 3 in the example in Figure 292: Call Vector screen on page 1174.

- **goto**

  The **goto** vector step has three conditions:

  – meet-me-idle

    The meet-me-idle condition routes the first caller who accesses a Meet-me Conference to the conference call. An announcement step that tells the caller that he is the first party to join the conference can be played. See vector steps 6 and 11 in the example in Figure 292: Call Vector screen on page 1174.

  – meet-me-full

    The meet-me-full condition is used when the Meet-me Conference already has the maximum of six parties on the call. See vector steps 7 and 14 in the example in Figure 293: Call Vector screen on page 1174.

  – meet-me access

    The meet-me access condition ensures that the access code is valid. If the access code that the caller dials is the same as the access code that is administered for the VDN, vector processing continues. See vector steps 2 and 4 in the example in Figure 292: Call Vector screen on page 1174.

- **route-to**

  The **route-to** vector step has one condition:

– meetme

This condition adds the caller to the Meet-me Conference call, and all parties on the call hear an entry tone. The meetme condition is valid when the caller enters the correct access code, and the number of parties who are on the call already is less than six. See vector steps 9 and 12 in the example in Figure 293: Call Vector screen.

If the **route-to meetme** step fails, vector processing stops, and the caller hears a busy tone.

How the vector processes a call

This section describes what occurs when a caller dials the Meet-me Conference telephone number that is managed by the vector in Figure 292: Call Vector screen on page 1174 and Figure 293: Call Vector screen on page 1174.

The caller hears announcement 12340. Announcement 12340 says, "Welcome to the Meet-me Conferencing service. Enter your conference access code." The caller dials the access code 937821. The **collect** vector step 1 collects the access code digits. If the access code is valid, the vector processing continues with vector step 6.

If the access code is invalid, vector step 3 plays announcement 12341. Announcement 12341 says, "The access code you entered is invalid. Please enter the access code again."

If the caller dials the wrong access code again, vector step 5 plays announcement 12342. Announcement 12342 says, "This access code is invalid. Please contact the conference call coordinator to make sure you have the correct conference telephone number and access code. Goodbye." The caller is disconnected.

Vector step 6 is only valid for the first caller into the Meet-me Conference. The meet-me-idle condition routes the first caller to announcement 12344, according to vector step 11. The announcement says, "You are the first party to join the call." The system then routes the caller to the Meet-me Conference call by vector step 12, and vector processing stops.

Vector step 7 is used when the Meet-me Conference maximum of six parties are already on the call. The meet-me-full condition disconnects the caller after announcement 12345 plays, according to vector step 14. Announcement 12345 says, "This Meet-me Conference is filled to capacity. Please contact the conference call coordinator for assistance. Goodbye."

If a caller dials the correct access code, is not the first caller, and the conference is not full, processing continues with vector step 8. Announcement 12343 plays. The announcement says, "Your conference call is already in progress." The system then routes the caller to the Meet-me Conference call by vector step 9, and vector processing stops.

When a caller enters the conference, all parties on the call hear an entry tone. When a party drops out of the conference, the remaining parties hear an exit tone.

Creating a Meet-me Conference VDN

To create a Meet-me Conference vector directory number (VDN):

1. Type **add vdn next**, or **add vdn *n***, where ***n*** is the extension that you want to use for the VDN. Note that if the VDN extension is one of your Direct Inward Dialing (DID) numbers, external users can access the conference VDN. If the VDN extension is not part of the DID block, only internal callers on the network, or remote access callers, can access the conference. Press **Enter**.

   The system displays the Vector Directory Number screen (Figure 294: Vector Directory Number screen on page 1177).

Figure 294: Vector Directory Number screen

```
                          VECTOR DIRECTORY NUMBER

                            Extension: 36090
                                 Name: Meet-me Conference VDN
                       Vector Number: 90

                 Meet-me Conferencing? y

                                 COR: 1
                                  TN: 1
```

2. In the **Extension** field, type the extension for the VDN. Or, if you typed the extension in Step 1 as part of the **add vdn** command, the system automatically displays the extension in the **Extension** field.
3. (Optional) In the **Name** field, type a name of up to 27 characters to identify this VDN.
4. In the **Vector Number** field, type the number for this vector. Or, if you typed **add vdn next** in Step 1, the system automatically displays the next available vector number in the **Vector Number** field.
5. In the **Meet-me Conferencing** field, type **y**.
6. Click **Next** until you see the Meet-me Conference Parameters page of the Vector Directory Number screen (Figure 295: Meet-me Conference Parameters screen on page 1178).

Figure 295: Meet-me Conference Parameters screen

```
                          VECTOR DIRECTORY NUMBER

                MEET-ME CONFERENCE PARAMETERS:

                  Conference Access Code: 937821
                   Conference Controller: 80214
```

7. In the **Conference Access Code** field, assign a 6-digit access code for the Meet-me Conference. Avaya recommends that you always assign an access code for a Meet-me Conference. However, if you do not want to assign an access code, leave the **Conference Access Code** field blank. Once you assign an access code, the system displays an asterisk (*) in this field for subsequent change, display, or remove operations by all users except the init superuser login. An administrator who uses the init login sees the actual access code instead of an asterisk.
8. In the **Conference Controller** field, type the extension of the person who is responsible to control or change the Meet-me Conference access code. If you type an extension, a user at that extension can use a Feature Access Code (FAC) to change the access code. If you leave the **Conference Controller** field blank, any station user to whom console permissions are assigned can change the access code. Remote access users can also use a FAC to change a Meet-me Conference access code.
9. Press **Enter** to submit the VDN.

To view a list of existing Meet-me Conference VDNs:

- Type **`list meet-me-vdn`**. Press **Enter**.

  The system displays the Meet-me Vector Directory Number screen (Figure 296: Meet-me Vector Directory Number screen on page 1179).

  An asterisk (*) in the **Access Code** field indicates that an access code is assigned for that Meet-me VDN. If the **Access Code** field is blank, no access code is assigned. An administrator who uses the *init* login sees the actual access code instead of an asterisk.

Figure 296: Meet-me Vector Directory Number screen

```
list meet-me-vdn

                    MEET-ME VECTOR DIRECTORY NUMBER

                                    Access          Vec Control
Name                             Ext  Code  COR  TN  Num   Ext

Secure Meet-me Conference       4000   *     1    1   1
Nonsecure Meet-me Conference    4006         1    1   2    84590
```

End-user procedures for Meet-me Conference

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures:

- Accessing a Meet-me Conference as an attendee
- Changing a Meet-me Conference access code
- Using Selective Conference Party Display, Drop, and Mute

Accessing a Meet-me Conference as an attendee

To access a Meet-me Conference as an attendee:

1. Dial the Meet-me Conference telephone number. If an access code is required, a recorded announcement tells you to enter the access code.
2. Enter the Meet-me Conference access code.

   The system verifies the access code, and connects you to the Meet-me Conference. You hear an entry tone when you join the conference.

If the maximum of six parties are already connected to the Meet-me Conference, a recorded announcement tells you that the Meet-me Conference is full.

Changing a Meet-me Conference access code

Both local and remote access telephone users can change access codes. However, an access code must first be administered through system administration before a telephone user can change a code. Access codes must be removed through system administration.

To change a Meet-me Conference access code:

1. Dial the Feature Access Code (FAC) for Meet-me Conference.
2. When you hear dial tone, dial the Meet-me Conference VDN, and then press the pound key (#).
3. Dial the current access code, and then press the pound key (#).
4. When you hear dial tone, dial the new access code, and then press the pound key (#).
5. Dial the new access code again, and then press the pound key (#).
6. When you hear the confirmation tone, hang up the telephone.

If any errors occur during this operation, you hear intercept tone, and the access code is not changed. You must start over.

Using Selective Conference Party Display, Drop, and Mute

You can use this feature from a digital display station or from an attendant console. In this example, stations A, C, and D are on a conference call. Caller B is on the conference call that uses an outside trunk or a cellular telephone.

1. Station A presses the Conference Display button.

   The LED for the Conference Display button lights. The station displays the name and the number for station C, if this information is available.
2. Station A can press the Conference Display button repeatedly to cycle through all parties who are on the call.
3. When the name and the number for station C is displayed on station A, station A presses the Drop button, or the Forced Release button on the attendant console.

   Station C is dropped from the conference call. Callers A, B, and D remain on the conference call. The display for station A now shows one of the other parties on the call.
4. Caller B from an outside trunk puts the conference call on hold. This action adds music-on-hold to the conference call.
5. Station A presses the Conference Display button until the station displays the name and the number for Caller B.
6. Station A presses the Far-End Mute button.

Note:
You can activate Far-end Mute only for trunks, and not for telephones.

Caller B is put into "listen-only" mode, and the music-on-hold is removed from the conference call. The Station A display indicates that the outside trunk call (Caller B) is muted.

7. Caller B selects the conference call appearance to return to the conference call. To exit "listen-only" mode, the outside trunk caller presses the pound key (#).

   Caller B is again active on the conference call.

8. Station A presses the Exit button, or the Normal button on the attendant console.

   Station A returns to normal mode. Conference 3 is displayed on station A. If station A is inactive for 60 seconds, Station A returns automatically to normal mode.

If the Selective Conference Party Mute feature is activated without the knowledge of the muted party, that party might think that a problem exists with the connection when no one responds on the conference call. Users must be instructed about this new feature, and how to return to the call if the users are muted. If the muted party does not know how to return to the call, another user on the conference call can use the Far-End Mute button to unmute the party.

Rotary telephone users who are muted by way of the Selective Conference Party Mute feature cannot add themselves back into the conference call. Another user on the conference call must use the Far-End Mute button to unmute the party.

Considerations for Meet-me Conference

This section provides information about how the Meet-me Conference feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the Meet-me Conference feature under all conditions.

- Attendant Intrusion

  An attendant can intrude on a station that is part of a Meet-me Conference, as long as the conference does not already include the maximum number of parties.

- Bridged Appearances

  Bridged appearance users can be added to a Meet-me Conference, and count against the total number of conference parties. As bridged appearance users join a Meet-me Conference, the users are not prompted to provide an access code. Bridged appearance users also receive no announcements, nor are entry or exit tones applied when the users are added to or dropped from the call. Avaya assumes that this scenario would only take place with the knowledge of the user of the appearance that originally dialed into the Meet-me Conference. That user can use the Exclusion feature to prohibit the bridged user from being a part of the Meet-me Conference call.

- Busy Verification

  If the system maximum of stations in a conference call is five or less, a station or an attendant can verify another station that is part of a Meet-me Conference. If the system maximum of stations in a conference call is six, a station or an attendant can verify another station that is part of a
  Meet-me Conference, as long as the conference does not already include the maximum number of parties.

- Call Vectoring

  If a Meet-me Conference VDN is administered to use a vector that has no steps, the call attempt is dropped, and a vector event is generated.

- Capacity issues

  A Meet-me Conference call can have a maximum of six parties on the call. Additional parties cannot join a Meet-me Conference once the maximum of six parties is reached.

- Changing vector types

  To change a Meet-me Conference vector to a non Meet-me Conference vector, you must first remove all vector steps. To change a non-Meet-me Conference vector to a Meet-me Conference vector, you must first remove all vector steps.

- Class of Service (COS)

  A user must have a COS that includes console permissions to change a Meet-me Conference access code from his own telephone.

- Conference

  Parties in a Meet-me Conference call can use the Conference feature to add other parties up to the system conference limit. When the parties are added to the call, the "entry" tone is not given. Two or more Meet-me Conference calls cannot be conferenced together.

- Conference Tone

  The purpose of the conference tone feature is to ensure that no one can be added to a call without the knowledge of the other parties. The Meet-me Conference already has entry and exit tones for all parties who enter the conference through vector processing. If one of the parties conferences in another user through the station Conference feature, the other parties are not aware of the additional party because no entry tone is played. In this scenario, the conference tone should be played if required as part of the system parameters administration.

- Conference/Transfer Toggle/Swap feature limitations

  The Conference/Transfer Toggle/Swap feature is unavailable on analog stations and the attendant console. The attendant console can use the Split Swap feature to perform a similar operation.

  The station user who presses the Toggle Swap button must be in the talk state with one of the parties. If the button is pressed during ringback, the system ignores the button push.

  Telephone users must not use the Selective Conference Party Display feature to scroll too rapidly through the displays. The station hyperactivity feature takes the station out of service if the user repeatedly scrolls through the displays at high enough rates. This action causes the system to reset, and drop the user from the call.

- Disabling Enhanced Conferencing

  To disable the Enhanced Conferencing option on the System Parameters Customer-Options screen, you must first remove all Meet-me Conference VDNs and vectors.

- Drop

  No controlling party exists in a Meet-me Conference. Therefore, if a caller who is on the conference call presses the Drop button, the system ignores the button push, and the last party who joined the conference call is not dropped from the call.

- Far-end Mute

  Only one trunk on a Meet-me Conference bridge can be far-end muted at any given time.

- Removing stations

  You cannot remove a station that is administered as a controlling station for a Meet-me Conference VDN unless you first remove the assignment on the VDN.

- Security issues

  The Meet-me Conference feature can present a potential security problem. If you assign Meet-me Conference VDNs without access codes, a hacker can gain control of Meet-me Conference facilities and keep others from conducting legitimate business. A hacker can also potentially access the system, and use the system to make unauthorized calls. Avaya recommends that you administer access codes, and change the codes regularly to reduce the risk of unauthorized access to the system. If a user tries to change the access code of a Meet-me Conference and is unsuccessful, or uses an invalid access code, the system records an event to the Event Log.

- Service Observing

  Service Observing by way of the VDN is not allowed for Meet-me Conference VDNs.

- Transfer

  When a user transfers a call to a Meet-me Conference, the transfer can be completed during vector processing only when a single party is on soft hold and waiting to be transferred. If two or more parties are on soft hold and waiting to be transferred, the transfer can only be completed after the party who initiates the transfer is connected to the Meet-me Conference.

- Vectoring options

  Attendant Vectoring and Meet-me Conference cannot both be enabled at the same time. If Enhanced Conferencing is enabled, but no other vectoring customer options are enabled, only Meet-me Conference vectors can be assigned. A non Meet-me Conference vector cannot be assigned to a Meet-me Conference VDN. A Meet-me Conference vector cannot be assigned to a non-Meet-me Conference VDN. No restrictions exist with regard to vector "chaining" between Meet-me Conference vectors and non Meet-me Conference vectors. When a call interflows from one type of vector processing to another, the call is removed from any queue, if applicable. The call is treated as a new call to vectoring, instead of a continuation of vectoring.

Interactions for Meet-me Conference

This section provides information about how the Meet-me Conference feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the Meet-me Conference feature in any feature configuration.

- Bridged Appearances

  If a station user who is active on a bridged appearance makes a conference or transfer, the user receives the enhanced displays based on the Class of Restriction (COR) of station of the user, and not the station with the primary extension.

- Call Detail Recording (CDR)

  As parties join a Meet-me Conference, a call record is created, if a record is required by system administration. If a record is required, the called party is the Meet-me Conference VDN number. The duration is the length of time that the party is included in the call. An individual record for each party is generated when the party drops from the call.

  One option for recording all calls to Meet-me Conference VDNs is to activate the Intraswitch CDR feature, and populate all system Meet-me Conference VDN numbers. If you use the Intraswitch CDR feature with the Meet-me Conference VDNs, set the condition code to **C** for all call records. If the Intraswitch CDR feature is inactive for Meet-me Conference VDNs, the creation and the content of call records depends on the trunk group translations for external callers to the Meet-me Conference. Internal callers to the Meet-me Conference do not generate any records if the Intraswitch CDR feature is inactive for either the Meet-me Conference VDN or the calling extension.

- Consult

  If the covering party is talking to the principal after the covering party presses the Consult button, the covering party can use the Toggle Swap button to toggle back and forth between the caller and the principal.

- Direct Inward Dialing (DID)

  If a Meet-me Conference VDN is one of your block of DID numbers, external users can access the conference VDN. If the VDN extension is not part of the DID block, only internal callers on the network or remote access callers can access the conference VDN.

- Pull Transfer

  If station A is talking to station B and station B begins a transfer to station C, only station C can use the Pull Transfer feature to grab the call. Furthermore, if station B uses the Toggle Swap feature to return to station A and station C is now in a soft hold state, station C cannot use the Pull Transfer feature until station B toggles back and has station C in the talk state.

Troubleshooting Meet-me Conference

This section lists the known or common problems that users might experience with the Meet-me Conference feature.

Problem	Possible cause	Action
The conference call drops abruptly for no apparent reason.	The **Vector Disconnect Timer** field on the System Parameters - Features screen is set to a value that is shorter than the duration of the Meet-me Conference session.	Increase the value in the **Vector Disconnect Timer** field.
The sound volume is too low.	The affected conference participants connect through international trunks in which central office (CO) loss plans are set for too much loss.	• Speak closer to the speaker phone. • If you are having conference calls in a large conference room, then use a microphone for the speaker. You can also use Polycom phones that have automatic gain control. • On the Location Parameters screen, adjust the values in the **End-to-End total loss (db) in a n-party conference** field. The loss can be as low as 15DB.

Modem Pooling

Use the Modem Pooling feature to enable switched connections between digital-data endpoints (data modules) and analog-data endpoints by way of pools of acoustic-coupled modems. The analog-data endpoint is either a trunk or a line circuit.

Detailed description of Modem Pooling

This section provides a detailed description of the Modem Pooling feature.

Data transmission between a digital-data endpoint and an analog-data endpoint requires conversion through a modem. Conversion is required because the **D**CP format that the data module uses is not compatible with the modulated signals of an analog modem. A modem translates DCP format into modulated signals and vice versa.

The Modem Pooling feature provides for the use of pools of integrated-conversion modems and combined-conversion modems.

Integrated-conversion modem pools have functionality that is integrated on the Pooled Modem circuit pack, providing two modems. Each one emulates a time-division multiplexing (TDM) cabled to a 212 modem. Integrated are modem pools not available in countries that use A-law companding.

Combined-conversion modem pools are TDMs that are cabled to any TDM-compatible modem. Combined-conversion modem pools can be used with all systems.

When the system needs a modem, the system queries the digital-data module that is associated with the call to determine if the options are compatible with the options that are supported by the modem pools. If the options are incompatible, the originating user receives intercept treatment. If the options are compatible, the system obtains a modem from the appropriate pool. If a modem is unavailable, the user receives reorder treatment.

The system can detect the need for a modem. Data calls from an analog-data endpoint require that the user indicate the need for a modem, because the system considers such calls to be voice calls. Users indicate this need by dialing the data-origination access code before the users dial the digital-data endpoint.

The system provides a Hold Time parameter. This parameter specifies the maximum time that any modem can be held but not used, while a data call is in queue.

The integrated-conversion modems support the following options:

- Receiver responds to remote loop
- Loss of carrier disconnect

- Send space disconnect
- Receive space disconnect
- CF-CB common
- Speed, duplex, and synch (administered)

Combined-conversion modems support the following:

- IBM bisynchronous protocols that are usually used in 3270 and 2780/3780 applications. Both require 2400 or 4800 bps, half-duplex, synchronous transmission.
- Interactive IBM-TSO applications that use 1200 bps, half-duplex, asynchronous transmissions
- DATAPHONE II switched-network modems that support asynchronous and synchronous communications, and autobaud at 300, 1200, or 2400 bps
- Communication Manager operating at up to 19.2 kbps
- Different pools with different data-transmission characteristics

Administering Modem Pooling

The following steps are part of the administration process for the Modem Pooling feature:

This section describes:

- The screens that you use to administer the Modem Pooling feature

Screens for administering Modem Pooling

Screen name	Purpose	Fields
Modem Pool Group	Define modem pool groups.	All
Feature Access Code (FAC)	Set data origination access.	**Data Origination Access Code**
Data Module	Define specific data modules.	All

Considerations for Modem Pooling

This section provides information about how the Modem Pooling feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Modem Pooling under all conditions. The following considerations apply to Modem Pooling:

- On data calls between a data module and an analog-data endpoint, Return-to-Voice releases the modem and returns the modem to the pool. The phone user connects to the analog-data endpoint.
- For traffic purposes, the system accumulates data on modem-pooling calls separately from voice calls. Measurements on the pools also accumulate.
- When a telephone user places a data call to a digital-data endpoint, does not transfer the call to another digital-data endpoint, and uses a modem or an acoustically-coupled modem, the user dials the data-origination access code before the user dials the distant endpoint.
- Modem Pooling is not restricted. Queuing for modems is not provided, although calls queued on a hunt group retain reserved modems.
- Avoid the use of modems from different vendors within a combined pool. Modems from different vendors might have different transmission characteristics.
- When you administer data-transmission characteristics (such as speed, duplex, and synchronization mode), they must be identical to the TDM and the optional modem selections made by the customer.
- Each data call that uses Modem Pooling uses four time slots, instead of two. As a result, heavy usage of Modem Pooling can affect TDM bus-blocking characteristics.
- Tandem servers or switches do not insert a pooled modem. The originating server or switch inserts a pooled modem.

Interactions for Modem Pooling

This section provides information about how the Modem Pooling feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Modem Pooling in any feature configuration.

- Call Detail Recording (CDR)

  Data call CDR records the use of modem pools on trunk calls.

- Data Call Setup

  Data calls to or from a TDM cannot use Modem Pooling.

- Data Privacy and Data Restriction

  The insertion of a modem pool does not turn off Data Privacy or Data Restriction.

- Data-Only Off-Premises Extensions

  Calls to or from a Data-Only Off-Premises Extension cannot use Modem Pooling, when this type of digital-data endpoint uses a TDM.

- Digital-multiplexed Interface (DMI) Trunks

  If you place a data call from a local analog-data endpoint to a DMI trunk, you must dial the data-origination access code to obtain a modem. Data calls on DMI trunks to local analog-data endpoints automatically obtain modems.

- DS1 Tie Trunk Service

  Connect modems are used for Modem Pooling to AVD DS1 tie trunks by Data Terminal Dialing or by dialing the Feature Access Code (FAC) for data origination.

Multifrequency Signaling

Use the Multifrequency (MF) signaling feature to perform signaling used between media servers and the Central Office (CO). It is similar to dual-tone multifrequency (DTMF) signaling in that tones convey the dialed number.

With MF signaling, the signal is usually a combination of two frequencies from a group of 5 or 6 frequencies (2/5 or 2/6). The origination and destination servers or switches exchange tones that have specific meanings according to the MF protocol.

Detailed description of Multifrequency Signaling

This section provides a detailed description of the Multifrequency Signaling feature.

Communication Manager supports two frequency groups:

- R2-multifrequency compelled signaling (R2-MFC) frequency
- R1 frequency (for Spain and Russia)

R2-MFC is a version of MFC recommended by the International Telecommunication Union (ITU). It provides signaling between a CO and a media server over analog or digital CO, Direct Inward Dialing (DID), or Direct Inward and Outward Dialing (DIOD) trunks. It also provides signaling between any 2 servers running Communication Manager.

Communication Manager provides MF signaling that complies with ITU regulations and national regulations for specific countries. It provides these types of MF signaling: MFE MF Shuttle, and multifrequency compelled (R2-MFC). These protocols signal the called number, the calling party's number (ANI), and information about the type of call or type of caller (category).

Communication Manager allows prefix digits for ANI sent on outgoing calls to be defined per server, or per the originator's class of restriction.

If a call is a tandem call and the incoming and outgoing trunk use different protocols, Communication Manager makes no attempt to convert between the various protocol's meanings for category. Instead,

- the server uses the incoming trunk's COR assigned category if the outgoing trunk is Russian or R2-MFC, and
- the server uses ARS call types if the outgoing trunk is MFE.

The server running Communication Manager provides the incoming ANI to all features on Communication Manager that need to identify the calling party.

MFE

MFE, for Country code 11 (Spain), uses R1 frequency and compelled signaling. It is available on CO and DID trunk groups. There are four types of MFE signaling:

- Public 2/5
- Public 2/6
- Ibercom 2/5
- Ibercom 2/6

MF Shuttle

MF shuttle signaling, for country code 15 (Russia), uses R1 frequency and noncompelled signaling. With MF shuttle signaling, it is possible to change to decadic rotary pulse in the middle of address signal exchange. MF shuttle signaling is available on CO, DID, and DIOD trunk groups.

Also, ANI transmission, for Country code 15, uses a gapless R1 MF signal and is completed within 800ms. This is available on an outgoing CO trunk group.

R2-MFC

R2 multifrequency compelled (R2-MFC) signaling allows each country to define the meanings of the R2 frequency combinations.

Guidelines for administering Multifrequency Signaling

To administer MF signaling, you must first identify the origination and destination server or media servers. The one making the call is the origination server. The one answering the call is the destination server.

- The origination server/media server creates forward signals, classified as group I and group II signals.
- The destination server/media server creates backward signals, classified as group A and group B signals.

Group I and group A signals comprise the basic signaling for the dialed number. More elaborate signaling requires Group II and group B signals. Signal meanings and timer values can be administered.

The following sequence shows a typical interaction between the origination server (forward group I and group II signals) and destination server (backward group A and group B signals).

Forward			Backward
Group I	digit	-->	
	<--	A.1	Group A
	digit	-->	
	<--	A.1	
	digit	-->	
	<--	A.1	
	digit	-->	
	<--	A.1	
	digit	-->	
	<--	A.3	End of dial
Group II	II.2	-->	
	<--	B.x	Group B

Second, you assign the correlation between signal codes and their meanings.

1. Assign a code to each message. The code consists of a group category, like group II or A, and a number.
   - For example, you might assign code A.1 to the message "next-digit."
2. Assign a signal to each identifying code.
   - In every country, the frequencies (levels might differ by country) assigned to the identifying codes are the same. However, the messages assigned to the identifying codes can be different.

     For example, in Switzerland the B.6 code and its associated signal convey the *free* message, while in Thailand, *free* is conveyed by the B.1 code and its associated signal. But in both Switzerland and Thailand, the frequency associated with the B.1 code is the same.

     As another example, you might assign the signal "busy" to the B.1 code.

To receive Russian incoming ANI:

- On the DID or DIOD Trunk Group screen, set the **Country** field to **15** and the **Protocol Type** field to **inloc**.
- On the AAR and ARS Digit Analysis Table screen, set the **ANI Req** field to **y**, or on the AAR and ARS Digit Conversion Table screen, set the **ANI Req** field to **y**.

Administering Multifrequency Signaling

The following steps are part of the administration process for the Multifrequency Signaling feature:

- None

Screens for administering Multifrequency Signaling

Screen name	Purpose	Fields
Multifrequency-Signaling Related Parameters	Sets the system parameters for multifrequency signaling	All
AAR and ARS Digit Conversion Table	Sets automatic number identification	**ANI Reqd**
AAR and ARS Digit Analysis Table	Sets automatic number identification	**ANI Reqd**

Considerations for Multifrequency Signaling

This section provides information about how the Multifrequency Signaling feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Multifrequency Signaling under all conditions. The following considerations apply to Multifrequency Signaling.

The following considerations apply to R2-MFC only:

- Both non-group II signaling and group II signaling are supported on incoming MF signaling calls. The group II signaling protocol has an extra signal that provides caller-category information. Only group II signaling is supported on outgoing MF signaling calls.
- MF signaling also can be used in tandem trunk groups. After address signals are collected from an incoming group II MF signaling call, the call can route to a group II MF signaling trunk.
- Both incoming and outgoing MF signaling calls support ANI displays, ANI information and the CDR records the information.
- When Communication Manager uses an open numbering plan, the end-of-dial signal must be defined in the incoming Group I signal administration. After sending all address digits, the CO sends the end-of-dial signal to Communication Manager.

- If Communication Manager makes an outgoing call to the CO that uses an open numbering plan, the CO must send the signal A.1 to Communication Manager after sending the last address digit to the CO. Then, the CO should time out and send a pulsed signal A.3 to Communication Manager requesting the Group II signal.
- Communication Manager offers the option to record the Calling Party Category in the CDR. For incoming external calls, this comes from the Group II signal. For internal calls and station-originated external calls, this comes from the COR of the originating station. For tandem calls, this value comes from the Group II signal, determined by the COR of the originating trunk group. The CDR device is capable of receiving this information.
- You can assign Calling Party Category and Called Party Category on a trunk-by-trunk basis.
- You can record an announcement to play when outgoing R2-MFC trunk calls do not complete. This applies when Communication Manager receives either group A or B signals from the called Central Office or other media server or switch.

Interactions for Multifrequency Signaling

This section provides information about how the Multifrequency Signaling feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Multifrequency Signaling in any feature configuration.

- ASAI

  ANI collected from incoming R2-MFC signaling can be used with ASAI.

- Abbreviated Dialing

  Although calls dialed automatically from an abbreviated dialing privileged list complete without COR checking, ANI prefix and ANI truncation still apply.

- Attendant Console

  If the attendant assists or extends a call for a station using Straightforward Outward Completion and Through Dialing, and if the attendant has not yet released the call when the request for ANI comes in from the far end, the attendant's COR is used to select the ANI for the call. If the attendant has already released the call when the request for ANI comes in from the far end, the attendant's COR is used to select the ANI for the call.

- Authorization Codes

  The COR of the authorization code as administered on the authorization-code screen is not used for ANI prefix determination, even if the originating endpoint enters an authorization code before call processing for an outgoing call seizes an outgoing trunk. If the originating endpoint is an extension, the extension's ANI is used. If the originating endpoint is an incoming trunk, the ANI for PBX is used.

- Bridging

  The ANI of a telephone's primary extension also applies to calls originated from a bridged call appearance of that extension on another terminal. ANI prefix and ANI truncation applies to the primary extension number of bridged call appearances.

- Call Detail Recording (CDR)

  CDR records ANI collected from incoming MF signaling.

  For India MFC, on incoming calls, ANI digits may be appended with zeroes if the actual ANI digits are less than the administered ANI-length; in those cases, the zero-digits appear on CDR.

- Call Redirection

  A call is redirected if any of the following are active: Call Forwarding, Call Coverage, Send All Calls, or Night Service.

- Call Vectoring

  Call Vectoring can now use ANI collected from incoming MFC signaling.

  The ANI of a call vector is not used when a call vectoring route-to command routes a call over an outgoing trunk. Instead, the ANI of the originating party is sent.

- **DID** No Answer Timer

  DID No Answer Timer is applied to MF signaling **DID** calls.

- Distributed Communications System (DCS)

  In a DCS arrangement, the ANI sent to the CO is determined by the **ANI for PBX on PBX_B**, but the category sent to the CO is determined by the **Category for MF ANI** field on the Class of Restriction screen for the incoming DCS trunk or by the type of call.

- Expert Agent Select (EAS)

  For ANI, the EAS agent's login extension number and COR overrides the extension number and COR of the physical terminal where the agent is logged in. ANI prefix and ANI truncation apply to logged in EAS agents.

- Hunt Groups and Automatic Call Distribution (ACD) Splits

  For ANI, a physical terminal's extension number and COR overrides the extension number and COR of the hunt group or ACD split that is a member of or logged into. ANI prefix and ANI truncation apply to terminals that are members of hunt groups or logged into ACD splits.

- Intercept treatment

  For **DID MF** signaling calls that are denied, you can administer whether the corresponding B.x signal or intercept tone should be sent to the **CO**. The default is to send the administered **DID**/**TIE**/**ISDN** Intercept Treatment. If the option to send the B.x signal is set, then:

  – For Group II calls, the B.x signal for the intercept is sent to the **CO**.

  - For non-Group II calls, if the **CO** dials an invalid number, the trunk is locked (regardless of this option). If the **CO** dials a number that is valid but not assigned, intercept tone is sent to the **CO**.

- Multimedia Call Handling (MMCH)

  For call origination, multimedia complexes use the COR assigned to their telephones. ANI prefix and ANI truncation will apply to the telephones assigned to multimedia complexes.

- Off-Net Call Coverage or Call Forwarding

  If the originating endpoint is an extension, the extension's ANI is used. If the originating endpoint is an incoming trunk that can supply ANI, the ANI received from the incoming trunk is used. If the originating endpoint is neither of the above, the ANI for PBX is used.

- Personal Station Access (PSA)

  For ANI, the PSA extension number and COR overrides the extension number and COR of the physical terminal where the PSA extension number is associated. ANI prefix and ANI truncation will apply to associated PSA extension numbers.

- Remote Access

  The COR of a remote access barrier code is not used for ANI prefix determination when the originating end point dials a remote access extension and then places a call. If the originating endpoint is an extension, the extension's ANI is used. If the originating endpoint is an incoming trunk, the ANI for PBX is used.

- Station Set Displays

  When no ANI is possible, if station sets are equipped with display option, they do not display the ANI digits. Instead, the trunk group name displays. When ANI is possible, ANI displays on the station set.

  Note:
  For India Only. If ANI digits are padded with "zero," then zeroes also are displayed along with ANI digits.

- Tandem / Offnet Calls

  If ANI digits are received on incoming MFC calls, the ANI digits are sent to outgoing tandem/off-net calls.

  Note:
  For Russia Only. The ANI is requested on incoming trunks only when all the address digits have been collected. When the incoming trunk on a tandem call is a Russian incoming local trunk administered to collect ANI, the server collects all ANI digits before seizing the outgoing tandem trunk. This happens even if ARS is administered with a min value low enough that it would be possible to determine an outgoing route through digit analysis.

Note:

For India Only. On an outgoing tandem-call, the default operation is to send the ANI-Not-Available forward signal if ANI is not available from the incoming trunk. However, in order to support this operation, leave the **ANI for PBX** field blank, and define the ANI-Not-Available signal.

Multiple Level Precedence and Preemption

Use the Multiple Level Precedence and Preemption (MLPP) feature to allow users to request priority processing of calls during critical situations.

CAUTION:
MLPP is currently designed to meet only Generic Switching Center Requirements (GSCR) for connection to a Defense Switched Network (DSN) by federal, state, or local government agencies. MLPP is not currently designed for use in commercial enterprise environments. Activation of this feature in any other type of network environment can result in unexpected or unwanted feature operations.

Detailed description of Multiple Level Precedence and Preemption

This section provides a detailed description of the Multiple Level Precedence and Preemption feature.

The Multiple Level Precedence and Preemption feature is available with Communication Manager Release 2.0 (V12) or later.

While the media servers and media gateways that are referenced in this document support MLPP, the Joint Interoperability Test Command (JITC) has certified only the following servers:

- DEFINITY Server CSI
- DEFINITY Server SI
- Avaya S8700 Server supporting an MCC1 or an SCC1 Media Gateway

Multiple Level Precedence and Preemption supports the following capabilities:

- Precedence Calling
- Announcements for Precedence Calling
- Precedence Call Waiting
- Precedence Routing
- Dual Homing
- End Office Access Line Hunting
- Preemption

- Line Load Control
- Worldwide Numbering and Dialing Plan

Precedence Calling

Precedence Calling allows users, on a call-by-call basis, to select a level of priority for each call. The need of the user and the importance of the call is the basis for the priority. The call can receive a priority routing whether the call is local or international.

Precedence levels

Users can access five levels of precedence:

- Flash Override, which is the highest precedence level
- Flash
- Immediate
- Priority
- Routine, which is the default and the lowest precedence level

If a user does not specify a precedence level, the system treats dialed calls as Routine level precedence calls.

The administrator assigns a maximum precedence level to each telephone user. The more important or higher in rank of the user, the higher the precedence level. Users cannot originate calls at precedence levels that are higher than the maximum administered level. Non-MLPP calls are treated as Routine level precedence calls.

For example, General Davis has a maximum precedence level of Flash assigned to his telephone. Without intervention, everyday calls are treated at the Routine level. One day, a crisis occurs at a military installation, and the general must make an emergency call to his field commanders over the Defense Switched Network (DSN). General Davis can use the Precedence Calling feature to raise the level of his call to Priority, Immediate, or Flash. When he places this call, the communication server gives the call priority handling, and the call is sent over the DSN access line.

Format for dialed digits

The following table shows the format for Precedence Calling dialed digits:

Access digits		Address digits		
FAC	**Precedence digit**	**Area code**	**Office code**	**Extension**
A	**P**	**[NXX]**	**NXX**	**XXXX**

Where:

A is the Feature Access Code (FAC) for Precedence Calling

P is any digit from 0 to 4 (digits from 5 to 9 can also be used)

X is any digit from 0 to 9

N is any digit from 2 to 9

Brackets **[ ]** indicate optional digits

Access digits

The access digits are comprised of the FAC for the Precedence Calling feature, plus a Precedence Level digit. The single-digit code used for the Precedence Level digit is administered as shown on Assigning Precedence Calling system parameters on page 1221.

The default Precedence Level digits are:

Digit	Precedence Level
0	Flash Override
1	Flash
2	Immediate
3	Priority
4	Routine

Address digits

The address digits are the 7-digit or the 10-digit telephone number.

Precedence calls above the Routine level use special precedence ringback tones for the calling party, and a special ringing pattern for the called party. The TN2182B or the TN2182C Tone Clock circuit pack generates the Precedence calling tones on the following media gateways and servers:

Media gateways	Supported by
• G650 Media Gateway • SCC1 Media Gateway • CMC1 Media Gateway • MCC1 Media Gateway	• DEFINITY Server • S8500 Server • S8700 Server

On a G350 or a G700 Media Gateway supported by an S8300, an S8500, or an S8700 Server, the media gateway processor generates precedence calling tones. The S8100 Server processor also generates tones.

- The ringback tone is a 1.65-second burst of mixed 440-Hz and 480-Hz tone, and then 0.35 seconds of silence. This tone repeats until the call is answered, the caller hangs up, or the Precedence Call Timeout occurs. For more information, see Assigning Precedence Calling system parameters on page 1221.
- The ringing pattern for precedence calls is the same three-burst ring that is used with Priority Calling.

Precedence Calling diversion scenarios

When a precedence call to a telephone goes unanswered, the system attempts to connect the caller to a backup point as follows:

1. The call is diverted to the attendant console.
2. If the console is in Night Service or no console is administered, the call is diverted to a night telephone.
3. If no console or night telephone is administered, the call can be diverted to a user-defined telephone. This user-defined telephone is called the Remote Attendant Route String.

   The Attendant Diversion Timing controls how long that this type of call rings before the system routes the call to the Remote Attendant Route String. The Remote Attendant Route String is any valid telephone number on the network, and is usually a backup answering position for the remote attendant console. The Remote Attendant Route String does not raise the precedence level of the call.
4. If the Remote Attendant Route String is undefined and there is no attendant console or night telephone is administered, the call rings until the call is answered or abandoned.

These Precedence Calling diversion scenarios have variations for DSN calls, non-DSN calls, and local calls:

DSN Calls: If an outgoing precedence call over a DSN trunk is unanswered after an administrable period of time, the system routes the call to the:

- Attendant console or night telephone on the remote communication server
- Remote Attendant Route String

The administrable period of time is the Precedence Call Timeout on the remote communication server.

Non-DSN Calls: If an outgoing precedence call over a non-DSN trunk is not answered after an administrable period of time, the system routes the call to:

- A local attendant console or night telephone on the local communication server
- The Remote Attendant Route String

The administrable period of time is the Attendant Diversion Timing on the local communication server.

Local calls: If a local, intraswitch precedence call is unanswered after an administrable period of time, the system routes the call to:

- A local attendant console
- A night telephone
- The Remote Attendant Route String

Note:

For a precedence call that diverts to a night telephone or to a Remote Attendant Route String, the number must be administered in the Precedence Routing digit-conversion tables. For more information, see Assigning digit conversion on page 1238 and Assigning Precedence Calling system parameters on page 1221.

The administrable period of time is the Precedence Call Timeout on the remote communication server.

When calls are redirected, a Call Purpose Indicator is displayed on the attendant console and on display telephone sets to indicate the precedence level of the call. The following indicators are provided:

- FO - Flash Override
- FL - Flash
- IM - Immediate
- PR - Priority

Routine precedence calls do not have a Call Purpose Indicator.

When callers attempt to use a precedence level that is higher than the authorized level, the caller hears the "Unauthorized precedence level attempted" recording. If an announcement is not assigned, the caller hears intercept tone.

The following table shows how precedence calls are processed depending on the precedence level and the administered maximum precedence level of the caller:

Maximum precedence level of the user	Precedence level of the call	Call treatment
Flash Override	Flash Override	Call completes normally
Flash Override	Flash	Call completes normally
Flash Override	Immediate	Call completes normally
Flash Override	Priority	Call completes normally
Flash Override	Routine	Call completes normally
Flash	Flash Override	Recorded announcement or intercept tone
Flash	Flash	Call completes normally
Flash	Immediate	Call completes normally
Flash	Priority	Call completes normally
Flash	Routine	Call completes normally
Immediate	Flash Override	Recorded announcement or intercept tone
Immediate	Flash	Recorded announcement or intercept tone
Immediate	Immediate	Call completes normally
Immediate	Priority	Call completes normally
Immediate	Routine	Call completes normally
Priority	Flash Override	Recorded announcement or intercept tone
Priority	Flash	Recorded announcement or intercept tone
Priority	Immediate	Recorded announcement or intercept tone
Priority	Priority	Call completes normally
Priority	Routine	Call completes normally
Routine	Flash Override	Recorded announcement or intercept tone
Routine	Flash	Recorded announcement or intercept tone
Routine	Immediate	Recorded announcement or intercept tone
Routine	Priority	Recorded announcement or intercept tone
Routine	Routine	Call completes normally

How service domains influence preemption and precedence

You define MLPP service domains at two levels:

- On the Class of Restriction screen, where you then assign the COR to a telephone of a user
- On the Multiple Level Precedence & Preemption Parameters screen, which applies to all resources on the server

The system uses the service domain to determine whether the system applies the preemption or precedence level of the caller to potentially preempt a routine call or another call of lower precedence. If an existing call has a different service domain than the service domain of the call that attempts a preemption, preemption is not allowed, regardless of the preemption levels of the two calls.

The two levels of service domain influence preemption and precedence capabilities in different ways, depending on which of the following resources the server recognizes as carrying the call:

- Intraswitch routing to another telephone on the same server
- Incoming ISDN-PRI trunks for a call that originates from another server on the network
- Incoming non-ISDN-PRI trunks for a call that originates from another server on the network

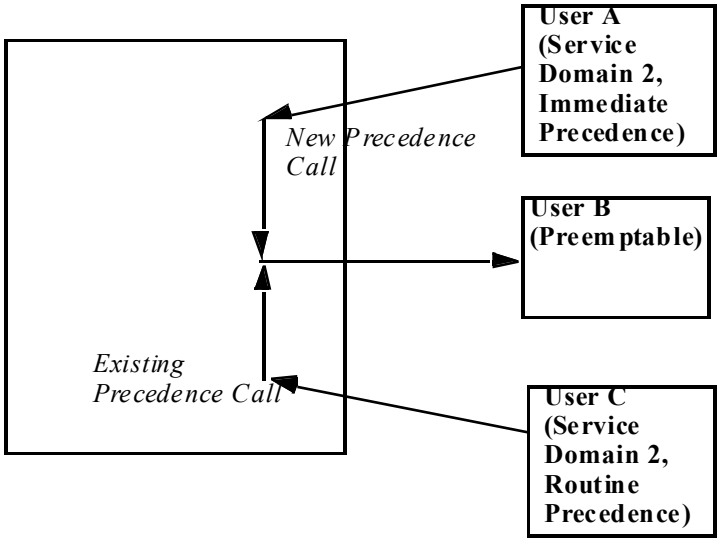
Station-to-station calls on the same server

If a user makes an MLPP call to another user whose telephone resides on the same server, and if the called telephone is busy with an existing call, the server uses the following process to determine whether to grant precedence to the new call:

1. The server assigns the existing call to the service domain that is defined in the Class of Restriction (COR) of the caller.
2. The server checks the COR of the new caller to define the service domain of the new call.
3. The server matches the service domain of the new call with the service domain of the existing call.
4. If the service domains match, the server matches the precedence level of the existing call with the precedence level of the new call. If the new call has a higher level, the new call preempts the existing call.

   If the service domains do not match, then the server gives the new call an announcement that says the MLPP call cannot be completed. Figure 297: Station-to-station calls on the same server on page 1206 shows this process.

Figure 297: Station-to-station calls on the same server



In Figure 297, the server uses the service domains and the precedence levels to treat calls as follows:

1. User C makes a routine call to user B and is still connected. The server checks the service domain of the COR of user C, and assigns service domain 2 to the call.
2. User A makes an immediate precedence call to user B. The server checks the service domain of the COR of user A, and assigns service domain 2 to the call.
3. The server matches the service domain of user C with the service domain of user A.
4. Because the calls are in the same service domain, and because user A used a higher precedence level than user C, the server allows user A to preempt the call of user C.

Precedence calls to destinations over ISDN-PRI trunks

If:

- A user makes an MLPP call to another user whose telephone resides on a different MLPP server, and
- The call arrives at the server of the called user over an ISDN-PRI trunk, and
- The called telephone is busy with an existing call.

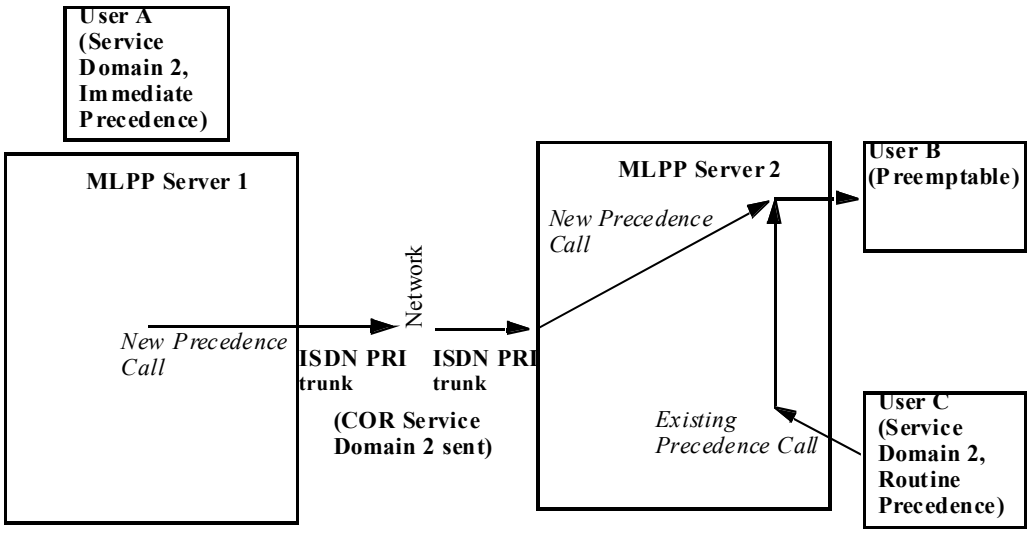
The destination MLPP server uses the following process to determine whether to grant precedence to the new call:

1. The server assigns the existing call to the service domain that is defined either in the COR of the caller, or by the system service domain.
2. The server checks the COR of the new caller to define the service domain of the new call.

3. The server matches the service domain of the new call with the service domain of the existing call.
4. If the service domains match, the server matches the precedence level of the existing call with the precedence level of the new call. If the new call has a higher level, the new call preempts the existing call.

   If the service domains do not match, the server gives the new call an announcement that says that the MLPP call cannot be completed. Figure 298: Precedence calls to destinations over ISDN-PRI trunks on page 1207 shows this process.

Figure 298: Precedence calls to destinations over ISDN-PRI trunks



In Figure 298, the destination server, MLPP Server 2, uses the service domains and precedence levels to treat calls as follows:

1. User C makes a routine call to user B and is still connected. The server checks the service domain of the COR of user C, and assigns service domain 2 to the call.
2. User A, who is on MLPP Server 1, makes a precedence call to user B. Server 2 checks the service domain on the incoming ISDN call and finds service domain 2, which is defined in the COR of user A on Server 1. Server 2 assigns service domain 2 to the call.
3. The server matches the service domain of user C with the service domain of user A.
4. Because the calls are in the same service domain, and because user A used a higher precedence level than user C, the server allows user A to preempt user C.

Precedence calls to destinations over non-ISDN-PRI trunks

If:

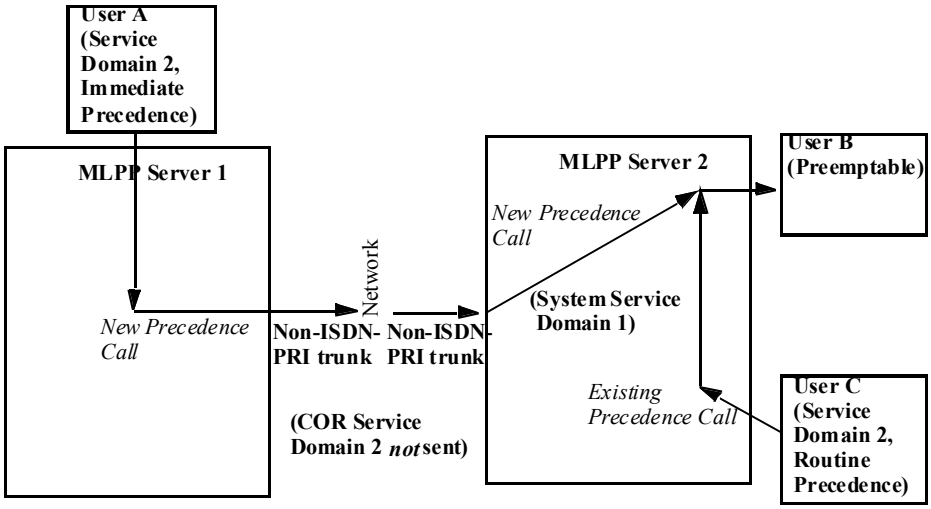
- A user makes an MLPP call to another user whose telephone resides on a different MLPP server, and
- The call arrives at the server of the called user over a non-ISDN-PRI trunk, and
- The called telephone is busy with an existing call,

The destination server uses the following process to determine whether to grant precedence to the new call:

1. The server assigns the existing call to the service domain that is defined either in the COR of the caller, or by its own system service domain.
2. The server checks its own system service domain to define the service domain of the new call.
3. The server matches the service domain of the new call with the service domain of the existing call.
4. If the service domains match, the server matches the precedence level of the existing call with the precedence level of the new call. If the new call has a higher level, the new call preempts the existing call.

   If the service domains do not match, then the server gives the new call an announcement that says that the MLPP call cannot be completed. Figure 299: Precedence calls to destinations over non-ISDN-PRI trunks on page 1208 shows this process.

Figure 299: Precedence calls to destinations over non-ISDN-PRI trunks



In Figure 299, the system uses the service domains and precedence levels to treat calls as follows:

1. User C makes a routine call to user B and is still connected. The server checks the service domain of the COR of user C, and assigns service domain 2 to the call.

2. User A, who is on MLPP Server 1, makes a precedence call to user B. Because the call from user A arrives at MLPP Server 2 on a non-ISDN-PRI trunk, Server 2 does not receive the service domain identifier of user A. Server 2 assigns the system service domain 1 to the call.
3. The server matches the service domain of user C with the service domain of user A.
4. Because the calls of users A and C are *not* in the same service domain, calls from user A receive an announcement that says that the MLPP call cannot be completed.

Announcements for Precedence Calling

In certain situations, precedence calls are blocked because of unavailable resources or improper use. The MLPP feature requires special announcements, for calls higher than Routine precedence, to notify users when Precedence Calling is denied, or when service is unavailable.

The announcements that MLPP uses include:

- Blocked precedence call

  This announcement plays when the system attempts to preempt an existing call with a call that has a precedence level higher than Routine precedence that is also equal to or lower than the precedence level of the current call. If an announcement extension is not assigned, the caller hears reorder tone (fast busy).

- Unauthorized precedence level attempted

  This announcement plays when a caller attempts to place a precedence call with a precedence level that is higher than the level that is authorized by the COR of the caller. If an announcement extension is unassigned, the caller hears intercept tone.

- Service-interruption-prevented call completion

  This announcement plays when a service interruption prevents a precedence call from being completed. If an announcement extension is not assigned, the caller hears reorder tone.

- Busy, not equipped for Preemption or Precedence Call Waiting

  This announcement plays when a precedence call is placed to a busy line, and the line does not have Precedence Call Waiting or cannot be preempted. If an announcement extension is not assigned, the caller hears reorder tone.

- Vacant code

  This announcement plays when a precedence call is placed to an unassigned extension. If an announcement extension is not assigned, the caller hears reorder tone.

If a caller is using Routine precedence and the call cannot be completed for any of these reasons, the caller hears busy tone.

Precedence Call Waiting

After the system routes a precedence call, the called party might already be busy on another call. Precedence Call Waiting allows the caller to "camp on" to the line of the called party, and wait for the called party to answer the call. The caller hears a special ringback tone, and the called party hears a call waiting tone. Depending on the type of telephone, the called party:

- Can put the current call on hold and answer the incoming call, or
- Must hang up on the current call to answer the incoming call

Precedence Routing

When precedence calls are destined for other switches in a network, the Precedence Routing feature routes the calls. The Precedence Routing feature routes calls based on the:

- Destination number
- Precedence level
- Time of day

These routing criteria are administrable and can be changed as required. Two related features are Dual Homing and End Office Access Line Hunting.

Dual Homing

Dual Homing allows a user to dial a telephone number and have the system route the call to its destination over alternate facilities if the initial route is unavailable. This operation is transparent to the user, and no special dialing is required.

Dual Homing uses the Precedence Routing feature to provide alternate routing to nodes on a DSN. If a call fails to complete over the first trunk access line, the call is rerouted over a different trunk access line. This process can continue for any number of alternate routes.

If the call fails to complete by the time the call gets to the last trunk access line, the system routes the call to either:

- Busy tone, or
- The Blocked precedence call recorded announcement (see Announcements for Precedence Calling on page 1209).

For example, a user dials a DSN number, such as 345-8854. Using Precedence Routing, you administer the system to route all calls that begin with the digits "345":

1. First over trunk group 20

2. Then over trunk group 21
3. Finally over trunk group 22

If all trunks in trunk group 20 are busy, the system next checks for idle trunks in trunk group 21, and finally in trunk group 22. If all trunks in all three trunk groups are busy, the system routes the call to fast busy tone or to a recorded announcement.

For a more detailed description of the available routing options, see Precedence Routing on page 1210.

End Office Access Line Hunting

The End Office Access Line Hunting feature automatically hunts for an idle trunk over end office access lines. This feature hunts for an idle trunk based on the precedence level of the call. The search occurs over either a preemptable trunk group or a nonpreemptable trunk group.

For calls that are higher than Routine precedence, the system hunts for an idle trunk in a preemptable trunk group. The following steps describe the hunting algorithm:

1. If the system finds an idle trunk, the system provides precedence ringing.
2. If the system does not find an idle trunk, the system reexamines a preemptable trunk group on a preemptive search. The system preempts an active call that is of the lowest available precedence level.
3. The system hunts for an idle trunk in a nonpreemptable trunk group. If the system finds an idle trunk, the system provides precedence ringing.
4. If the system cannot find a trunk, the call is routed to the Blocked precedence call recorded announcement (see Announcements for Precedence Calling on page 1209). If announcements are not recorded or administered, the caller hears reorder tone.

For calls that are Routine precedence, the system hunts for an idle trunk in a nonpreemptable trunk group and attempts to connect the call. If the system does not find an available trunk, the caller hears busy tone. For more information about preemptable and nonpreemptable trunks, see Preemption on page 1211.

Preemption

Preemption works with Precedence Routing to further extend the call routing capabilities of MLPP. Preemption actually disconnects an existing, lower-priority call to complete a more important precedence call. Even non-MLPP calls are treated as Routine level precedence calls, and can be preempted.

When preemption occurs, the callers on the existing call hear a tone that indicates that the system is about to preempt the call. The callers have 3 seconds to end the call before the system automatically disconnects the call. After the system disconnects the call, the system places the new call over the preempted facility.

Line Load Control

Line Load Control (LLC) is a feature that restricts a predefined set of telephone users from originating calls during a crisis or an emergency. LLC systematically reduces the number of telephones that can originate calls during high-traffic periods. This situation is sometimes called a "lockdown." When the lockdown situation passes, the LLC restriction levels can be reduced or removed completely.

Users are assigned to a Line Load Control level based on the relative importance of the position of the user within the organization. When an emergency occurs, the administrator manually activates the LLC feature to restrict calls by users with positions that are of lower importance. When the emergency is over, the administrator manually disables the LLC feature.

For example, if a security emergency occurs, telephone users who are responsible for managing the crisis are unrestricted from originating calls. Other telephone users, for example, users in the accounting department, are restricted. When the crisis is over, the administrator returns the system to normal operation.

The LLC feature can be controlled at four levels. These levels determine what telephones, based on the Class of Restriction (COR), are restricted from originating calls. This feature does not restrict incoming calls, or calls that originate from an attendant console or a night telephone.

The four levels are as follows:

Level	Definition
0	The LLC feature is inactive, that is, no restrictions exist. This is the default setting.
2	Restrict telephones with a COR that is assigned to LLC levels 2, 3, and 4.
3	Restrict telephones with a COR that is assigned to LLC levels 3 and 4.
4	Restrict telephones with a COR that is assigned to LLC level 4.

System level 1 is not a valid value. The LLC feature cannot restrict telephones with a COR that is assigned to LLC level 1 from originating calls.

When LLC is activated, the system restricts all telephones with a COR at that LLC level and below from originating any calls. If a restricted telephone is already active on a call when the restriction is activated, the call is not interrupted or disconnected. The telephone becomes restricted only after the user hangs up from the active call.

When the need for LLC has passed, the administrator can change the LLC to a less-restrictive level, or completely deactivate the feature.

The following table shows how the LLC feature can be used.

Extension	COR	LLC Level
5300	11	0
5350	12	2
2540	13	3
3300	14	4
2635	14	4

For this example, the LLC is at Level 0, and extension 2635 is active on a call.

1. Because of high telephone traffic, the system administrator changes the LLC to level 3.

   Extensions 2635, 2540, and 3300 cannot originate calls because the assigned COR LLC level for these extensions is equal to or less than the system LLC level.

   The active call on extension 2635 is not disturbed. As soon as extension 2635 hangs up, that extension cannot originate calls.

   Extensions 5300 and 5350 can originate calls because the assigned COR LLC level of these extensions is higher than the system LLC level.

2. Call traffic is still too high, so the system administrator changes the LLC to level 2.

   Now extension 5350, in addition to extensions 2635, 2540, and 3300, cannot originate new calls. Extension 5300 can still originate new calls.

3. Call traffic subsides. The system administrator changes the LLC back to level 0.

   All extensions can now originate calls.

Worldwide Numbering and Dialing Plan

The Worldwide Numbering and Dialing Plan (WNDP) feature is compatible with the standard numbering system that the Defense Communications Agency (DCA) established. WNDP is a dialing system that is used in a Defense Switched Network (DSN). WNDP is similar to Precedence Calling, but the pattern of digits that users dial is different.

The following table shows the format of the dialed digits:

Access digits		Address digits		
FAC	**Route code**	**Area code**	**Office code**	**Extension**
A	**[[1]X]**	**[NXX]**	**NXX**	**XXXX**

Where:

A is the 2-digit WNDP FAC for the precedence level

1 is a Route Code setup digit.

X is any digit from 0 to 9

N is any digit from 2 to 9

Brackets **[ ]** indicate optional digits

Feature Access Code

The Feature Access Code (FAC) is the set of two-digit WNDP FACs. Each precedence level uses a unique FAC.

- Flash Override - **90**
- Flash - **91**
- Immediate - **92**
- Priority - **93**
- Routine - **94**

Route Code

After dialing the FAC, the user has the option to dial a Route Code. The Route Code is a 2-digit DSN code that consists of a Route Code Setup digit and the Route Code digit. The Route Code informs the communication server of special routing or termination requirements. The Route Code is limited to the DSN. The Route Code determines whether a call uses data-grade or voice-grade trunking. The Route Code also indicates whether the dialed number is a Federal Telephone System (FTS) or a Continental US (CONUS) commercial number.

If you do not require special call features, and you want to use the default value **0**, you do not have to use the Route Code. If you want to use a value other than the default value **0**, you must use the Route Code.

- The first digit of the Route Code is the Route Code Setup digit. The Route Code Setup digit is the number **1**. The Route Code Setup digit indicates that the next digit gives instructions to the network for specialized routing. If a Route Code is dialed, the Route Code Setup digit is deleted, and the second digit is saved.
- The second digit of the Route Code is the Route Code digit. Valid entries are:

  0 - Voice call (the default value)

  1 - Circuit switched data call

  2 - Satellite avoidance call

  3 - (reserved)

  4 - (reserved)

  5 - Hotline voice-grade call

  6 - Hotline data-grade call

  7 - (reserved)

  8 - (reserved)

  9 - (reserved)

The Route Code digit becomes part of the dialed number, and can be used for route selection by the Precedence Routing translations. Precedence Routing allows digit strings to be modified before outpulsing. This capability modifies the Route Code as needed by the terminating trunk group. If a Route Code digit is not dialed, the system inserts the default Route Code Digit of **0** as defined on the Multiple Level Precedence & Preemption Parameters screen. The default Route Digit routes the calls over the voice network, not the data network.

Address Digits

The Address Digits are the 7-digit or the 10-digit DSN number.

The following table shows the format of the outpulsed digits:

Precedence digit	Route code	Address digits		
		Area code	Office code	Extension
P	[[1]X]	[NXX]	NXX	XXXX

Use the Precedence Routing functionality to administer the digit outplusing. For more information, see Precedence Routing on page 1210. Precedence Routing allows flexible routing of dialed numbers, and the ability to modify the digits outpulsed digits as needed. For example, you can administer Precedence Routing to outpulse no Route Digit, only the Route Digit, or the number **1** and the Route Digit. The digits sent to Precedence Routing are of the form:

PRXXX...

Where:

P is the Precedence Digit

R is the Route Code (if WNDP is active)

XXX... are the Address Digits

If a particular route requires the Route Code of the form **1X**, you can use the digit modification translations for the route to insert the number **1**. If the route does not require the Route Digit, the digit modification can be translated to delete the Route Digit. The digit modification translations insert a Default Route Digit if the Default Route Digit is not dialed.

Administering Multiple Level Precedence and Preemption

The following steps are part of the administration process for the Multiple Level Precedence and Preemption feature:

Precedence Calling

- Assigning an MLPP Feature Access Code
- Assigning Precedence Calling system parameters
- Assigning a maximum precedence level
- Assigning trunks
- Assigning a hot line number
- Assigning attendant queue priorities

Announcements for Precedence Calling

- Adding extensions
- Assigning announcement types
- Recording announcements
- Deleting announcements
- Saving announcements

Precedence Call Waiting

- Enabling Precedence Call Waiting for a telephone
- Setting the Precedence Call timeout
- Assigning Feature Access Codes

Precedence Routing

- Assigning digit analysis
- Assigning route patterns

Dual Homing

- see Precedence Routing

End Office Access Line Hunting

- see Precedence Routing

Preemption

- Assigning Preemption to a COR
- Assigning trunks for Preemption
- Setting the Precedence Call timeout

Line Load Control

- Assigning the LLC level for the system
- Assigning the LLC to a COR

Worldwide Numbering and Dialing Plan (WNDP)

- Assigning WNDP system parameters
- Assigning WNDP Feature Access Codes
- Assigning a hot line number
- Assigning attendant queue priorities

This section describes:

- Any prerequisites for administering the Multiple Level Precedence and Preemption feature
- The screens that you use to administer the Multiple Level Precedence and Preemption feature
- Complete administration procedures for the Multiple Level Precedence and Preemption feature

Prerequisites for administering Multiple Level Precedence and Preemption

You must complete the following actions before you can administer the Multiple Level Precedence and Preemption feature:

- On the Optional Features screen, ensure that the **G3 Version** field is set to **V12** (Communication Manager Release 2.0) or later. If this field is not set to **V12** or later, your system is not enabled for the Multiple Level Precedence and Preemption feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- Click **Next** until you see the **Multiple Level Precedence and Preemption** field. Ensure that the **Multiple Level Precedence and Preemption** field is set to **y**. If the **Multiple Level Precedence and Preemption** field is set to **n**, contact your Avaya representative before you continue with this procedure.

Screens for administering Multiple Level Precedence and Preemption

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 2.0 (V12) or later.	**G3 Version**
	Ensure that the MLPP feature is on.	**Multiple Level Precedence & Preemption**
Feature Access Code (FAC)	Set up FACs for users to activate the MLPP features.	• **Precedence Calling Access Code** • All the fields in the **WNDP Precedence Access Codes** area
	Set up a FAC for users to answer a Precedence Call Waiting call from a single-line analog telephone.	**CAS Remote Hold/ Answer Hold-Unhold Access Code**
Multiple Level Precedence & Preemption Parameters	Set up the system parameters for MLPP.	All

Screen name	Purpose	Fields
Class of Restriction	• Apply administration settings to all objects that share the same COR number. • Restrict the types of calls that a user can make and receive.	• **Maximum Precedence Level** • **Preemptable** • **MLPP Service Domain** • **Lineload Control**
Trunk Features	Assign a trunk group as a DSN termination telephone.	**DSN Term**
	For DS1 and analog TIE trunks only, indicate if the system sends or receives the precedence level as digits (rotary pulses) or as dual-tone multifrequency (DTMF) signals (touchtones).	• **Precedence Incoming** • **Precedence Outgoing**
Station	Activate or deactivate Precedence Call Waiting for a telephone.	**Precedence Call Waiting**
	Assign a telephone as a hot line telephone for a precedence call or a WNDP call.	All the fields in the **Hot Line Destination** area
Abbreviated Dialing List	Set up the dialing list and specific dialed string to be used with a hot line telephone.	All
Console Parameters	Assign attendant queue priorities.	All the fields in the **Queue Priorities** area
Announcements/Audio Sources	Assign extensions for Precedence Calling announcements.	All
Precedence Routing Digit Analysis Table	Administer how the system analyzes Precedence Routing digits.	All

Screen name	Purpose	Fields
Pattern Number	Administer how the system handles route patterns for outgoing Precedence calls.	All
Precedence Routing Digit Conversion Table	Administer how the system takes digits of incoming calls, and converts the digits to local telephone numbers.	All

Precedence Calling

Assigning an MLPP Feature Access Code

To assign a Feature Access Code (FAC):

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Click **Next** until you see the **MLPP Features** area (Figure 300: Feature Access Code (FAC) screen on page 1220).

Figure 300: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 6 of 6
                              FEATURE ACCESS CODE (FAC)
                                 MLPP Features

             Precedence Calling Access Code: 8


   WNDP PRECEDENCE ACCESS CODES:
                Flash Override Access Code: 90
                         Flash Access Code: 91
                     Immediate Access Code: 92
                      Priority Access Code: 93
                       Routine Access Code: 94
```

3. In the **Precedence Calling Access Code** field, type a FAC that conforms to your dial plan.
4. Press **Enter** to save your changes.
5. Ensure that you notify all users about the assigned FAC.

Assigning Precedence Calling system parameters

To assign the Precedence Calling system parameters:

1. Type **change system-parameters mlpp**. Press **Enter**.

   The system displays the Multiple Level Precedence & Preemption Parameters screen (Figure 301: Multiple Level Precedence & Preemption Parameters screen on page 1221).

Figure 301: Multiple Level Precedence & Preemption Parameters screen

```
change system-parameters mlpp                                  Page  1 of 1

                 MULTIPLE LEVEL PRECEDENCE & PREEMPTION PARAMETERS
  ANNOUNCEMENTS
          Blocked Precedence Level: 6801          Service Interruption: 6803
     Unauthorized Precedence Level: 6802            Busy, Not Equipped: 6804
                       Vacant Code: 6805

  PRECEDENCE CALLING-DIALED DIGIT ASSIGNMENT
     Flash Override: 0  Flash: 1  Immediate: 2  Priority: 3  Routine: 4

         Attendant Diversion Timing (sec): 60
            Remote Attendant Route String:
     Worldwide Numbering Dial Plan Active? y      Default Route Digit: 0
            Precedence Call Timeout (sec): 30
      Line Load Control Restriction Level: 0
          WNDP Emergency 911 Route String:
                    Default Service Domain: 1
       ISDN Precedence Call Timeout (sec): 30
```

2. In the **Precedence Calling-Dialed Digit Assignment** fields, make any necessary changes.

   CAUTION:
   Avaya recommends that you do not change the default Precedence Calling dialed digits unless you are coordinating this change with other companion networks in your system. If the Precedence Calling digits do not match across networks, the system does not properly process the calls. Each of the Precedence Calling digits must be different. You cannot use the same digit for two different precedence levels.

   - **Flash Override**. **0** to **9** or blank (the default is **0**)
   - **Flash**. **0** to **9** or blank (the default is **1**)
   - **Immediate**. **0** to **9** or blank (the default is **2**)
   - **Priority**. **0** to **9** or blank (the default is **3**)
   - **Routine**. **0** to **9** or blank (the default is **4**)

- **Attendant Diversion Timing**. **10** to **99** seconds or blank (the default is blank)
- **Remote Attendant Route String**. 1 to 24 numeric digits or blank (the default is blank). When you administer this string, use address digits only. Do not use FACs. For more information, see Precedence Calling diversion scenarios on page 1202.
- **Precedence Call Timeout**. **10** to **60** seconds (the default is **30**)
- **Default Service Domain**. **0** to **16777215**. This number defines the system service domain, and must be unique within a switching network. The system uses the system service domain to determine eligibility for precedence calling when interswitch precedence calls over non-ISDN trunks occur.

3. Press **Enter** to save your changes.

Assigning a maximum precedence level

Maximum precedence levels are assigned to Classes of Restriction (COR).

To assign a maximum precedence level to a COR:

1. Type **`change cor n`**, where ***n*** is the number of a specific COR. Press **Enter**.

   The system displays the Class of Restriction screen.

2. Click **Next** until you see the **Maximum Precedence Level** and **MLPP Service Domain** fields (Figure 302: Class of Restriction screen on page 1222).

Figure 302: Class of Restriction screen

```
change cor 1                                                  Page   2 of 4
                              CLASS OF RESTRICTION

                     MF Incoming Call Trace? n
                Brazil Collect Call Blocking? n
                     Block Transfer Display? n
Block Enhanced Conference/Transfer Displays? y
                     Remote Logout of Agent? y

                           Station Lock COR: 1
  Outgoing Disconnect Trunk Timer (Minutes):
        Line Load Control: 3
 Maximum Precedence Level: ro           Preemptable? y
 MLPP Service Domain: 1
```

3. In the **Maximum Precedence Level** field, type one of the following values:
   - fo (Flash Override)
   - fl (Flash)
   - im (Immediate)

- pr (Priority)
- ro (Routine, the default value)

4. In the **MLPP Service Domain** field, type a number from 0 to **16777215**.

   This number defines the service domain for users and trunks to which this particular COR is assigned. The system uses the service domain to create a group of MLPP users or facilities, within which precedence calls can be made.

5. Press **Enter** to save your changes.

Assigning trunks

To assign trunks:

1. Type **add trunk-group *n***, where ***n*** is the number of a trunk group. Press **Enter**.

   The system displays the Trunk Features screen.

2. Click **Next** until you see the **DSN Term** field (Figure 303: Trunk Features screen on page 1223).

Figure 303: Trunk Features screen

```
add trunk-group 10                                    Page   2 of X
                              TRUNK FEATURES
          ACA Assignment? n             Measured: none
                                 Internal Alert? n        Maintenance Tests? y
                               Data Restriction? n
                                 Glare Handling: none
            Used for DCS? n
   Suppress # Outpulsing? n
                     Seize When Maintenance Busy: neither-end




Incoming Tone (DTMF) ANI: no                    Per Call CPN Blocking Code:
         Connected to CO? n                   Per Call CPN Unblocking Code:

                              US NI Delayed Calling Name Update? y
DSN Term? y   Precedence Incoming? dtmf(a-d)   Precedence Outgoing? dtmf(a-d)
```

3. Use the **DSN Term** field to identify the trunk group as a DSN termination telephone. The default is n.

   - The system displays the **Precedence Incoming** and **Precedence Outgoing** fields, if:
     - You type **y** in the **DSN Term** field, and

  - The value in the **Group Type** field on page 1 of this screen is **tie**.

  These two fields define whether the precedence level for dual-tone multifrequency (DTMF) or tone trunks is received or sent as digits (rotary pulses) or as DTMF signals (touchtones).

- The system does not display the **Precedence Incoming** and **Precedence Outgoing** fields, if:
  - You enter **n** in the **DSN Term** field, or
  - You enter **y** in the **DSN Term** field, and the value in the **Group Type** field on page 1 of this screen is **isdn**, or
  - You enter **y** in the **DSN Term** field, and the value in the **Group Type** field on page 1 of this screen is **tie**, and the value in both the **Outgoing Dial Type** and **Incoming Dial Type** fields on page 1 of this screen is **mf2/6**.

4. Press **Enter** to save your changes.

Assigning a hot line number

A hot line is an extension that the system automatically dials when you pick up the receiver. On a single-line telephone, assign a hot line destination. Use a system, a group, or a personal list that is administered to the hot line destination.

The hot line number must include the:

- Precedence Calling FAC
- Precedence Level digit (see Precedence Calling on page 1200)
- Destination telephone number

For example, when the system dials 807208451111, the system processes the call as a Flash Override precedence voice call to extension **720-845-1111**.

- **8** is the Precedence Calling FAC
- **0** is the Precedence Level digit for Flash Override
- **720-845-1111** is the destination telephone number

The following procedure explains how to administer number 807208451111 as a hot line destination number. To administer a hot line destination number, you must first set up a group list that contains the hot line destination number. Then you must set up the hot line destination number that references the group list.

To set up a group list:

1. Type **`add abbreviated-dialing group next`**. Press **Enter**.

   The system displays the Abbreviated Dialing List screen (Figure 304: Abbreviated Dialing List screen on page 1225).

Figure 304: Abbreviated Dialing List screen

```
add abbreviated-dialing group next                              Page 1 of 1

                            Abbreviated Dialing List

              Group List: 1           Group Name: _____________
    Size (multiple of 5): 5          Program Ext: _________ Privileged? n

DIAL CODE
     01: 807208451111
     02: _____________________________
     03: _____________________________
     04: _____________________________
     05: _____________________________
```

2. Write down the Group List number that the system assigns to this Abbreviated Dialing List.

   You use this Group List number when you set up the hot line destination number.

3. In the **Dial Code** field, type the dial code that is associated with the hot line destination number. In this example, that number is **807208451111**.
4. Press **Enter** to save your changes.

   In the next procedure, you use the Group List number that you set up in this procedure.

To set up the hot line destination number:

1. Type **add station *807208451111***. Press **Enter**.

   The system displays the Station screen (Figure 305: Station screen on page 1226).

Figure 305: Station screen

```
add station 807208451111                                        Page 1 of 4
                                    STATION

Extension: 807208451111                Lock Messages? n           BCC: 0
     Type: 2500                        Security Code:              TN: 1
     Port:                          Coverage Path 1:             COR: 1
     Name:                          Coverage Path 2:             COS: 1
                                    Hunt-to Station:

STATION OPTIONS
              Loss Group: 2            Personalized Ringing Pattern: 1
            Data Module? n                      Message Lamp Ext: 23
           Speakerphone: 2-way                Mute Button Enabled? y
       Display Language: english
                                                 Media Complex Ext:
                                                      IP Softphone? n
                                               Remote Office Phone? n
```

2. In the **Type** field, type the model of analog telephone, such as **2500**.
3. Type information in the other fields that the system requires to add this new extension.
4. Click **Next** until you see the **Hot Line Destination** area (Figure 306: Station screen on page 1226).

Figure 306: Station screen

```
add station 807208451111                                        Page 3 of 4

                                    STATION

 SITE DATA
      Room:                                              Headset? n
      Jack:                                              Speaker? n
     Cable:                                             Mounting: d
     Floor:                                          Cord Length: 0
  Building:                                            Set Color:


ABBREVIATED DIALING
     List1: 1                  List2:                     List3:

HOT LINE DESTINATION
         Abbreviated Dialing List Number (From above 1, 2, or 3): 1
                                                        Dial Code:

     Line Appearance: call-appr
```

5. In the **Abbreviated Dialing List Number (From above 1, 2, or 3)** field, type the Group List number that contains your hot line destination number.

   This is the Group List number that you wrote down from the previous procedure.

6. Press **Enter** to save your changes.

Assigning attendant queue priorities

To assign attendant queue priorities:

1. Type **change console-parameters**. Press **Enter**.

   The system displays the Console Parameters screen.

2. Click **Next** until you see the **MLPP Precedence Call** area (Figure 307: Console Parameters screen on page 1227).

Figure 307: Console Parameters screen

```
change console-parameters                                    Page 4 of 5
                              CONSOLE PARAMETERS

QUEUE PRIORITIES

               MLPP Precedence Call
                Flash Override: 2
                         Flash: 3
                     Immediate: 4
                      Priority: 5
```

3. Use the **MLPP Precedence Call** area to assign attendant queue priorities for precedence calls and nonprecedence calls. This process determines how the system queues calls to the attendant console. Depending on the priority that you want for processing calls, you can change the system defaults. The defaults are:

   - **Flash Override: 2**
   - **Flash: 3**
   - **Immediate: 4**
   - **Priority: 5**

   Important:
   By default, emergency access calls receive a higher priority processing than MLPP Precedence Calls. You can change the order of priority, but be careful when designating emergency calls to an equal or lower priority. Call types with equal priority enter the queue on a first-in, first-out basis.

   Routine precedence calls are treated as normal calls and use the same queue priorities as nonemergency and nonMLPP calls.

4. Press **Enter** to save your changes.

Announcements for Precedence Calling

This feature uses the standard recorded announcements feature in Communication Manager. For more information about administering recorded announcements, see the "Announcements" feature description.

Adding extensions

To assign extensions for Precedence Calling announcements:

1. Type **`change announcements`**. Press **Enter**.

   The system displays the Announcements/Audio Sources screen (Figure 308: Announcements/Audio Sources screen on page 1228).

Figure 308: Announcements/Audio Sources screen

```
change announcements                                        Page 1 of 16
                          ANNOUNCEMENTS/AUDIO SOURCES
     Ext.  Type       COR TN   Name                       Q   QLen Pr  Rt  Port

  1: 6801  integrated 1   1    Call blocked announcement n   N/A  n   16  01A14
  2: 6802  integrated 1   1    Unauthorized level annc   n   N/A  n   16  01A14
  3: 6803  integrated 1   1    Service interrupt annc    n   N/A  n   16  01A14
  4: 6804  integrated 1   1    Busy, not equipped annc   n   N/A  n   16  01A14
  5: 6805  integrated 1   1    Vacant code announcement  n   N/A  n   16  01A14
  6:                   1   1                              n
  7:                   1   1                              n
  8:                   1   1                              n
  9:                   1   1                              n
 10:                   1   1                              n
 11:                   1   1                              n
 12:                   1   1                              n
 13:                   1   1                              n
 14:                   1   1                              n
 15:                   1   1                              n
 16:                   1   1                              n
```

2. Assign extensions for the different MLPP recorded announcements. The extensions that you use for recorded announcements must already be administered in your dial plan. The extensions cannot be used for any other purpose, such as individual telephones or directory numbers.

3. Press **Enter** to save your changes.

   In the next procedure, you use the announcement that you set up in this procedure.

Assigning announcement types

After you add the announcement extensions, you must designate the extensions to use for each of the announcement types. This administration is unique to the Announcements for Precedence Calling feature.

To assign announcement types:

1. Type **`change system-paramters mlpp`**. Press **Enter**.

   The system displays the Multiple Level Precedence & Preemption Parameters screen (Figure 301: Multiple Level Precedence & Preemption Parameters screen on page 1221).

2. Match the extensions that you set on the Announcements/Audio Sources screen (see Figure 308: Announcements/Audio Sources screen on page 1228) with the five announcements.

3. Click **Enter** to save your changes.

Recording announcements

Once you designate the extensions to use for recorded announcements, use the following procedures to record and test the announcements. You must record the announcements from the attendant console or from a telephone that has console permissions.

To record each announcement:

1. Go off-hook and dial the FAC for the Announcement feature.
2. Dial the extension of the announcement that you want to record.

   If an announcement session is already in progress, or if a save or a restore command is in progress, you hear reorder tone. Try again later.

3. Press **1** and record the announcement after the tone.

Note:
If the announcement already exists and is marked as "protected" in the Announcements screen, you hear intercept tone.

The following wording is suggested for each of the five announcements:

- Blocked precedence call: "Equal or higher precedence calls prevented completion of your call. Please hang up and try again later."
- Unauthorized precedence level attempted: "The precedence level that you requested is not authorized for your line. Please use an authorized precedence level, or ask your operator for assistance."

- Service interruption prevented call completion: "A service interruption prevented the completion of your call. Please wait 30 seconds and try again. In case of emergency, call your operator."
- Busy, not equipped for Preemption or Precedence Call Waiting: "The number that you dialed is busy and not equipped for Preemption or Precedence Call Waiting."
- Vacant code announcement: "Your call cannot be completed as dialed. Please consult your directory and call again, or ask your operator for assistance."

4. Hang up when you finish recording each message.

Note:
The system records the sound of the receiver returning to the telephone cradle. To hang up gently, either press **Drop**, or quietly press the switchhook with your finger.

5. Wait for 15 seconds, and then dial the extension of the announcement that you just recorded. Listen to the recording.
   - If you need to record the message again, repeat this procedure.
   - If the message is satisfactory, hang up and repeat this procedure to record the other announcements.

Deleting announcements

To delete a recorded announcement:

1. Go off-hook and dial the FAC for the Announcement feature.
2. Dial the extension of the announcement that you want to delete.
3. Press **3**.

   The system deletes the announcement.
4. Hang up.
5. Type **`change announcements`** to delete the announcement extension. For more information, see Adding extensions on page 1228.

Saving announcements

If your system uses the TN750 or the TN750B circuit packs, you must manually save the announcements that you record on those circuit packs. If you do not manually save the announcements, all announcements that were recorded since the last save are lost if the:

- System loses power, or
- TN750 or the TN750B circuit packs are removed from the system

For the procedure to save announcements, see the "Announcements" feature description.

If your system uses only the TN750C circuit pack, you do not need to save the announcements. The TN750C has on-board memory for all announcements.

The announcements on a TN2501AP circuit pack, and virtual VAL announcements on the S8300 Server, are not saved through system administration. You can back up the announcement to a personal computer. For procedures to back up the announcements, see the Announcements feature description.

Precedence Call Waiting

Enabling Precedence Call Waiting for a telephone

Enable or disable the Precedence Call Waiting feature for each telephone on your system. The default assignment for each telephone is **y** (enabled).

To enable or disable Precedence Call Waiting for a telephone:

1. Type **change station *n***, where ***n*** is the telephone extension that you want to enable or disable. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Precedence Call Waiting** field (Figure 309: Station screen on page 1232).

Figure 309: Station screen

```
change station 9876543                                          Page 2 of 4

                                    STATION
FEATURE OPTIONS
           LWC Reception: spe           Auto Select Any Idle Appearance? n
          LWC Activation? y                     Coverage Msg Retrieval? y
  LWC Log External Calls? n                               Auto Answer: none
            CDR Privacy? n                          Data Restriction? n
   Redirect Notification? y                 Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                   Restrict Last Appearance? y
  Active Station Ringing? single

        H.320 Conversoin? n       Per Station CPN - Send Calling Number? n
       Service Link Mode: as-needed
         Multimedia Mode: basic                 Audible Message Waiting? y
    MWI Served User Type:                    Display Client Redirection? n
             AUDIX Name:                    Select last Used Appearance? n
                                              Coverage After Forwarding? s
         Automatic Moves: no
                                         Direct IP-IP Audio Connections? y
  Emergency Location Ext: 23                       IP Audio Hairpinning? y
 Precedence Call Waiting? y
```

3. In the **Precedence Call Waiting** field, perform one of the following actions:
   - Type **y** to enable the Precedence Call Waiting feature.
   - Type **n** to disable the Precedence Call Waiting feature.
4. Press **Enter** to save your changes.

Setting the Precedence Call timeout

To set the Precedence Call Waiting timeout:

1. Type **`change system-paramters mlpp`**. Press **Enter**.

   The system displays the Multiple Level Precedence & Preemption Parameters screen (Figure 301: Multiple Level Precedence & Preemption Parameters screen on page 1221).
2. In the **Precedence Call Timeout (sec)** field, set the number of seconds before a precedence call is timed out.

   The valid values are 10 to 60 seconds, with a default of 30 seconds.
3. In the **ISDN Precedence Call Timeout (sec)** field, set the number of seconds before an ISDN precedence call is timed out.

   The valid values are 10 to 60 seconds, with a default of 30 seconds.

4. Press **Enter** to save your changes.

Assigning Feature Access Codes

For users of single-line analog telephones, you must assign a Feature Access Code (FAC) to answer a Precedence Call Waiting call.

To assign a FAC:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 310: Feature Access Code (FAC) screen on page 1233).

Figure 310: Feature Access Code (FAC) screen

```
change feature-access-codes                                  Page   1 of 8
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: #01
         Abbreviated Dialing List2 Access Code: #02
         Abbreviated Dialing List3 Access Code: #03
Abbreviated Dial - Prgm Group List Access Code: #04
                      Announcement Access Code: #05
                       Answer Back Access Code: #14
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: *9    Access Code 2: *33
                Automatic Callback Activation: #55    Deactivation: *55
                   Call Forwarding Activation: #44    Deactivation: *44
                         Call Park Access Code: #76
                       Call Pickup Access Code: #33
CAS Remote Hold/Answer Hold-Unhold Access Code: #57
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
                  Contact Closure    Open Code:          Close Code:
                  Contact Closure   Pulse Code:
```

2. In the **CAS Remote Hold/Answer Hold-Unhold Access Code** field, assign a FAC that matches your dial plan.
3. Press **Enter** to save your changes.
4. Ensure that you notify all users about the assigned FAC.

Precedence Routing

This section contains procedures for administering Precedence Routing when the local and the remote DSN nodes are both Avaya communication servers. Contact your Avaya representative for assistance with:

- Trunk administration when you connect local DS1 trunks to a DSN node that uses an Avaya communication server
- Administration procedures when you connect local DS1 trunks to a DSN node that uses a Nortel switch
- Administration procedures when you connect local DS1 trunks to a DSN node that uses a Siemens switch

Assigning digit analysis

Digit analysis determines what routes are used for outgoing calls based on the digits dialed.

To assign digit analysis:

1. Type **`change precedence-routing analysis n`**, where ***n*** is the digit or digits being analyzed. Press **Enter**.

   The system displays the Precedence Routing Digit Analysis Table screen (Figure 311: Precedence Routing Digit Analysis Table screen on page 1235).

Figure 311: Precedence Routing Digit Analysis Table screen

```
change precedence-routing analysis 10                          Page 1 of 2

                    PRECEDENCE ROUTING DIGIT ANALYSIS TABLE
                                                      Percent Full: 22

          Dialed          Total     Route    Preempt
          String         Min  Max  Pattern   Method
    002383               9    9     36       group
    002385               9    9     35       group
    002388               9    9     86       group
    003032383            12   12    36       group
    003032388            12   12    86       group
    003033383            12   12    34       group
    003033388            12   12    84       group
    003034383            12   12    32       group
    003034388            12   12    82       group
    003035383            12   12    30       group
    003035388            12   12    80       group
    003383               9    9     34       group
    003385               9    9     33       group
    003388               9    9     84       group
    004383               9    9     32       group
```

Except for the **Preempt Method** field, the digit analysis administration is the same as Automatic Route Selection (ARS) and Automatic Alternate Routing (AAR) digit analysis.

2. Format the **Dialed String** field for routing DSN numbers:

   - For non-WNDP dialing, enter the precedence digit and the address digits. The precedence digit is usually a number from 0 to 4.
   - For WNDP dialing, enter the precedence digit, the route code, and the address digits. The precedence digit is usually a number from 0 to 4.

   An **x** in the digit string is a wildcard that matches any single digit.

   The **Preempt Method** field has two possible values, **group** and **route**. The default preemption is **group**.

   With group preemption:

   a. The system checks the first trunk group in the route pattern to determine if any trunks are idle. If the system finds an idle trunk, the system connects the call.

   b. If no trunks are idle, the system checks the same trunk group to determine if any trunks are preemptable. If the system finds a preemptable trunk, the system preempts the current call and connects the new call.

   c. If no trunks are idle or preemptable, the system checks the next trunk group to determine if any trunks are idle. If the system finds an idle trunk, the system connects the call.

d. If no trunks are idle, the system checks the same trunk group to determine if any trunks are preemptable. If the system finds a preemptable trunk, the system preempts the current call and connects the new call.

e. If the system does not find an idle trunk or a preemptable trunk within the Precedence Call Timeout interval, the caller hears either the Blocked Precedence recorded announcement or reorder tone. For more information, see Announcements for Precedence Calling on page 1209. Calls with Routine precedence cannot preempt any other calls. If a call with Routine precedence does not find an idle trunk, the caller receives busy tone.

For example, trunk groups 1, 2, and 3 are set up as follows:

- Trunk group 1 has two trunk members active with Flash and Flash Override precedence calls.
- Trunk group 2 has two trunk members active with Immediate and Priority precedence calls.
- Trunk group 3 has two trunk members, both of which are idle.

A user makes a new call with the Flash precedence level. The system processes the call as follows:

1. The system checks trunk group 1, and does not find an idle trunk. The system then checks trunk group 1, and does not find a preemptable active call.
2. The system checks trunk group 2, and does not find an idle trunk. The system then checks trunk group 2, and finds two preemptable active calls. The system preempts the first trunk member that the system finds with a lower precedence level. In this example, the new Flash call preempts the active Immediate precedence call.
3. The system never checks trunk group 3, even though trunk group 3 has idle trunks.

With route preemption:

1. The system checks each trunk group in the route pattern to determine if any trunks are idle. If the system finds an idle trunk, the call is connected.
2. If the system does not find an idle trunk, the system checks each trunk group in the route pattern to determine if any trunks are preemptable. If the system finds a preemptable trunk, the system preempts the current call and connects the new call.
3. If the system does not find an idle trunk or a preemptable trunk within the Precedence Call Timeout interval, the caller hears either the Blocked Precedence recorded announcement or reorder tone. For more information, see Announcements for Precedence Calling on page 1209. Calls with Routine precedence cannot preempt any other calls. If a call with Routine precedence does not find an idle trunk, the caller receives busy tone.

For example, trunk groups 1, 2, and 3 are set up as follows:

- Trunk group 1 has two trunk members active with Flash and Flash Override precedence calls.

- Trunk group 2 has two trunk members active with Immediate and Priority precedence calls.
- Trunk group 3 has two trunk members, both of which are idle.

A user makes a new call with the Flash precedence level. The system processes the call as follows:

1. The system checks trunk group 1, and does not find an idle trunk.
2. The system checks trunk group 2, and does not find an idle trunk.
3. The system checks trunk group 1, and finds an idle trunk. The system completes the new Flash call using the first idle trunk.
4. Press **Enter** to save your changes.

Assigning route patterns

The system uses these routing patterns for outgoing calls.

To assign route patterns:

1. Type **change route-pattern *n***, where ***n*** is a route pattern from the Precedence Routing Digit Analysis Table screen. Press **Enter**.

   The system displays the Pattern Number screen (Figure 312: Pattern Number screen on page 1238).

Figure 312: Pattern Number screen

```
change route-pattern 36                                          Page 1 of 1
                           Pattern Number: 36

   Grp. FRL NPA Pfx Hop Toll No.  Inserted                          DCS/IXC
   No.          Mrk Lmt List Del  Digits                            QSIG
                              Dgts                                  Intw
 1: 15    0                   1                                    n    user
 2: 12    1                   1                                    n    user
 3: 7     0                   1                                    n    user
 4: 22    0                   1                                    n    user
 5:                                                                n    user
 6:                                                                n    user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature BAND  No. Numbering LAR
    0 1 2 3 4 W     Request                                  Dgts Format
                                                          Subaddress
 1: y y y y y n  n           rest                                      none
 2: y y y y y n  n           rest                                      none
 3: y y y y y n  n           rest                                      none
 4: y y y y y n  n           rest                                      none
 5: y y y y y n  n           rest                                      none
 6: y y y y y n  n           rest                                      none
```

2. For DSN trunks that have the **Precedence Mode Outgoing** field set for DTMF, you must delete one digit. If you do not delete one digit, the system sends the precedence level digit twice.
3. Press **Enter** to save your changes.

Assigning digit conversion

Digit conversion takes digits that were dialed on incoming calls, and converts the digits to local telephone numbers. These local numbers usually are extensions.

To assign the Precedence Routing digit conversion:

1. Type **`change precedence-routing digit-conversion`**. Press **Enter**.

   The system displays the Precedence Routing Digit Conversion Table screen (Figure 313: Precedence Routing Digit Conversion Table screen on page 1239).

Figure 313: Precedence Routing Digit Conversion Table screen

```
change precedence-routing digit-conversion 0            Page   1 of   2

                  PRECEDENCE ROUTING DIGIT CONVERSION TABLE
                                                          Percent Full: 11

  Matching Pattern     Min   Max   Del   Replacement String   Net  Conv

  x2386                8     8     4                          ext   n
  x3032386             11    11    7                          ext   n
  x3033386             11    11    7                          ext   n
  x3034386             11    11    7                          ext   n
  x3035386             11    11    7                          ext   n
  x3386                8     8     4                          ext   n
  x4386                8     8     4                          ext   n
  x5386                8     8     4                          ext   n
  x6                   5     5     1                          ext   n
  xx2386               9     9     5                          ext   n
  xx3032386            12    12    8                          ext   n
  xx3033386            12    12    8                          ext   n
  xx3034386            12    12    8                          ext   n
  xx3035386            12    12    8                          ext   n
```

2. Format the **Matching Pattern** field for routing DSN numbers:
   - For non-WNDP dialing, enter the precedence digit and the address digits. The precedence digit is usually a number from 0 to 4.
   - For WNDP dialing, enter the precedence digit, the route code, and the address digits. The precedence digit is usually a number from 0 to 4.

   An **x** in the digit string is a wildcard that matches any single digit.
3. In the **Net** fields, type **ext** or **pre**.
   - **ext** stands for extension, and uses ARS tables or AAR tables to route the call.
   - **pre** stands for precedence routing, and uses the Precedence Analysis Tables to route the call.
4. Press **Enter** to save your changes.

Dual Homing

You administer Dual Homing when you administer the Precedence Routing feature. For more information, see Precedence Routing on page 1234.

End Office Access Line Hunting

You administer End Office Access Line Hunting when you administer the Precedence Routing feature. For more information, see Precedence Routing on page 1234.

Preemption

Assigning Preemption to a COR

To assign Preemption to a COR:

1. Type **change cor *n***, where ***n*** is the number of a specific COR. Press **Enter**.

   The system displays the Class of Restriction screen.

   Click **Next** until you see the **Preemptable** field (Figure 314: Class of Restriction screen on page 1240).

Figure 314: Class of Restriction screen

```
change cor 36                                                Page 2 of 4

                              CLASS OF RESTRICTION

                    MF Incoming Call Trace? n
               Brazil Collect Call Blocking? n
                    Block Transfer Display? n
Block Enhanced Conference/Transfer Display? n
                    Remote Logout of Agent? n

                           Station Lock COR:
 Outgoing Trunk Disconnect Timer (minutes):
       Line Load Control:1
Maximum Precedence Level: ro              Preemptable? y
MLPP Service Domain?
```

2. In the **Preemptable** field, define whether extensions or trunks that you assign to this COR can be preempted. The default value is **y**.
3. Press **Enter** to save your changes.

Assigning trunks for Preemption

For the Preemption feature, enabling a trunk as a DSN termination telephone guarantees that the trunk can accept the Preemption signaling over the DSN. To assign trunks, see Assigning trunks on page 1223.

Setting the Precedence Call timeout

See Assigning Precedence Calling system parameters on page 1221.

Line Load Control

Line Load Control (LLC) is assigned on a system-wide basis and on a COR basis.

Assigning the LLC level for the system

1. Type **`change system-parameters mlpp`**. Press **Enter**.

   The system displays the Multiple Level Precedence & Preemption Parameters screen (Figure 301: Multiple Level Precedence & Preemption Parameters screen on page 1221).
2. Set the LLC level for the system. In the **Line Load Control Restriction Level** field, type one of the following options:
   - 0 - The LLC feature is not active. There are no restrictions. This is the default value.
   - 2 - Restrict extensions with a COR that is assigned to LLC level 2, 3, or 4.
   - 3 - Restrict extensions with a COR that is assigned to LLC level 3 or 4.
   - 4 - Restrict extensions with a COR that is assigned to LLC level 4.
3. Press **Enter** to save your changes.

Assigning the LLC to a COR

1. Type **`change cor n`**, where ***n*** is the number of a specific COR. Press **Enter**.

   The system displays the Class of Restriction screen.
2. Click **Next** until you see the **Line Load Control** field (Figure 302: Class of Restriction screen on page 1222).
3. Set the LLC level for each COR. In the **Line Load Control** field, type one of the following options:
   - 1 - LLC Level 1. The COR cannot be restricted by LLC. This is the default value.
   - 2 - LLC Level 2
   - 3 - LLC Level 3

- 4 - LLC Level 4

4. Press **Enter** to save your changes.

Worldwide Numbering and Dialing Plan

Assigning WNDP system parameters

To assign WNDP system parameters:

1. Type **`change system-parameters mlpp`**. Press **Enter**.

   The system displays the Multiple Level Precedence & Preemption Parameters screen (Figure 301: Multiple Level Precedence & Preemption Parameters screen on page 1221).

2. Administer the following fields:

   - **Worldwide Numbering Dial Plan Active**. Type either y or n . The default is n.
   - **Default Route Digit**. The system displays this field when the **Worldwide Numbering Dial Plan Active** field is enabled. You must enter a valid digit in this field. Valid entries are:

     0 - Voice call (the default value)

     1 - Circuit switched data call

     2 - Satellite avoidance call

     3 - (reserved)

     4 - (reserved)

     5 - Hotline voice grade call

     6 - Hotline data grade call

     7 - (reserved)

     8 - (reserved)

     9 - (reserved)

   - **WNDP Emergency 911 Route String**. 1 to 24 numeric digits or blank. The default is blank. For more information, see Interactions for Multiple Level Precedence and Preemption on page 1247.

     Valid entries for this field can be a trunk access code (TAC), the AAR or the ARS access code, a WNDP access code, or an extension. The extension might be, for example, the firehouse at a base that handles emergency calls. If you use a WNDP access code, use the access code for the lowest precedence calling level in the system.

3. Press **Enter** to save your changes.

Assigning WNDP Feature Access Codes

Administer the WNDP precedence FACs only when you use WNDP dialing. Do not administer the WNDP precedence FACs when you use precedence dialing.

To assign a FAC:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Click **Next** until you see the **WNDP Precedence Access Codes** area (Figure 300: Feature Access Code (FAC) screen on page 1220).

Note:
You must also define a value in the **Precedence Calling Access Code** field, even when you use WNDP dialing. Use the Precedence Calling FAC when you administer Precedence Routing trunks. For more information, see Assigning an MLPP Feature Access Code on page 1220.

3. In the **WNDP Precedence Access Codes** area, type a 2-digit FAC that conforms to your dial plan in each field. Each FAC must begin with the number **9**.
4. Press **Enter** to save your changes.
5. Ensure that you notify all users about the assigned FACs.

Assigning a hot line number

A hot line is an extension that the system automatically dials when you pick up the receiver. On a single-line telephone, assign a hot line destination. Use a system, a group, or a personal list that is administered to the hot line destination.

The hot line number must include:

- The WNDP Dialing 2-digit FAC for the precedence level that you want.
- As an option, you can also include the number **1** as the Route Code setup digit. For more information, see Worldwide Numbering and Dialing Plan on page 1213. If you do not use a Route Code setup digit, the system uses the default digit **0**.

  If you use the Route Code setup digit **1**, you must use a routing digit. The next number in the sequence is the routing digit. For example, **5** is a hot line voice call, and **6** is a hot line data call. For more information, see Worldwide Numbering and Dialing Plan on page 1242.
- The destination telephone number.

For example, when the system dials 90157208451111, the system processes the call as a Flash Override WNDP voice call to extension **720-845-1111**.

- **90** is the two-digit WNDP dialing FAC indicating Flash Override.
- **1** is the optional Route Code setup digit.
- **5** is the routing digit that indicates a voice hot line call.

- **720-845-1111** is the destination telephone number.

The following procedure explains how to administer number 90157208451111 as a hot line destination number. To administer a hot line destination number, you must first set up a group list that contains the hot line destination number. Then you must set up the hot line destination number that references the group list.

To set up a group list:

1. Type **`add abbreviated-dialing group next`**. Press **Enter**.

   The system displays the Abbreviated Dialing List screen (Figure 304: Abbreviated Dialing List screen on page 1225).

2. Write down the Group List number that the system assigns to this Abbreviated Dialing List.

   You use this Group List number when you set up the hot line destination number.

3. In the **Dial Code** field, type the dial code that is associated with the hot line destination number. In this example, that number is 90157208451111.

4. Press **Enter** to save your changes.

   In the next procedure, you use the Group List number that you set up in this procedure.

To set up the hot line destination number:

1. Type **`add station`** ***`90157208451111`***. Press **Enter**.

   The system displays the Station screen (Figure 305: Station screen on page 1226).

2. In the **Type** field, type the model of analog telephone, such as **2500**.

3. Type information in the other fields that the system requires to add this new extension.

4. Click **Next** until you see the **Hot Line Destination** area (Figure 306: Station screen on page 1226).

5. In the **Abbreviated Dialing List Number (From above 1, 2, or 3)** field, type the Group List number that contains your hot line destination number.

   This is the Group List number that you wrote down from the previous procedure.

6. Press **Enter** to save your changes.

Assigning attendant queue priorities

See Assigning attendant queue priorities on page 1227.

Considerations for Multiple Level Precedence and Preemption

This section provides information about how the Multiple Level Precedence and Preemption feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Multiple Level Precedence and Preemption under all conditions. The following considerations apply to Multiple Level Precedence and Preemption:

Precedence Calling

Except for a G350 or a G700 Media Gateway that is supported by an S8300, an S8500, or an S8700 Server, a tone clock circuit pack is required for this feature. On the DEFINITY server, all tone clocks must be TN2182B or later, except when you use MF 2/6 trunks. MF 2/6 trunks require the TN2182C, vintage 2, circuit pack or later.

Announcements for Precedence Calling

When you use the announcement capabilities on a G650, an SCC1, or a MCC1 Media Gateway, use the TN2501AP or the TN750 circuit packs to record announcements on the following servers:

- DEFINITY server
- S8100 Server
- S8500 Server
- S8700 Server

You can also use existing analog announcement equipment with the MLPP features.

If you have multiple integrated announcement circuit packs, only one of those circuit packs can be a TN750 or a TN750B. Any additional circuit packs must be a TN2501AP or a TN750C.

Precedence Call Waiting

Except for an S8300 Server, a tone clock circuit pack is required for this feature. On a DEFINITY server and an IP600 IP Server, all tone clocks must be TN2182B or later, except when using MF 2/6 trunks. MF 2/6 trunks require the TN2182C, vintage 2, circuit pack or later.

You can assign Precedence Call Waiting to all models of telephones, including IP hardphones and softphones.

Precedence Routing

The routing that you administer with Precedence Routing uses the same capacity tables as the ARS feature. These tables include patterns and analysis tables. You can view the real-time capacity usage with the **change precedence-routing analysis** command. The **Percent Full** field displays how much of the available capacity is used for routing information.

H.323 IP trunks do not support data calls that use any type of modem or data module. Do not administer H.323 IP trunks for users who make data calls over trunk facilities. H.323 IP trunks can be used for voice calls.

Preemption

A tone clock circuit pack is required for this feature. All tone clocks must be TN2182B or later, except when using MF 2/6 trunks. MF 2/6 trunks require the TN2182C, vintage 2, circuit pack or later.

The call progress tones for Preemption consist of a fixed tone and a pattern. You cannot change the call progress tones by typing the **change system-parameters country-options** command.

Line Load Control

When a system reload occurs, the LLC system-level settings revert to the default factory setting. The default factory setting is LLC level **0**, which indicates no restrictions. Normal telecommunications service is restored after a system reload.

The LLC COR settings, however, are saved in translations. The settings do not revert to the factory defaults if the settings were saved in translations.

Worldwide Numbering and Dialing Plan

The Route Control Digit of the Worldwide Numbering and Dialing Plan (WNDP) feature is not available as part of the MLPP feature set.

The Route Control Digit of WNDP is not the same as the Route Code digit.

Users must dial any destination telephone number that starts with the number **1**, such as extension 1500, as follows: **1**, the Route Code digit, then the destination number. For example, dial 1*x*1500, where *x* is the Route Code digit.

H.323 IP trunks do not support data calls. Do not administer H.323 IP trunks for users that make data calls over trunk facilities. H.323 IP trunks can be used for voice calls.

Interactions for Multiple Level Precedence and Preemption

This section provides information about how the Multiple Level Precedence and Preemption feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Multiple Level Precedence and Preemption in any feature configuration.

Precedence Calling

- Attendant Vectoring

  Attendant Vectoring uses the Call Vectoring feature to provide flexible routing of attendant-seeking calls. When the system accesses an attendant VDN, the call can be answered by the attendant, routed to an announcement, or routed to the voice mailbox of the assigned night station. This process reduces the chance of precedence calls remaining in the attendant queue, specifically where the attendant has not answered all calls in the queue, and the console is placed in night mode. Attendant Vectoring can be purchased as a standalone feature. Contact your Avaya representative for more information.

  For more information about Attendant Vectoring, see *DEFINITY ECS Call Vectoring/EAS Guide*, 555-230-521.

- Call Coverage

  Calls above Routine precedence do not follow administered coverage paths. The calls ring until the Timeout for Precedence Calls expires, and the call goes to a console or a night telephone. If the called party is on an active call and Preemption is enabled, the call is preempted.

- Call Detail Recording (CDR)

  No separate CDR field is supplied for the precedence level of a call. **No separate CDR** field creates an incompatibility between current call accounting software and the new call record format. With the current call record format, you can examine the call record for the Precedence Calling FAC to determine the precedence level of a call. If the call is a precedence call, the first digit of the number that was dialed indicates the precedence level of the call. If WNDP is active, you need to examine only the FAC because the precedence level is implied from the FAC. The CDR feature does not record the precedence level for a station-to-station call.

  CDR can be administered to record either the dialed digits or the outpulsed digits. In the case of Precedence Routing, the outpulsed digits can appear dramatically different from the dialed digits. When you view CDR records, remember that the precedence level digit might not be recorded.

- Conference

  When two calls are merged during a conference, the precedence level of a call is set to the highest active precedence level.

- Hunting

  When you administer a hunt group with preemption, set the **Maximum Preemption Level** field and the **Preemptable** field in the Class of Restriction screen. The hunt group **Group Type** must use **circular** or **ucd-mia queuing**, and the **ACD**, the **Queue**, and the **Vector** fields must be set to **n**.

- Night Service

  When the attendant console goes into Night Service, users can answer precedence calls from a night telephone, a night or a day/night console, or the Trunk Answer Any Station (TAAS) feature. If calls are in the queue when the attendant console goes into Night Service, those queued calls are diverted to a night or a day/night console or TAAS, based on the attendant queue priorities. For more information, see "Assigning attendant queue priorities" in the "Administering" section.

- Preemption

  When a precedence call attempts to preempt an existing call, call progress tones, or the "blocked precedence call" announcement, indicates why the system did not complete the call.

  The following table shows how the system processes precedence calls based on the precedence level of the call and the precedence level of the preempted trunk.

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Flash Override	Flash Override	Recorded announcement or busy tone
Flash	Flash Override	Recorded announcement or busy tone
Immediate	Flash Override	Recorded announcement or busy tone
Priority	Flash Override	Recorded announcement or busy tone
Routine	Flash Override	Busy tone
Flash Override	Flash	Call completes normally
Flash	Flash	Recorded announcement or busy tone
Immediate	Flash	Recorded announcement or busy tone
Priority	Flash	Recorded announcement or busy tone
Routine	Flash	Busy tone

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Flash Override	Immediate	Call completes normally
Flash	Immediate	Call completes normally
Immediate	Immediate	Recorded announcement or busy tone
Priority	Immediate	Recorded announcement or busy tone
Routine	Immediate	Busy tone
Flash Override	Priority	Call completes normally
Flash	Priority	Call completes normally
Immediate	Priority	Call completes normally
Priority	Priority	Recorded announcement or busy tone
Routine	Priority	Busy tone
Flash Override	Routine	Call completes normally
Flash	Routine	Call completes normally
Immediate	Routine	Call completes normally
Priority	Routine	Call completes normally
Routine	Routine	Busy tone

- Restrict Last Appearance

  If the Restrict Last Appearance telephone option is enabled, and only one idle call appearance is available on the telephone when a precedence call is made to that telephone, callers who use Routine precedence hear busy tone. Callers who use any other precedence level connect to the restricted last call appearance.

  If the Restrict Last Appearance telephone option is not enabled, and only one idle call appearance is available on the telephone when a precedence call is made to that telephone, callers using any precedence level connect to the last call appearance.

- Send All Calls

  Calls above Routine precedence do not follow administered coverage paths. Calls ring until the Timeout for Precedence Calls expires, and then calls go to an attendant console or a night telephone.

- Transfer

  When two calls are merged during a transfer, the precedence level of a call is set to the highest active precedence level.

- Worldwide Numbering and Dialing Plan (WNDP)

  When WNDP is enabled, users must dial a FAC for the precedence level that the users want to use. Users cannot use the Precedence Calling FAC. In addition, the Route Code function and the implied precedence level are provided.

  When WNDP is disabled, users must dial the Precedence Calling FAC, and then the precedence level, a number between **0** and **4**. The WNDP FACs can be administered, but cannot be used.

Precedence Call Waiting

- Attendant Console

  Precedence Call Waiting calls from attendant consoles or telephones with console permissions are not allowed. Calls from an attendant console cannot camp onto a call with Precedence Call Waiting. The attendant console user hears a recorded announcement.

- Automatic Callback

  If the Automatic Callback feature is activated and Precedence Call Waiting is attempted, the caller hears a recorded announcement.

- Call Forwarding

  An extension can have Precedence Call Waiting and Call Forwarding active at the same time. If the user is active on a call and another call comes in, the called party hears the Precedence Call Waiting tone. The call is forwarded after the timeout. Any other calls that arrive during the timeout period go immediately to the forwarded telephone.

- Call Pickup

  If a member of a pickup group who is active on a call receives Precedence Call Waiting, other members of the pickup group cannot pick up the call.

- Call Waiting
  - For a Routine Precedence Call, a user who is on an active call hears the standard Call Waiting tone.
  - Precedence Call Waiting is denied if the called party already has one call currently waiting in queue.

- Data Privacy

  Precedence Call Waiting cannot be applied to a line with Data Privacy.

- Data Restriction

  Precedence Call Waiting cannot be applied to a line with Data Restriction.

- Line Load Control (LLC)

  If the LLC feature restricts a telephone, that user must hang up to answer a Precedence Call Waiting call.

- Preemption

  Regardless of how you administer Precedence Call Waiting, calls with a higher level of precedence always preempt calls with a lower level of precedence.

- Tenant Service Partitioning

  Timeout redirection does not occur. Tenant Service Partitioning calls continue to ring at the called extension.

Precedence Routing

- General

  Precedence Routing allows calls with a precedence higher than Routine to terminate to:

  — Trunks
  — Telephones
  — Attendant consoles
  — Hunt groups
  — Recorded announcements

  Precedence Routing calls cannot terminate at Vector Directory Numbers (VDNs) or Terminating Extension Groups (TEGs).

- Call Detail Recording (CDR)

  No separate CDR field is supplied for the precedence level of a call. **No separate CDR** field creates an incompatibility between current call accounting software and the new call record format. With the current call record format, you can examine the call record for the Precedence Calling FAC to determine the precedence level of a call. If the call is a precedence call, the first digit of the number that was dialed indicates the precedence level of the call. If WNDP is active, you need to examine only the FAC because the precedence level is implied from the FAC. The CDR feature does not record the precedence level for a station-to-station call.

  CDR can be administered to record either the dialed digits or the outpulsed digits. In the case of Precedence Routing, the outpulsed digits can appear dramatically different from the dialed digits. When you view CDR records, remember that the precedence level digit might not be recorded.

- Shortcut Dialing

  When you use the Shortcut Dialing feature over DSN trunks, the system uses the Precedence Routing analysis tables to administer the incoming Shortcut Dialing digit analysis. The system does not use the ARS analysis tables.

- Traveling Class Marks TCM)

  Precedence Routing passes all TCM information over DSN and non-DSN trunks.

Preemption

- General

  Calls can be preempted that terminate at:

  - Trunks
  - Telephones
  - Attendant consoles
  - Nonqueued hunt groups
  - Vector Directory Numbers (VDNs)

  Since Precedence Routing does not allow precedence calls to terminate at queued hunt groups or Terminating Extension Groups (TEGs), other calls to these facilities cannot be preempted.

- Adjunct Switch Applications Interface (ASAI)

  ASAI is notified if a call is preempted and disconnected from the current call.

- CM Messaging system

  The CM Messaging system is notified if a call is preempted and disconnected from the current call.

- Call Detail Recording (CDR)

  CDR has two records for a preempted call. CDR has a record of the original call, and a record of the new call after the preemption.

- Call Management System (CMS)

  CMS is notified if a call is preempted and disconnected from the current call.

- Call Coverage

  A call that the system redirects to a coverage point cannot be preempted.

- Call Pickup

  A call that uses Call Pickup cannot be preempted.

- Code Calling Access

  A call that uses Code Calling Access cannot be preempted.

- Avaya Interactive Voice Response (IVR) system

  The system notifies the IVR system if the system preempts and disconnects a call from the current call.

- Group Paging

  A call that is part of a group page cannot be preempted.

- Loudspeaker Paging

  A call that uses Loudspeaker Paging cannot be preempted.

- Malicious Call Trace

  A call that uses Malicious Call Trace cannot be preempted.

- Modem Pooling

  A call that uses a modem pool cannot be preempted.

- Personal central office line (PCOL)

  A call that uses PCOL cannot be preempted.

- Precedence Calling

  When a precedence call attempts to preempt an existing call, call progress tones or the "blocked precedence call" announcement indicates why the system did not complete the call.

  The following table shows how precedence calls are processed, depending on the precedence level of the call and the precedence level of the preempted trunk.

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Flash Override	Flash Override	Recorded announcement or busy tone
Flash	Flash Override	Recorded announcement or busy tone
Immediate	Flash Override	Recorded announcement or busy tone
Priority	Flash Override	Recorded announcement or busy tone
Routine	Flash Override	Busy tone
Flash Override	Flash	Call completes normally
Flash	Flash	Recorded announcement or busy tone
Immediate	Flash	Recorded announcement or busy tone
Priority	Flash	Recorded announcement or busy tone
Routine	Flash	Busy tone
Flash Override	Immediate	Call completes normally
Flash	Immediate	Call completes normally
Immediate	Immediate	Recorded announcement or busy tone
Priority	Immediate	Recorded announcement or busy tone

Precedence level of the call	Precedence level of the DSN trunk call that is being preempted	Call treatment
Routine	Immediate	Busy tone
Flash Override	Priority	Call completes normally
Flash	Priority	Call completes normally
Immediate	Priority	Call completes normally
Priority	Priority	Recorded announcement or busy tone
Routine	Priority	Busy tone
Flash Override	Routine	Call completes normally
Flash	Routine	Call completes normally
Immediate	Routine	Call completes normally
Priority	Routine	Call completes normally
Routine	Routine	Busy tone

- Precedence Call Waiting

  Regardless of how you administer Precedence Call Waiting, calls with a higher level of precedence always preempt calls with a lower level of precedence.

- Radio Paging

  You cannot preempt a call that uses Radio Paging.

- Recorded Announcements

  You cannot preempt a call that is connected to a recorded announcement.

- Secondary Extension

  You cannot preempt a call that uses a secondary extension.

- Transient calls

  You cannot preempt calls, either ringing or on hold, that are in a transient mode.

Line Load Control

- General

  Since the Line Load Control (LLC) feature restricts telephones from originating calls, features that require dial tone or a new call appearance for activation are unavailable when LLC is restricting the telephone. Some of those features include:

  - Call Forwarding
  - Call Pickup
  - Conference
  - Transfer

  You can still activate features that use buttons, where dial tone is not required. Some of those features include:

  - Send All Calls
  - Inspect
  - Integrated Directory

- Bridged Call Appearance

  The LLC feature restricts originating new calls from all call appearances on a telephone, including bridged appearances. A telephone that is restricted by the LLC feature, and that has a bridged appearance of an extension whose telephone is *not* restricted, can bridge onto an active call, but cannot originate a new call through that bridged extension.

  A telephone that is *not* restricted by the LLC feature, and that has a bridged appearance of an extension whose telephone *is* restricted, can originate a new call through that bridged extension.

- Call Park

  A user on a call becomes restricted by the LLC feature. The user can park the call, but cannot retrieve the call until the LLC restriction is removed. Another user that is not currently restricted by the LLC feature can retrieve the call.

- Call Waiting

  A user whose telephone is restricted by the LLC feature must hang up to answer a Call Waiting call. The LLC feature does not restrict incoming calls.

- Hold

  Telephones that are restricted by the LLC feature, and that are on an active call, can place a call on hold and later retrieve the call that is on hold.

- Precedence Call Waiting

  A user whose telephone is restricted by the LLC feature must hang up to answer a Precedence Call Waiting call.

Worldwide Numbering and Dialing Plan (WNDP)

- Emergency 911 Calling

  If WNDP dialing is administered to use the digits 91 as a FAC, this FAC conflicts with dialing 911 to reach an emergency service agency. If a user dials 911 with WNDP enabled, the call does not go through to the emergency service agency because the system is waiting for more digits after dialing 91.

  To work around this interaction, you can take all or any the following actions:

  - Instruct users to first dial the ARS FAC and then dial 911. For example, if the ARS FAC is 8, a user can dial **8911**. This option works for any emergency number, such as 999 in the United Kingdom.
  - Instruct users to dial the assigned WNDP FAC followed by 911. For example, if one of the WNDP FACs is 92, a user can dial **92911**. This option works for any emergency number, such as 999 in the United Kingdom.
  - Administer a WNDP Emergency 911 Route String. This route string is outpulsed when a user dials either 911 and waits for the interdigit timeout, or dials 911 and then presses the pound key (#). This dialing option works only when the WNDP Flash FAC is 91.

  If the telephone that you use for an emergency call does not have adequate calling permissions, the emergency call does not go through. This situation can happen in the following conditions:

  - The Facility Restriction Level (FRL) of the telephone is not high enough.
  - The precedence calling level of the telephone is not high enough.
  - The telephone is not allowed to use a higher precedence level for the call.
  - No trunk facilities are available, and the precedence level of the call is not high enough to preempt another call.
  - The hop limit is exceeded when call is routed over tandem trunks.

- Hunting

  When you administer a hunt group with preemption, set the **Maximum Preemption Level** field and the **Preemptable** field in the Class of Restriction screen. The hunt group **Group Type** must use **circular** or **ucd-mia queuing**, and the **ACD**, the **Queue**, and the **Vector** fields must be set to **n**.

- Precedence Calling

  When WNDP is enabled, users must dial a FAC for the precedence level that the users want to use. Users cannot use the Precedence Calling FAC. In addition, the Route Code function and the implied precedence level are provided.

  When WNDP is disabled, users must dial the Precedence Calling FAC, and then the precedence level, a number between **0** and **4**. The WNDP FACs can be administered, but cannot be used.

Multi-Location Dial Plan

Use the Multi-Location Dial Plan feature to preserve dial plan uniqueness for extensions and attendants when you migrate to a single S87xx distributed network. Without this feature, dial plan uniqueness is not preserved when you migrate from multiple QSIG or distributed communication system (DCS) networks.

Migrating to a single distributed network reduces the number of systems you must maintain. With a single network, you administer one system and one dial plan. However, with a single distributed network, some features no longer work transparently across multiple locations as before the migration.

For example, in multiple QSIG or DCS networks, each location of a department store might have its own system. Therefore, the same telephone extension might represent a unique department in all stores. Extension 4321 might be the luggage department in all stores. Store employees at any location can dial 4321 and get the luggage department in the store.

If you migrate to a single distributed network, store employees can no longer dial 4321 to reach the local luggage department. The system cannot correctly analyze the digits and route the call to the correct store. Store employees now have to dial a complete telephone extension to reach the luggage department in the store.

This problem is solved with the Multi-Location Dial Plan feature. With the Multi-Location Dial Plan feature, Communication Manager adds the location prefix digits to the front of the dialed number. The software then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters screen.

With the Multi-Location Dial Plan feature, a user can dial a shortened version of an extension instead of having to dial a complete extension. For example, the store employee can continue to dial 4321 instead of having to dial 765-4321 to reach the luggage department.

Note:
Beginning with Communication Manager Release 5.0, you can use different length short number extensions for different locations.

Without the Multi-Location Dial Plan feature in a single distributed network, a call that is routed to an attendant might not terminate at the local attendant. For example, if a school district migrates to a single distributed network, dialing the attendant access code may not route the call to the local school attendant. With the Multi-Location Dial Plan feature, the system can route an attendant-seeking call to a local centralized answering point (LCAP), such as a local station or an attendant console. However, the normal attendant features like system attendant queues are not available in such instances.

The Multi-Location Dial Plan feature provides dial plan capabilities that are similar to those of QSIG networks or DCS networks. These capabilities include:

- Extension uniqueness
- Announcements for each location

- Local attendant access
- Local Automatic Route Selection (ARS) code administration

On Linux platforms only, the Multi-Location Dial Plan feature also enhances the dial plan and the Uniform Dial Plan Table screen so that users can:

- Dial a shortened version of a telephone extension, and reach the same destination as before the migration
- Dial and reach a centralized local answering point
- Dial a local attendant Feature Access Code (FAC) or ARS FAC, and access the same feature as before the migration

On Linux platforms only, you can also play administered announcements in a language that is based on location.

Detailed description of Multi-Location Dial Plan

This section provides a detailed description of the Multi-Location Dial Plan feature.

With the Multi-Location Dial Plan feature, users in a single distributed network can dial a local extension to reach a number in their area. Before this can happen, the administer must first retranslate their dial plan and extensions. This feature inserts leading digits from the calling number to the called number for intralocation dialing.

This feature also provides a local centralized answering point for attendants. Finally, with this feature, you can administer multiple Feature Access Codes for ARS and for attendants.

Location prefix

A new value is available in the **Insert Digits** field on the Uniform Dial Plan Table screen. This new value takes the location prefix of the caller from the Locations screen. The software adds the location prefix to the front of the called number. The software then analyzes the entire dialed string, and routes the call based on the administration on the Dial Plan Parameters screen.

- Non-IP telephones and trunks inherit the location number of the cabinet, the remote office, or the media gateway to which they are connected.
- IP telephones and trunks obtain their location number indirectly.
  - On the Network Region screen, you administer a location number that applies to all telephones in that IP region. If a location field is left blank on the Network Region screen, an IP telephone obtains its location from the location of the cabinet that contains the C-LAN board.

— IP trunks obtain the location from the location of their associated signaling group.

Either direct administration, which is only possible for remote office signaling groups, or the ways described for IP telephones, determines the location.

If the location prefix is not administered correctly, the software does not route calls correctly. A location prefix is not administered correctly if:

- You administer the prefix with incorrect digits
- The entry on the Uniform Dial Plan Table screen does not match the length of the location prefix

Feature Access Codes

- The software uses the **Auto Route Selection (ARS) - Access Code** fields on the Feature Access Code (FAC) screen when no value exists in the **ARS FAC** field on the Locations screen. If a value exists in the **ARS FAC** field on the Locations screen, the software uses that location **ARS FAC**. The **Auto Route Selection (ARS) - Access Code** fields on the Feature Access Code (FAC) screen are ignored.

  If you use the **ARS FAC** field on the Locations screen, you lose the ability to administer two ARS codes on the Feature Access Code (FAC) screen.

  The location **ARS FAC** is accessible only for calling numbers at locations that are administered with that **ARS FAC**. The software denies any attempt to use an **ARS FAC** at a location for which the FAC is not valid.

- The **Attendant Access Code** field on the Feature Access Code (FAC) screen has the same characteristics as the **attd** call type on the Dial Plan Analysis Table screen.

  You can administer only one attendant code. You can administer the attendant code either on the Dial Plan Analysis Table screen, or on the Feature Access Code (FAC) screen. You cannot administer the attendant code on both screens.

  If you want to:

  — Administer an attendant access code for different locations, use the **Attendant Access Code** field on the Feature Access Code (FAC) screen.

  — Use one attendant code for all locations, administer the code as **attd** in the **Call Type** field on the Dial Plan Analysis Table screen.

    You cannot reuse the value that you use for the **attd** call type for any FACs. Nor can you reuse the value for the **ARS FAC** or **Attd FAC** on the Locations screen.

  Attd FAC, the attendant code on the Locations screen, is accessible only for calling numbers at locations that are administered with that attendant access code. The software denies any attempt to use an attendant code at a location for which the code is not valid.

- Only one attendant or ARS access code is valid for a location. The global ARS access code and the attendant access code, and the dialed string for the attendant call type, are valid for a location only if:
  - A local ARS access code does not exist, or
  - An attendant access code does not exist

Announcements

With multiple QSIG or DCS networks, multiple switches can handle announcements in multiple languages. Without the Multi-Location Dial Plan feature in a single distributed network, the software cannot play announcements in multiple languages.

With the Multi-Location Dial Plan feature, announcement extensions are stored as digit strings. The software routes these digit strings through Uniform Dial Plan (UDP) processing. This processing is similar to dialing a telephone extension. When the software dials a shortened extension for an announcement, the software prepends the location prefix onto the extension. With both the location prefix and the extension, the software can play the announcement to the caller in the proper language.

Invalid announcements

The software provides intercept treatment if the following announcements are invalid:

- DID/Tie/Intercept
- Controlled Outward Restriction Intercept Treatment
- Controlled Termination Restriction (Do Not Disturb)
- Controlled Station to Station Restriction
- Controlled Toll Restriction Intercept Treatment
- Invalid Number Dialed Intercept Treatment

The software skips and does not play the following announcements if the announcements are invalid:

- Analog Busy Auto Callback
- Direct Agent Announcement Extension
- Hospitality

The treatment for an announcement that is invalid during vector processing is the same as if the announcement did not exist. Call processing continues and does not wait. Any previous feedback that precedes the announcement continues.

- An announcement step continues at the next step.

- A wait step that references an announcement continues after any specified wait treatment expires.
- A disconnect step disconnects immediately.
- A collect step continues at the next step.

If the VDN of Origin Announcement (VOA) does not exist, vector processing bypasses the VOA, and delivers the call to the agent.

Maintenance

When you migrate to a single distributed network, you must re-administer your dial plan if you want to maintain extension uniqueness. You can administer the UDP so that users can dial a local extension at an individual location the same as before the migration.

If you administer local ARS FACs on the Locations screen, you lose the ability to administer two ARS codes. The ability to administer two ARS codes is currently provided only on the Feature Access Code (FAC) screen.

Administering Multi-Location Dial Plan

The following steps are part of the administration process for the Multi-Location Dial Plan feature:

- Changing extensions
- Prepending numbers to the dialed string
- Setting up announcements
- Setting up a local centralized answering point
- Setting up multiple Feature Access Codes for attendants
- Setting up multiple Feature Access Codes for ARS

This section describes:

- Any prerequisites for administering the Multi-Location Dial Plan feature
- The screens that you use to administer the Multi-Location Dial Plan feature
- Complete administration procedures for the Multi-Location Dial Plan feature

Prerequisites for administering Multi-Location Dial Plan

You must complete the following actions before you can administer the Multi-Location Dial Plan feature:

- On the Optional Features screen, ensure that the **Multiple Locations** field is set to **y**. If this field is set to **n**, your system is not enabled for the Multi-Location Dial Plan feature. Contact your Avaya representative for assistance.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- On the Daylight Savings Rules screen, ensure that rules for daylight savings time are administered.

  To view the Daylight Savings Rules screen, type **`change daylight-savings-rules`**. Press **Enter**.

  For a complete description of the many Optional Features screens, and the Daylight Savings Rules screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Screens for administering Multi-Location Dial Plan

Screen name	Purpose	Fields
Optional Features	Ensure that the multiple locations feature is enabled.	**Multiple Locations**
Daylight Savings Rules	Ensure that rules for daylight savings time are administered.	All
Locations	• Set up a FAC to access ARS for a location. • Set up a FAC to access an attendant for a location. • Include the prefix for the specific location.	• **ARS FAC** • **Attd FAC** • **Prefix**
Change Station Extension	Change multiple extensions in the software from one extension to another simultaneously.	All
Uniform Dial Plan Table	Set up your dial plan.	All

Changing extensions

You can change multiple extensions in the software from one extension to another, simultaneously.

To change multiple extensions simultaneously:

1. Type **change extension-station** *n*, where *n* is the extension number that you want to change. Press **Enter**.

   The system displays the Change Station Extension screen (Figure 315: Change Station Extension screen on page 1265).

   CAUTION:
   The Change Station Extension screen does not change the emergency location extension that is administered within the system. You cannot use this screen to change an extension that is administered as an emergency location extension on either the Station screen or the IP Address Mapping screen.

Figure 315: Change Station Extension screen

```
change extension-station xxxxxxx                                Page 1 of 1
                              CHANGE STATION EXTENSION

          Station Name: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx     Port: xxxxxx

                           FROM EXTENSION           TO EXTENSION
                           --------------           ------------
                      Station: xxx-xxxx               xxx-xxxx
                Message Lamp: xxx-xxxx                xxx-xxxx
       Emergency Location Ext.: xxx-xxxx              xxx-xxxx
IP Parameter Emergency Location: xxx-xxxx             See IP-Network Map Form
```

2. In the **TO EXTENSION** fields:
   a. Type a new extension that you want the current extension changed to.
   b. Type a new extension for the message lamp extension.
   c. Type a new extension for the **emergency location ext.** field.
   d. In the **IP Parameter Emergency Location** field, the system displays the words **See IP-Network Map Form**.

      You can change the **IP Parameter Emergency Location** field only on the IP Address Mapping screen. Use the **change ip-network-map** command.
3. Press **Enter** to save your changes.

Function

When you complete and submit the Change Station Extension screen, all administration that was associated with the previous extension is now associated with the new extensions. This administration includes any references used in a vector, in coverage, and elsewhere in the system. Once you change an extension, the software removes all references to the previous extension.

If you change an extension that is also administered on an adjunct, you must also change the extension on the adjunct. Examples of adjuncts include voice mail and an Adjunct-Switch Application Interface (ASAI) link.

Exceptions

- The **change extension-station *n*** command does not change the administration that is associated with call forwarding digits and abbreviated dialing buttons on the current extension.
- To change a forwarded extension that is administered as a button, do not use the **change extension-station *n*** command. The extension for the call forwarded button is stored as digits rather than as a UID. Avaya recommends that you use the **list usage** command before you change any extensions.
- The **change extension-station *n*** command does not update the **ISDN BRI SPID** field for BRI telephones. To update this field, you must make manual changes on both the switch and the telephone.

Audits

- If you try to change an extension that is administered on the same switch as an **emergency location extension** on the Station screen or on the IP Address Mapping screen, the system displays the following warning message:

  Extension exists as Emergency Location. Continue?

  Click **yes** to process the change. Click **no** to stop the process.
- The **change extension-station *n*** command is be denied under the following conditions:
  - If the extension being changed is active on a call
  - If the administrator is accessing the extension

- If you attempt to change an extension that is administered on the same system as a **media complex extension** on the Station screen, the extension cannot be changed to a 6-digit or 7-digit number. The **media complex extension** field on the Station screen does not support 6-digit or 7-digit numbers.

  For example, extension 50002 is an IP (H.323) telephone extension. Extension 50002 is administered on extension 51234 as the media complex. You cannot use the **change extension-station *n*** command to change extension 50002 to 7050002 because the software does not support a 7-digit media complex number. You can, however, use the command to change 50002 to 52222, because 52222 is a 5-digit extension.

Prepending numbers to the dialed string

The software allows a new value in the **Insert Digits** field in the Uniform Dial Plan Table screen. The value is **L***x*. In the value **L***x*, *x* indicates a number from 1 to 5. The number *x* must match the number of digits in the **Prefix** field on the Locations screen. For example, if the **Prefix** field on the Locations screen contains three digits, assign the value **L3**.

When you use the value **L***x* in the Uniform Dial Plan Table screen, the software takes the value in the **Prefix** field from the Locations screen, and prepends the number of digits to the dialed string.

To prepend numbers to the dialed string:

1. Type **uniform-dialplan *n***, where ***n*** is the number of the dial plan. Press **Enter**.

   The system displays the Uniform Dial Plan Table screen (Figure 316: Uniform Dial Plan Table screen on page 1268).

Figure 316: Uniform Dial Plan Table screen

```
change uniform-dialplan 3                                        Page 1 of 2
                            UNIFORM DIAL PLAN TABLE

                                                                 Percent Full: 0

  Matching          Insert          Node Matching         Insert          Node
  Pattern   Len Del Digits Net Conv Num  Pattern  Len Del Digits Net Conv Num
  3          3   0  L3     ext  y                                    n
  5          5   1  005    aar  y                                    n
  538        7   0         aar  y                                    n
  6          5   1  006    aar  y                                    n
  852        7   0         aar  y                                    n
                            n                                       n
                            n                                       n
                            n                                       n
                            n                                       n
                            n                                       n
                            n                                       n
                            n                                       n
                            n                                       n
```

2. In the **Insert Digits** field, type **L** and a number from 1 to 5. The number that you type must equal the number of digits in the **Prefix** field on the Locations screen. This number is the number of digits that the software prepends to the dialed telephone number.

   For more information on the Uniform Dial Plan Table screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

3. Press **Enter** to save your changes.

Setting up announcements

In addition to the shortened extensions, you must also administer announcements. If your organization has multiple locations with announcements in multiple languages, you must administer the announcement for each location, even if many of the announcements are identical.

For example, if your organization has 100 locations, announcements in 90 locations are in English. In the remaining 10 locations, announcements are in non-English languages. You must administer announcements in all 100 locations, even if 90 of the locations use the same English announcements.

For some announcements, such as the **DID/Tie/Intercept** announcement, you can administer only a single announcement. This restriction can create a problem in a single distributed network. For example, an S8700 Media Server might support multiple countries, and therefore require that announcements play in the language of the country. This example poses a problem because you can only administer a single announcement.

To accommodate several announcements that share a single administered field, use the Multi-Location Dial Plan feature. With the Multi-Location Dial Plan feature, the announcement that plays is based upon the calling number, and the **Location Prefix** field on the Locations screen.

For example, 4567 is the extension administered in the **DID/Tie/ISDN Intercept Announcement** field on the System Features screen. You can record multiple announcements for extension *xxx*-4567:

- 420-4567 in English
- 813-4567 in German
- 964-4567 in French
- 371-4567 in Spanish
- 628-4567 in a user-defined language

You must administer all announcements - 420-4567 in English, 813-4567 in German, 964-4567 in French, 371-4567 in Spanish, and 628-4567 in the user-defined language. When a person calls and is about to hear announcement 4567, the system inserts the prefix digits based on the location of the caller. The system then plays announcement 4567 in the proper language.

Setting up a local centralized answering point

With the Multi-Location Dial Plan feature, you can use vector routing or hunt groups to set up a local centralized answering point (LCAP). The LCAP gives users access to a local attendant.

With vector routing, you can administer a VDN with extension "0" with a vector "route-to" step for a shorter extension. You then administer the Uniform Dialing Plan screen with an entry for the shorter extension in the vector step. The purpose is to prepend digits from the calling party number. The system routes the call to the extension that you designate as the LCAP.

You can also use a hunt group to set up an LCAP. You administer the Uniform Dialing Plan screen so that the shorter extension for the hunt group prepends digits for the calling party number. One of the members of a local hunt group can be designated as the LCAP.

Note that if you use an LCAP, you cannot also use local access codes. LCAPs and multiple Feature Access Codes for the attendant are mutually exclusive.

Setting up multiple Feature Access Codes for attendants

Without the Multi-Location Dial Plan feature, you can administer only one attendant Feature Access Code (FAC) on the Dial Plan Analysis Table screen. With this feature, you can administer multiple attendant FACs. The Multi-Location Dial Plan feature adds the administration of the attendant dial access code to the Feature Access Code (FAC) screen. The **call type** is **attd**. This change allows different locations to share the value that is used for the attendant access.

For example, you might enter the access code **9** for ARS on the Feature Access Code (FAC) screen. You might then enter the attendant access code on a Locations screen as **8**. When a user dials **8** from that location, the software routes the call to an attendant.

Only one attendant group can exist in the software at a time.

Setting up multiple Feature Access Codes for ARS

Without the Multi-Location Dial Plan feature, you can administer only two attendant FACs on the Feature Access Code (FAC) screen. With this feature, you can administer multiple ARS FACs. You can either use the global ARS codes, or provide ARS codes for a location.

For example, you might enter the access code **9** for ARS on the Feature Access Code (FAC) screen. You might then enter the ARS access code on a Locations screen as **1**. When a user dials **1** from that location, the system routes the call with ARS. A user at that location cannot dial **9** to reach ARS.

Interactions for Multi-Location Dial Plan

This section provides information about how the Multi-Location Dial Plan feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of the Multi-Location Dial Plan in any feature configuration.

- Attendant

  This feature allows you to administer multiple attendant codes. This feature does not allow you to administer multiple attendant groups. Only one attendant group is allowed, unless you have Attendant Partitioning. This feature provides a way to support multiple local centralized answering points (LCAPs). The LCAPs do not use attendant groups.

- Attendant Vectoring

  Attendant Vectoring, if enabled, takes precedence over any local attendant codes that are administered. The software uses call vectors to process calls to an attendant. Such calls are:

- Local attendant codes
- The attendant code on the Dial Plan Analysis Table screen
- The attendant access code on the Feature Access Code (FAC) screen

- Automatic Circuit Assurance (ACA)

  The **ACA Referral Destination** field on the System Features Parameters screen requires that an attendant group exists. This field also requires either:

  - The **attd** administration on the Dial Plan Analysis Table screen, or
  - Administration of the **attendant access code** on the Feature Access Code (FAC) screen

- Automatic Wakeup

  If a telephone has Automatic Wakeup requests pending when you run the **change extension-station** command, the system cancels the wakeup requests.

- Call Forwarding

  Any call forwarding information that is stored with an extension is lost when you use the **change extension-station** command. If the telephone that you change with the **change extension-station** command is a forwarded-to telephone, you must manually update the extension that uses the forwarded-to extension. If you do not manually update the extension, the system does not forward calls correctly.

- Call Park

  This feature does not support common shared extensions to park calls. Since common shared extensions are not assigned to physical telephones, the range of common shared extensions can be shared in all locations.

- Crisis Alert

  The **change extension-station** command does not update the **Originating Extension** field on the Crisis Alert System Parameters screen. You must manually update the **Originating Extension** field if you change the **originating extension** field.

- Leave Word Calling (LWC)

  The **Stations with System-wide Retrieval Permission for the Leave Word Calling Parameters** field on the System Features Parameters screen requires that an attendant group exists. This field also requires either:

  - The **attd** administration on The Dial Plan Analysis Table screen, or
  - Administration of the **Attendant Access Code** on the Feature Access Code (FAC) screen

- Local Survivable Processor (LSP)

  If you run the **change extension-station** command on the controller, but do not also save the translations to the LSP, the two system translations might not be synchronized.

  Use either of these following commands to save the translations to the LSP:

- The **save trans lsp** command locally saves the translations, and performs a filesync operation to all registered LSPs.
- The **save trans lsp *n*** command, where ***n*** is the IP address of a specific LSP, locally saves the translations, and performs a filesync operation to the specified LSP.

- Night Service

  This feature does not support location-based Night Service. Therefore, you might want to restrict calls to attendants who are local to the calling party. The attendant most likely speaks the same language as the caller. At night, instead of putting the entire system into Night Service, you might want an attendant to put only one location into Night Service.

  To accomplish this, you can use hunt groups as attendant queues. Each hunt group can be put into Night Service separately, and have its own Night Service destination. You can also administer the Night Service destination by tenant, trunk group, and trunk group number.

- Security Violations Notification

  The referral destination fields on the Security-Related System Parameters screen requires that an attendant group exists. This field also requires either:

  - The **attd** administration on the Dial Plan Analysis Table screen, or
  - Administration of the **attendant access code** on the Feature Access Code (FAC) screen

  The referral destination fields are:

  - **SVN Login Violation Notification Enabled**
  - **SVN Remote Access Violation Notification Enabled**
  - **SVN Authorization Code Violation Notification Enabled**
  - **SVN Station Security Code Violation Enabled**

- Station Hunting

  Changing a telephone extension with the **change extension-station** command maintains the hunting chain.

- Survivable Remote EPN/WAN Spare Processor

  If you run the **change extension-station** command in a configuration where a survivable remote processor exists, you must also run the command on the survivable processor. If you do not, the extensions that you changed on the server do not exist on the survivable remote when the remote processor takes control.

- Uniform dial plan (UDP)

  The **change extension-station** command does not update extensions that are in the Uniform Dial Plan Table screen. Avaya supports external system management tools that handles changes to the UDP table.

Music-on-Hold

Use the Music-on-Hold feature to automatically provide music, silence, or tone to a caller who:

- Is on hold
- Is transferred
- Is parked
- Waits in a queue

Detailed description of Music-on-Hold

This section provides a detailed description of the Music-on-Hold feature.

Use the Music-on-Hold feature to automatically provide music, silence, or tone to a caller. Table 82: Music, silence, and tone options on page 1273 shows the audio options that you can provide to a user.

Table 82: Music, silence, and tone options

Caller status	Music	Silence	Tone
On hold	Yes	No	Yes
On a trunk call that is being transferred	Yes	Yes	No
Parked	Yes	No	Yes
Waits in a queue	Yes	No	Yes

Note:

If you use equipment that rebroadcasts music or other copyrighted materials, you might be required to obtain a copyright license from, or pay fees to, a third party such as the American Society of Composers, Artists, and Producers (ASCAP), or Broadcast Music Incorporated (BMI).

Administering Music-on-Hold

The following steps are part of the administration process for the Music-on-Hold feature:

- Assigning music tones, music ports, and music for transferred trunks
- Defining a Class of Restriction for Music-on-Hold
- Connecting a music source to the server
- Assigning a source of music to a port

This section describes:

- Any prerequisites for administering the Music-on-Hold feature
- The screens that you use to administer the Music-on-Hold feature
- Complete administration procedures for the Music-on-Hold feature

Prerequisites for administering Music-on-Hold

You must complete the following actions before you can administer the Music-on-Hold feature:

- None

Screens for administering Music-on-Hold

Screen name	Purpose	Fields
Feature-Related System Parameters	Assign music tones, music ports, and music for transferred trunks.	• **Music/Tone On Hold** • **Music Port** • **Music (or Silence) on Transferred Trunk Calls**
Music Sources	Assign a music source to a port.	All
CPE Trunk Group	Connect a music source to the server.	All
Class of Restriction	Define a Class of Restriction (COR) for Music-on-Hold.	**Hear System Music on Hold**

Assigning music tones, music ports, and music for transferred trunks

To assign music tones, music ports, and music for transferred trunks:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen (Figure 317: Feature-Related System Parameters screen on page 1275).

Figure 317: Feature-Related System Parameters screen

```
change system-parameters features                                    page 1
                         FEATURE-RELATED SYSTEM PARAMETERS
                            Self Station Display Enabled? n
                                 Trunk-to-Trunk Transfer? none
 Automatic Callback - No Answer Timeout Interval (rings): 4_
                     Call Park Timeout Interval (minutes): 10
     Off-Premises Tone Detect Timeout Interval (seconds): 20_
                               AAR/ARS Dial Tone Required? y
                        Music/Tone On Hold: music__ Type: Group 1_
           Music (or Silence) On Transferred Trunk Calls: all
                    DID/Tie/ISDN/SIP Intercept Treatment: attd

 Internal Auto-Answer of Attd-Extended/Transferred Calls? y
               Automatic Circuit Assurance (ACA) Enabled? y
                                     ACA Referral Calls: local
                                ACA Referral Destination: ________
            ACA Short Holding Time Originating Extension: ______
             ACA Long Holding Time Originating Extension: ______
          Abbreviated Dial Programming by Assigned Lists:
     Auto Abbreviated/Delayed Transition Interval(rings):
                  Protocol for Caller ID Analog Terminals: Bellcore
 Display Calling Number for Room to Room Caller ID Calls?
```

2. In the **Music/Tone on Hold** field, perform one of the following actions:
   - If you want a caller who is on hold to hear music, type **music**.
   - If you want a caller who is on hold to hear a tone, type **tone**.
   - If you want a caller who is on hold to hear neither music nor a tone, type **none**.

   If the **Tenant Partitioning** field on the Optional Features screen is set to **y**, you cannot administer the **Music/Tone on Hold** field. If the **Tenant Partitioning** field on the Optional Features screen set to **y**, you must use the Music Sources screen to assign music to a port.

   When you enter **music**, the **Type** field appears. Type one of the following values:

- Type **ext** and the corresponding extension number of the music-on-hold.
- Type **group** and the corresponding music-on-hold group number.
- Type **port** and the corresponding port location of the music-on-hold. Table 83: Port field values on page 1276 shows how to construct a port number. You must specify a port on a TN763 Auxiliary Trunk circuit pack, or any supported analog line circuit pack.

For more information on music-on-hold groups see Locally Sourced Announcements and Music.

Table 83: Port field values

Characters	Description	Value
1-2	Cabinet number	**01** through **44** (For DEFINITY R configurations) **01** through **03** (For DEFINITY SI configurations) **01** through **64** (For IP-PNC)
3	Carrier	**A** through **E**
4-5	Slot number	**0** through **20**
6-7	Circuit number	**01** through **04** (x.25 circuit pack) **01** through **31** (DEFINITY SI, IP-PNC (tdm, pdm) configurations) **01** through **16** (ppp for IP-PNC) **01** through **08** (system-port for IP-PNC) **17/33** (ethernet on IP-PNC)
x	Administration without Hardware	If the **Secondary data module?** field, is set to **n**, you can type **x** in the **Port** field. A **Port** field set to **x** indicates that no hardware is associated with the port assignment.

3. In the **Music (or Silence) On Transferred Trunk Calls** field, perform one of the following actions:
   - If you want all transferred trunk calls to receive music until the call is answered, type **all**.
   - If you want a caller on the trunk call to hear music while the caller waits to be transferred, or ringback tone as soon as the transfer is complete, type **no**.

     The caller on the trunk call hears neither music nor a tone if Music-on-Hold is not administered.
   - If you want a trunk call that transfers to a station, and then waits at the station, to hear music, if music is administered, type **call-wait**.

     All other transferred trunk calls receive the ringback tone.
4. Press **Enter** to save your changes.

Defining a Class of Restriction for Music-on-Hold

To define a Class of Restriction for Music-on-Hold:

1. Type **change cor *n***, where n is the Class of Restriction (COR) to which you want to add Music-on-Hold. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 318: Class of Restriction on page 1277).

Figure 318: Class of Restriction

```
change cor 1                                                Page   1 of 4
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 7                                APLT? y
  Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n            Called Party Restriction: none
        Time of Day Chart: 2       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? y                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                         Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

2. In the Hear System Music on Hold field, perform one of the following actions:
   - If you want Music-on-Hold to be activate at a telephone, type **y**.
   - If you do not want Music-on-Hold to be activate at a telephone, type **n**.
3. Press **Enter** to save your changes.

Connecting a music source to the server

To connect a music source to the server:

1. Type **add trunk-group *next***. Press **Enter**.

   You use the customer-premises equipment (CPE) trunks to connect a music source to the server.

   For more information on how to administer trunk groups, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Assigning a source of music to a port

To assign the sources of music to a port:

1. Type **change music-sources**. Press **Enter**.

   The system displays the Music Sources screen (Figure 319: Music Sources screen on page 1278).

Figure 319: Music Sources screen

```
change music-sources                                          Page 1 of X
                              Music Sources
            Source    Type         Source             Description

              1      music Type:  port 01A1003       Easy listening
              2      tone                            Tone-on-Hold
              3      music Type:  group 49           Rock
              4      none
              5      none
              6      none
              7      music Type:  extenstion 20003   Oldies
              8      none
              9      none
             10      none
             11      music Type:  group 50           Classical
             12      none
             13      none
             14      none
             15      none
```

2. In the **Type** field, perform one of the following actions:
   - If you want the user to hear music, type **music**.

- If you want the user to hear the tone-on-hold tone, type **tone**.

  You can specify **tone** for only one music source on the Music Sources screen.

- If you want the user to hear neither music nor a tone, type **none**.

3. In the **Source** field, type the auxiliary trunk address, the analog port address, the group address, or the extension address of the music source. You cannot enter duplicate addresses in the **Source** field.

   The system displays the **Source** field only if you typed **music** in the **Type** field.

   Table 83: Port field values on page 1276 shows you how to construct a port number.

4. In the **Description** field, type a maximum of 20 characters that describe the source of the music.

   The system displays the **Description** field, only if you typed **music** or **tone** in the **Type** field.

5. Press **Enter** to save your changes.

Reports for Music-on-Hold

The following reports provide information about the Music-on-Hold feature:

- None

Considerations for Music-on-Hold

This section provides information about how the Music-on-Hold feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Music-on-Hold under all conditions. The following considerations apply to Music-on-Hold:

- If the **Tenant Partitioning** field on the Optional Features screen is set to **y**, you cannot administer the **Music/Tone on Hold** field on the Feature-Related System Parameters screen. If the **Tenant Partitioning** field on the Optional Features screen set to **y,** you must use the Music Sources screen to assign music to a port.
- Any number of calls can simultaneously connect to music.
- The system does not provide music to callers, in a multicaller connection, who are in a queue, on hold, or parked.

Interactions for Music-on-Hold

This section provides information about how the Music-on-Hold feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Music-on-Hold in any feature configuration.

- Automatic Call Distribution (ACD)

  If you administer Music-on-Hold to provide music, the system provides the music after the ACD split delayed announcement.

- Data Privacy and Data Restriction

  If a user or an attendant places a call that has either Data Privacy or Data Restriction activated on hold, the system withholds Music-on-Hold. The system withholds Music-on-Hold to prevent transmission of a musical tone that a connected data service might falsely interpret as a data transmission.

- Hunting

  If you administer Music-on-Hold to provide music, the system provides the music after the Direct Departmental Calling (DDC) group or the uniform call distribution (UCD) group delayed announcement.

Night Service

Use the Night Service feature to direct incoming calls to other answering points at night.

Detailed description of Night Service

This section provides a detailed description of the Night Service feature.

Communication Manager provides the following Night Service capabilities:

- Hunt Group Night Service
- Night Console Service
- Night Station Service
- Trunk Answer from Any Station
- Trunk Group Night Service

Hunt Group Night Service

With Hunt Group Night Service, an attendant or a split supervisor can assign a hunt group or a split to Night Service mode. All calls for the hunt group then are redirected to the hunt group's designated Night Service Extension (NSE). When a user activates Hunt Group Night Service, the associated button lamp lights.

Night Console Service

Night Console Service directs all calls for primary and daytime attendant consoles to a night console. When a user activates Night Console Service, the Night Service button for each attendant lights, and all attendant-seeking calls (and calls that are waiting) in the queue, are directed to the night console.

To activate and deactivate this feature, the attendant usually presses the **Night** button on the principal attendant console or a designated console.

Night Station Service

Night Station Service directs incoming calls for the attendant to designated extensions. To activate Night Station Service, attendants press the **Night** button on the principle console, if there is not an active night console. If the night station is busy, calls including emergency attendant calls, receive busy tone. Calls do not queue for the attendant.

When Night Station Service is active, the system routes the incoming calls to the attendant as follows:

- **Direct Inward Dialing (DID)** Listed Directory Number (**LDN)** calls are routed to a designated **DID**-**LDN** night extension.
- Internal calls route to the **DID**-**LDN** night extension, unless you administer the system so only **DID**-**LDN** calls can route to the **LDN** night extension.
- Non-DID calls are routed to the night destination that you specify for the trunk group or for the individual trunk. If you do not specify a night destination, the calls route to the **DID-LDN** night extension.

You can assign a unique extension as the night destination for each incoming central-office, foreign-exchange, or 800-Service trunk group. Both the extension assigned as a trunk group's night destination and the **DID**-**LDN** night extension can be phones or answering groups (such as **DDC** group, **UCD** group, or terminating extension group (**TEG)**.

Trunk Answer from Any Station

With Trunk Answer from Any Station (TAAS), telephone users can answer all incoming calls to the attendant when the attendant is not on duty, and when other telephones are not designated to answer the calls. The incoming call activates a gong, a bell, or a chime and a telephone user dials an access code to answer the call.

Users can activate TAAS if each of the following conditions is met:

- The attendant pressed the **Night** button on the primary console or a user (if Communication Manager has no attendant administered) pressed the Night Service button on the designated Night Service phone.
- A night console is not assigned or is not operational.
- Night Station Service is not active.

Trunk Group Night Service

WIth Trunk Group Night Service, an attendant or a designated Night Service telephone user can assign one or all trunk groups to Night Service mode. When a user activates Night Service, trunk groups that are assigned a Trunk Group Night Service termination change to Individual Trunk Night Service mode. The system redirects the calls that come into the trunk group to the group's designated **NSE**. Incoming calls on trunk groups that are not assigned to Trunk Group Night Service are queued in the attendant queue. If the call remains unanswered during the Night Service Disconnect Timer interval, the incoming trunk disconnects.

A user can also assign all the trunk groups to the Night Service mode at the same time. Then all the trunk groups are in the System Night Service mode. The system redirects any incoming calls made on the trunk groups to their designated **NSE for the trunk group**. To assign all the trunk groups to System Night Service, the user presses the System Night Service button on the principal attendant console or the Night Service button on a designated phone. You can assign a Night Service button to only one telephone.

To activate Trunk Group Night Service, you press the individual Trunk Night Service buttons on the attendant console or on a telephone. You can assign Trunk Night Service buttons on more than one telephone.

Administering Night Service

The following steps are part of the administration process for the Night Service feature:

- Setting up night station service to voice mail
- Setting up Night Console Service
- Setting up Night Station Service
- Setting up Trunk Answer from Any Station
- Setting up external alerting
- Setting up external alerting Night Service
- Setting up Night Service for trunk groups
- Setting up Night Service for hunt groups

This section describes:

- Any prerequisites for administering the Night Service feature
- The screens that you use to administer the Night Service feature
- Complete administration procedures for the Night Service feature

Screens for administering Night Service

Screen name	Purpose	Fields
Hunt Group	Set Night Station Service to voice mail.	**Group Number**
Listed Directory Number		**Night Destination**
Console Parameters		**DID-LDN Only to LDN Night Ext**
Attendant Console	Set up Night Console Service.	**Console Type**
Listed Directory Numbers	Set up Night Station Service.	**Night Destination**
Console Parameters		**DID-LDN Only to LDN Night Ext**
Feature Access Codes	Set up Trunk Answer from Any Station (TAAS)	**Trunk Answer Any Station Access Code**
Console Parameters	Set up external alerting.	**EXT Alert Port (TAAS)**
Listed Directory Numbers	Set up external alerting night service.	**Night Destination**
Console Parameters		• **EXT Alert Port (TAAS)** • **DID-LDN to Night Ext.**
Trunk Group	Set up Trunk Group Night Service.	**Night Service**
Hunt Group	Set up Night Service for hunt groups.	**Night Service Destination**

Setting up night station service to voice mail

To set up a night station service to voice mail:

1. Type **`add hunt-group next`**. Press **Enter**.

   The system displays the Hunt Group screen (Figure 320: Hunt Group screen on page 1285).

   The **Group Number** field fills in automatically with the next hunt group number.

Figure 320: Hunt Group screen

```
                                                              Page 1 of X
                                  HUNT GROUP
        Group Name: ldn nights
      Group Number: 5              Group Extension: 51002___ Group Type:
   MM Early Answer? _                            Skill? _            ACD?
             Queue? _                          Vector? _            AAS?
_     Security Code: ____                                           COR:
  ISDN Caller Disp: _________                                      TN: _

                  Measured: _________            Supervisor: Extension: _______
      Controlling Adjunct: ____
   Multiple Call Handling: ___________
                Objective: ____

            Queue Length: ___
Calls Warning Threshold: ___             Calls Warning Port: __
 Time Warning Threshold: ___              Time Warning Port: __

                    Redirect on No Answer (rings): _  Redirect to VDN: _
               Forced Entry of Stroke Counts or Call Work Codes? _
```

2. In the **Group Name** field, type the name of the group.

   This example uses **ldn nights** in the **Group Name** field. There can be no members in this hunt group.

3. Press **Enter** to save your changes.

Note:
If you are using tenant partitioning, the command for the next step is **change tenant *n***. If you are using tenant partitioning, the **Night Destination** field does not appear on the Listed Directory Numbers screen. Instead, the **Night Destination** field is on the Tenant screen.

4. Type **change listed-directory-numbers**. Press **Enter**.

   The system displays the Listed Directory Numbers screen (Figure 321: Listed Directory Numbers screen on page 1286).

Figure 321: Listed Directory Numbers screen

```
                                                              Page 1 of 2

                      LISTED DIRECTORY NUMBERS

                      Night Destination: 51002

       Ext      Name                            TN
 1: 51001     Attendant                         1
 2:                                             1
 3:                                             1
 4:                                             1
 5:                                             1
 6:                                             1
 7:                                             1
 8:                                             1
 9:                                             1
10:                                             1
```

5. In the **Night Destination** field, add the night destination on the listed directory phone.

   This example uses **51002**.

6. Press **Enter** to save your changes.

7. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 322: Console Parameters screen on page 1286).

Figure 322: Console Parameters screen

```
                          CONSOLE PARAMETERS
    Attendant Group Name: 27 character name  OPERATOR
                     COS: 1                                  COR: 1
  Calls in Queue Warning: 5                    Attendant Lockout? y
   Ext Alert Port (TAAS):
                     CAS: none
         SAC Notification? n              Night Service Act. Ext.: 1234
             IAS (Branch)? n              IAS Tie Trunk Group No.:
    IAS Att. Access Code:                   Alternate FRL Station:
          Backup Alerting? n        DID-LDN Only to LDN Night Ext? n
```

8. In the **DID-LDN Only to LDN Night Ext** field, type **n**.

9. Press **Enter** to save your changes.

10. From a phone with console permissions, dial the call forwarding Feature Access Code, then the hunt group's extension, followed by the main number of CM Messaging.

    In this example, dial 51002.

    Note:
    You should receive a confirmation tone that consists of three beeps. This step is very important because calls to the LDN night service extension do not follow coverage.

11. In your voice mail, build the automated attendant with the extension of the Listed Directory Number (LDN), not the hunt group.

    The originally dialed number was the LDN, which is the number Communication Manager passes to the voice mail application. In the case of the CM Messaging voice mail systems, you can use the Auto Attendant routing table to send the calls to a common automated attendant mailbox.

Setting up Night Console Service

To set up night console service:

1. Type **`change attendant n`**, where ***n*** is the number of the attendant console. Press **Enter**.

   The system displays the Attendant Console screen (Figure 323: Attendant Console screen on page 1288).

Figure 323: Attendant Console screen

```
                              ATTENDANT CONSOLE 2

        Type: console           Name: 27 character attd cons name
   Extension: 1000             Group: 1                Auto Answer: none
Console Type: principal           TN: 1                Data Module? n
        Port: 01C1106             COR: 1          Disp Client Redir? n
                                  COS: 1           Display Language: english

DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS (Trunk Access Codes)
    Local Remote            Local Remote              Local Remote
 1: 9                    5:                        9:
 2: 82                   6:                       10:
 3:                      7:                       11:
 4:                      8:                       12:

HUNDREDS SELECT BUTTON ASSIGNMENTS
 1:           5:            9:           13:           17:
 2:           6:           10:           14:           18:
 3:           7:           11:           15:           19:
 4:           8:           12:           16:           20:
```

2. In the **Console Type** field, type **principal**.

   The system can include only one night-only or one day/night console, unless you administer Tenant Partitioning. Night Service is activated from the principal console, or from the one station set per system that has a **nite-serv** button.

3. Press **Enter** to save your changes.

Setting up Night Station Service

To set up night station service:

1. Type **`change listed-directory-numbers`**. Press **Enter**.

   The system displays the Listed Directory Numbers screen (Figure 324: Listed Directory Numbers screen on page 1289).

Figure 324: Listed Directory Numbers screen

```
                          LISTED DIRECTORY NUMBERS

                        Night Destination: 1234

          Ext     Name                          TN
     1: 8100     attendant 8100
     2:
     3:
     4:
     5:
     6:
     7:
     8:
     9:
    10:
```

2. Type the extension number in the **Night Destination** field. In this example, the extension number is **1234**.

   The destination can be an extension, a recorded announcement extension, a vector directory number, or a hunt group extension.

3. Press **Enter** to save your changes.

4. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 325: Console Parameters screen on page 1289).

Figure 325: Console Parameters screen

```
CONSOLE PARAMETERS
        Attendant Group Name: 27 character name  OPERATOR
                         COS: 1                                  COR: 1
      Calls in Queue Warning: 5                    Attendant Lockout? y
       Ext Alert Port (TAAS):
                         CAS: none
             SAC Notification? n              Night Service Act. Ext.: 1234
                 IAS (Branch)? n              IAS Tie Trunk Group No.:
        IAS Att. Access Code:                   Alternate FRL Station:
              Backup Alerting? n        DID-LDN Only to LDN Night Ext? n
     Attendant Vectoring VDN:
```

5. In the **DID-LDN Only to LDN Night Extension** field, type **n**.

6. Press **Enter** to save your changes.

After you set up night station service, you must have the attendant use the night console button to activate and deactivate night service.

Setting up Trunk Answer from Any Station

To set the FAC for TAAS:

1. Type **change feature-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Click **Next** until you see the **Trunk Answer Any Station Access Code** field (Figure 326: Feature Access Code (FAC) screen on page 1290).

Figure 326: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 3 of x
                            FEATURE ACCESS CODE (FAC)

                  Priority Calling Access Code:
                         Program Access Code:
       Refresh Terminal Parameters Access Code:
              Remote Send All Calls Activation:       Deactivation:
              Self Station Display Access Code:
                     Send All Calls Activation:       Deactivation:
         Station Firmware Download Access Code:
                       Station Lock Activation:       Deactivation:
     Station Security Code Change Access Code:
              Station User Admin of FBI Assign:                 Remove:
  Station User Button Ring Control Access Code:
                          Telephone Activation: #*
             Terminal Dial-up Test Access Code:
Terminal Translation Initialization Merge Code:       Separation Code:
            Transfer to Voice Mail Access Code:
          Trunk Answer Any Station Access Code: 71
              User Control Restrict Activation:       Deactivation:
  Voice Coverage Message Retrieval Access Code:
 Voice Principal Message Retrieval Access Code: *80
```

3. In the **Trunk Answer Any Station Access Code** field, type the access code. In this example, the access code is **71**.
4. Press **Enter** to save your changes.

Setting up external alerting

Once you set the FAC, you must determine where the external alerting device is connected to the server that is running Communication Manager (this example uses port 01A0702).

To set up external alerting:

1. Type **change console-parameters**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 327: Console Parameters screen).

Figure 327: Console Parameters screen

```
change console-parameters                                    Page   1 of x
                              CONSOLE PARAMETERS
         Attendant Group Name: OPERATOR
                         COS: 0                                  COR: 0
       Calls in Queue Warning: 5                    Attendant Lockout? y
        Ext Alert Port (TAAS): 01A0702
                         CAS: none
                                                Night Service Act. Ext.:
                IAS (Branch)? n                 IAS Tie Trunk Group No.:
          IAS Att. Access Code:                   Alternate FRL Station:
               Backup Alerting? n          DID-LDN Only to LDN Night Ext? n
      Attendant Vectoring VDN:
```

2. In the **EXT Alert Port (TAAS)** field, type the port address that is assigned to the external alerting device. In this example, the number is **01A0702**.
3. Press **Enter** to save your changes.

Setting up external alerting Night Service

To send Listed Directory Number (LDN) calls to the attendant during the day and to the desk of a security guard at night:

1. Type **change listed-directory-numbers**. Press **Enter**.

   The system displays the Listed Directory Numbers screen (Figure 328: Listed Directory Numbers screen on page 1292).

Figure 328: Listed Directory Numbers screen

```
LISTED DIRECTORY NUMBERS

                        Night Destination: 3000


          Ext      Name                            TN
     1: 2000     Attendant                       1
     2:                                          1
     3:                                          1
     4:                                          1
     5:                                          1
     6:                                          1
     7:                                          1
     8:                                          1
     9:                                          1
    10:                                          1
```

2. In the **Night Destination** field, verify that this field is blank.
3. Press **Enter** to save your changes.
4. Type **`change console-parameters`**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 329: Console Parameters screen on page 1292).

Figure 329: Console Parameters screen

```
CONSOLE PARAMETERS
        Attendant Group Name: Operator
                         COS: 0                                  COR: 0
      Calls in Queue Warning: 5                    Attendant Lockout? y
       Ext Alert Port (TAAS): 01A0702
                         CAS: none
             SAC Notification? n              Night Service Act. Ext.:
                 IAS (Branch)? n              IAS Tie Trunk Group No.:
        IAS Att. Access Code:                   Alternate FRL Station:
             Backup Alerting? n        DID-LDN Only to LDN Night Ext? n
     Attendant Vectoring VDN:
```

5. In the **EXT Alert Port (TAAS)** field, type the port address that is assigned to the external alerting device. In this example, the number is **01A0702**.
6. Press **Enter** to save your changes.

The system is in Night Service.

- Any calls to extension 2000 now go to extension 3000, the desk of the security guard.

- Any "0" seeking calls go to extension 3000 (the guard's desk).

To send LDN calls to the attendant during the day and to the TAAS bell at night:

1. Type **change console-parameters**. Press **Enter**.

   The system displays the Console Parameters screen (Figure 330: Console Parameters screen on page 1293).

Figure 330: Console Parameters screen

```
                          CONSOLE PARAMETERS
    Attendant Group Name: Operator
                     COS: 0                                    COR: 0
  Calls in Queue Warning: 5                      Attendant Lockout? y
   Ext Alert Port (TAAS): 01A0702
                     CAS: none
         SAC Notification? n                Night Service Act. Ext.:
             IAS (Branch)? n                IAS Tie Trunk Group No.:
     IAS Att. Access Code:                    Alternate FRL Station:
          Backup Alerting? n          DID-LDN Only to LDN Night Ext? y
 Attendant Vectoring VDN:
```

2. In the **DID-LDN Only to Night Ext.** field, type **y**.

   This allows only LDN calls to go to the Listed Directory Night Service Number Extension.

3. In the **Ext Alert Port (TAAS)** field, type the port address that is assigned to the external alerting device. In this example, the number is **01A070**.

4. Press **Enter** to save your changes.

The system is in night service. Any Dialed Number Identification Service (DNIS) extension 2000 and any 0-seeking calls now go to the TAAS bell.

Setting up Night Service for trunk groups

To set up Night Service for trunk groups:

1. Type **change trunk-group *n***, where ***n*** is the number of a trunk group. Press **Enter**.

   The system displays the Trunk Group screen. In this example, direct night calls for trunk group **2** to extension **1245**.

2. In the **Night Service** field, type the extension number that you want the calls to go to. In this example, the extension number is **1245**.

   The destination can be a station extension, a recorded announcement extension, a vector directory number (VDN), a hunt group extension, a terminating extension group (TEG), or **attd** if you want to direct the call to the attendant.

3. Press **Enter** to save your changes.

Setting up Night Service for hunt groups

To set up Night Service for a hunt group:

1. Type **change hunt-group *n***, where ***n*** is the number of a hunt group. Press **Enter**.

   The system displays the Hunt Group screen (Figure 331: Hunt Group screen on page 1294).

Figure 331: Hunt Group screen

```
                                HUNT GROUP

           Group Number: 3                                    ACD? n
             Group Name: Accounting                         Queue? y
        Group Extension: 2011                             Vector? n
             Group Type: ucd-mia                    Coverage Path: 1
                     TN: 1                 Night Service Destination: 1234
                    COR: 1                           MM Early Answer? n
          Security Code: ____
       ISDN Caller Disp: ________

           Queue Length: 4
Calls Warning Threshold: ___   Port: x      Extension: _______
 Time Warning Threshold: ___   Port: x      Extension: _______
```

2. In the **Night Service Destination** field, type the extension number. In this example, the extension number is **1234**.

   The destination can be an extension, a recorded announcement extension, a VDN, a hunt group extension, **attd** if you want to direct calls to the attendant.

   Calls to hunt group 3 follow the coverage path that is assigned to extension 1234.

3. Press **Enter** to save your changes.

Considerations for Night Service

This section provides information about how the Night Service feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Night Service under all conditions. The following considerations apply to Night Service:

Considerations for Hunt Group Night Service

- Both Hunt Group Night Service and Trunk Group Night Service can be active at the same time. An incoming trunk call is redirected to the trunk group's designated NSE. If this NSE is a hunt group or split that is in Hunt Group Night Service mode, the call is redirected to the Hunt Group NSE.
- Calls in progress (such as talking, on hold, or waiting in queue) on the hunt group or split are not affected when the hunt group or split is put in Hunt Group Night Service mode.
- When a hunt-group queue becomes empty, all idle members are placed in a busy condition.
- If Night Service is activated for a hunt group or split and a power failure occurs, the hunt group or split automatically returns to the Night Service mode.

Considerations for Night Console Service

- The night console must be identical to and have the same features as the primary console. A daytime console can double as the night console.
- Night Console Service calls to the attendant group are still handled by an attendant, even though the primary and daytime attendant consoles are out of service.
- Only one night console is allowed in the system. The night console can be activated only when the primary and daytime consoles have been deactivated.
- If Night Console Service is active and a power failure occurs, the system automatically returns to Night Console Service mode when it is powered up.

Considerations for Night Station Service

- When Night Station Service is active but you have not established Night Station extensions, a user can activate TAAS.

- You can assign a **Night-Serv** button to either an attendant extension or a phone extension. An individual trunk group or hunt group can be put into night service by either an attendant extension or a phone extension with the necessary button. When a user presses this button to activate Night Station Service, all calls to that particular trunk group or hunt group are routed to the Night Service extension assigned to that group.
- If a trunk without disconnect supervision goes to Night Service, the system drops the trunk after a period of time to avoid locking up the trunk. The call is not routed to the DID-LDN night extension.

Considerations for TAAS

- If Night Service is active and a power failure occurs, the system, when brought back up, automatically returns to Night Service mode.

Considerations for Trunk Group Night Service

- All incoming calls on Night Service trunk groups go to the trunk group's NSE unless the trunk group member has its own Trunk Group Member Night Destination, in which case the calls are redirected to that destination instead of the trunk group's NSE.
- Calls already in progress on a trunk group (such as talking, on hold, or waiting in queue), are not affected when the individual Trunk Group Night Service or System Night Service is activated.
- Trunk Group Night Service and System Night Service work independently of one another.
  - When a user activates System Night Service, any trunks that are controlled by individual Trunk Group Night Service buttons remain in day service. Trunk groups that are not currently assigned to Trunk Group Night Service are assigned to System Night Service.
  - Trunks with individual Trunk Group Night Service can be removed from Night Service even though the rest of the system remains in Night Service.
  - When a user deactivates System Night Service, any trunks that have individual Trunk Group Night Service still active remain in night service.
  - Trunks with individual Trunk Group Night Service can be placed into Night Service even though the rest of the system remains in day service.
- If a trunk is added to a trunk group while that trunk group is in Trunk Group Night Service, the trunk is brought up in night service.
- Individual Trunk Group Night Service does not apply to DID trunk groups.
- If Night Service is activated for a trunk group, and a power failure occurs, the trunk group automatically returns to the Night Service mode.

- If for some reason, a phone with a trunk-ns button remains out of service after a system reboot and later comes back in service, the **trunk-ns** lamp shows the trunk status within 10 seconds of coming back in service. For example, a telephone with a trunk-ns button might be unplugged when the system is rebooted. If the phone is plugged back in later, the trunk status is shown on the trunk-ns button within 10 seconds.

Interactions for Night Service

This section provides information about how the Night Service feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Night Service in any feature configuration.

Interactions for Hunt Group Night Service

- Automatic Call Distribution (ACD)

  When Hunt Group Night Service is active for a split and the night-service destination is a hunt group, the caller hears the first forced announcement for the original split. The system then redirects the call to the Night Service destination hunt group. When an agent in the Night Service hunt group becomes available, the call goes to that agent. If all agents in the hunt group are busy, the caller hears the following: forced or delayed first announcement, ringback, music-on-hold or silence, and a second announcement.

- Call Coverage

  Coverage takes precedence over Night Service. When Hunt Group Night Service is active, the NSE's normal coverage criteria and path apply. If the coverage path destination is CM Messaging, CM Messaging answers with the mail of the original hunt group. If the NSE is a hunt group or split of any type, the hunt group or split's call coverage criteria and coverage path apply. The coverage criteria and path can be different from that assigned to the phones that are members of that hunt group or split.

  If a coverage point is a hunt group or split in Night Service, the system considers the point to be unavailable and does not forward the call to the coverage point's NSE.

- Call Forwarding All Calls

  If a hunt group or split is in Hunt Group Night Service mode and the hunt group or split's NSE has Call Forwarding - All Calls active, the system forwards night-service calls terminating to that NSE to its designated call-forward extension.

  If the forwarded-to destination is a hunt group or split in Night Service mode, the system terminates the call at the forwarding extension.

Interactions for Night Console Service

- Trunk Group Night Service

  Activation of Night Console Service for the attendant consoles also puts trunk groups into night service, except those trunk groups for which you administered a Trunk Group Night Service button.

Interactions for Night Station Service

- Call Coverage

  Calls routed to the night extension using Night Station Service follow the coverage path of the night extension under all coverage criteria except Send All Calls.

  If a night extension has a coverage path in which Cover All Calls is administered, all attendant-seeking calls redirect to coverage. Changes to the protocol for handling DID-LDN calls (that is, forwarding attendant-seeking calls on or off premise from the night extension) do not work.

- Call Forwarding All Calls

  Calls redirected to the attendant through Call Forwarding All Calls do not route to the DID-LDN extension.

- Inward Restriction

  Inward-restricted phones can be administered for Night Station Service. Night Service features override Inward Restriction.

- Night Console Service

  Do not provide Night Console Service with this Night Station Service.

- Remote Access

  A Remote Access extension can be specified as the Night Station extension on an incoming, non-DID, trunk group.

- Tenant Partitioning

  Each tenant may have a designated night-service station. The system directs calls to an attendant group in night service to the night-service station of the appropriate tenant (when a night attendant is not available). When someone places an attendant group into night service, all trunk groups and hunt groups that belong to tenants served by that attendant group go into night service. In this case, the system routes incoming calls to the night-service destination of the appropriate tenant.

  Each tenant can have its own LDN night destination, TAAS port, or night attendant.

- Timed Reminder

  Timed Reminder calls returning to a console that has been placed in Night Service and has an assigned DID-LDN night extension are not redirected to the DID-LDN night extension. Rather, they are dropped.

- Trunk Answer from Any Station

  TAAS and Night Station Service can both be assigned within the same system, but cannot be assigned to the same trunk group.

Interactions for TAAS

- Call Coverage

  If Night Station Service is active, calls that are redirected to the attendant through Call Coverage can be answered by way of TAAS.

- Call Forwarding All Calls

  If Night Station Service is active, calls that are redirected to the attendant through Call Forwarding All Calls can be answered by way of TAAS.

- Inward Restriction

  Inward-restricted phones can activate TAAS for incoming trunk calls. Night Service features override Inward Restriction.

- Night Console Service

  Do not provide a Night Console Service with TAAS.

- Night Station Service

  TAAS and Night Station Service can both be assigned within the same system, but cannot be assigned to the same trunk group. Activating Night Station Service also activates Night Service - Trunk Group for any trunk group without an individual trunk-group Night Service button.

- Tenant Partitioning

  Each tenant can have its own LDN night destination, TAAS port, or night attendant.

Interactions for Trunk Group Night Service

- Call Forwarding All Calls

  If the individual Trunk Group Night Service mode and the trunk group's NSE have Call Forwarding All Calls activated, the night service calls that terminate to that NSE are forwarded to the designated extension.

- Forced First Announcements

  An interaction occurs with System Night Service and Forced First Announcement. For example, if hunt group A has a forced first announcement, assign the incoming CO trunk to terminate at hunt group A. Assign the incoming trunk's night-service destination to be another hunt group (hunt group B). Assign a Night Service button to the attendant.

  With night service active on the attendant, the incoming CO call routes to the night-service destination hunt group B and does not play the Forced First Announcement of the incoming destination's hunt group A.

- Listed Directory Number

  In System Night Service mode, all incoming LDN calls (except those using DID trunks) which have activated night service are redirected to their corresponding trunk group's NSE. Incoming LDN calls using DID trunks are directed to the Night Console Service, Night Station Service, or Trunk Answer From Any Station, respectively, whichever applies first. Non-LDN DID trunk calls terminate at the dialed extension.

Off-Premises Station

Use the Off-Premises Station feature to connect a telephone that is in a different building than the server that runs Communication Manager to your system.

Detailed description of Off-Premises Station

This section provides a detailed description of the Off-Premises Station feature.

With the Off-Premises Station feature, you can connect a telephone that is located in a different building than the server that runs Communication Manager to your system.

If you use central office (CO) trunk circuits, the telephone must be:

- Analog
- FCC registered, if the telephone is in the United States
- Registered by the appropriate governmental agency, if the telephone is located outside the United States

You can use digital communications protocol (DCP) sets as off-premises telephones if you add IP Softphone or IP Office. You can set up IP stations as off-premise stations if you use point-to-point protocol (PPP) connections. DS1 trunk service provides a digital interface for off-premises stations.

A trunk-data module connects off-premises private-line trunk facilities and Communication Manager. The trunk-data module converts between the RS-232C and the DCP, and can connect to Direct Distance Dialing (DDD) modems as the DCP member of a modem pool.

Off-Premises Station requires cross-connecting capabilities, and one port on an analog line or a DS1 tie trunk circuit pack for each interface that you want to provide. Not all analog lines can support an off-premises station. For more information, see the user guide for the appropriate telephone.

The maximum loop distance for off-premises stations is 20,000 feet (6093.34 meters) if you do not use repeaters. For information about the cable distance, see the user guide for the appropriate telephone.

Note that the system does not support the use of a message waiting indicator lamp (MWI) on an off-premises station.

Administering Off-Premises Station

The following steps are part of the administration process for the Off-Premises Station feature:

- Activating Off-Premises Station for a user

This section describes:

- Any prerequisites for administering the Off-Premises Station feature
- The screens that you use to administer the Off-Premises Station feature
- Complete administration procedures for the Off-Premises Station feature

Screens for administering Off-Premises Station

Screen name	Purpose	Fields
Station (analog)	Activate an off-premises station for a user.	• **Off Premise Station** • **R Balance Network**

Activating Off-Premises Station for a user

To activate Off-Premises Station for a user:

1. Type **`change station`** ***`n`***, where ***`n`*** is the extension of the user for whom you want to activate an off-premises station. Press **Enter**.

   The system displays the Station screen for the extension that you requested (Figure 332: Station screen on page 1303).

Figure 332: Station screen

```
change station 105 Page   1 of   3
                                    STATION

Extension: 106                          Lock Messages? n          BCC: 0
     Type: 2500                         Security Code:             TN: 1
     Port:                            Coverage Path 1:            COR: 1
     Name:                            Coverage Path 2:            COS: 1
                                      Hunt-to Station:          Tests? y

STATION OPTIONS
              Loss Group: 1               Message Waiting Indicator: none
    Off Premises Station? n




                                                  Remote Office Phone? n
```

2. In the **Off-Premises Station** field, perform the following actions:
   - If the telephone associated with this Station screen is not located in the same building as the server, type **y**.

     If you type **y**, you must administer the **R Balance Network** field on the Station screen.
   - If the telephone associated with this Station screen is located in the same building as the server, type **n**.
3. In the **R Balance Network** field, perform one of the following actions.
   - Type **y** to select the R Balance Capacitor network. Type **y** in all other cases, except for the following cases:
   - Type **n**:
     - To select the standard resistor capacitor network
     - When the station port circuit is connected to the terminal equipment. Terminal equipment includes, for example, SLC carriers or impedance compensators. These are optioned for 600-ohm input impedance and the distance between the server and the equipment is less than 3,000 feet (914.4 meters).

     You must complete the **R Balance Network** field if the **Off-Premises Station** field on the Station screen is set to **y**

Interactions for Off-Premises Station

This section provides information about how the Off-Premises Station feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Off-Premises Station in any feature configuration.

- Distinctive Ringing

  The Distinctive Ringing feature might function improperly at an off-premises telephone because of the distance of the telephone from the server. However, the Distinctive Ringing feature can be disabled when you set the **Off-Premises Station** field on the Station screen to **y**. If the Distinctive Ringing feature is not used with an off-premises station, the telephone receives one-burst ringing for all calls.

Overriding of SAC/CF

Use the **Send All Calls and Call Forwarding (SAC/CF) Override** feature to override active rerouting. This feature overrides these active rerouting settings:

- Send All Calls (SAC)
- Call Forwarding (CF) all
- Enhanced Call Forwarding (ECF) unconditional

The Overriding of SAC and CF feature is a standard feature starting with Communication Manager Release 5.2.

Detailed description

Enabling the SAC/CF override feature depends on call initiation. Call using the dial pad (dialing) or using the Priority button. On enabling SAC/CF override, the call may:

- Execute override – Ring called station
- Execute no override
- Display message – Wait for further input

The settings controlling SAC/CF override are listed here:

Class of Restriction (COR) settings

- COR of calling station – SAC/CF Override by Dialing
- COR of calling station – SAC/CF Override by Priority button
- COR of called station – SAC/CF Override Protection

Station screen:

- Calling station screen: SAC/CF Override

Administer overriding of SAC/CF

Enable overriding by administering the settings on the Class of Restriction screen (COR), Systems Parameters and the corresponding calling station screens. These settings enable a user at the calling station to override active rerouting.

- Set **SAC/CF Override by Dialing** on the Class of Restriction screen (COR).
- Set **SAC/CF Override by Priority Call** on the COR screen.
- Set **SAC/CF Override Protection for Dialing** on the COR screen of the called station to disable **SAC/CF Override by Dialing Call** for the calling station.
- Set **SAC/CF Override Protection for Priority Calls** on the COR screen of the called station to disable the **SAC/CF Override by Priority Call** setting.
- Specify permissions to allow or restrict call override by selecting **ask / no / yes** on the Station screen.

Enabling SAC/CF Override by Dialing or Priority calling

To enable SAC/CF override by Dialing / Priority calling feature:

1. Type **`change cor`**.

   The system displays the Class of Restriction screen with the **SAC/CF Override by Dialing** and **SAC/CF Override by Priority Call** field.

Figure 333: COR Settings

```
Change cor 1                                                    Page   3 of  x
                              CLASS OF RESTRICTION

            SAC/CF Override by   Team Btn? n  Priority Call? n  Dialing? n
SAC/CF Override Protection for   Team Btn? n  Priority Call? n  Dialing? n
Display Names on Bridged Appearance Labels? n
         Remove Caller Id from Set Display? n
_   ___     n
```

2. Enter **y** to enable the override for Dialing or Priority calling. The default setting is **n**.

Note:
To view the settings of SAC/CF override on Class of Restriction screen:

- Type **`display cor`**.

The system displays the Class of Restriction screen with the **SAC/CF Override by Dialing** or **SAC/CF Override by Priority Call** field.

Enabling SAC/CF Override Protection

To enable settings of SAC/CF override protection by Dialing or Priority calling feature:

1. Type **change cor**.

   The system displays the Class of Restriction screen displaying the **SAC/CF Override Protection by Dialing** and **SAC/CF Override Protection by Priority Call** field.

2. Enter **y** to enable the override protection. The default setting is **n**.

Note:
To view settings of SAC/CF override protection feature on Class of Restriction screen:

- Type **display cor**.

The system displays Class of Restriction screen with the **SAC/CF Override Protection by Dialing** and **SAC/CF Override Protection by Priority Call** field.

Enabling SAC/CF Override for station with or without display

To enable SAC/CF override for a station with or without display:

1. Type **add station** or **change station**.

   The system displays the Station screen with the **SAC/CF Override** field in the Enhanced Call Forwarding area.

2. Enter **y** to enable the override or enter **ask** to see message on a station with display. The default setting is **n**.

Using SAC/CF Override

This section describes the following usage of the SAC/CF Override feature. Some prerequisite settings, configured by the administrator are also listed:

- Overriding of SAC/CF on page 1308
- Asking for Overriding of SAC/CF on page 1310
- No Overriding of SAC/CF on page 1313

Overriding of SAC/CF

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional settings	Notes / Results
yes	no	ask	**Call Forward Override** on System Parameters screen Call Coverage / Call Forwarding is set to **y**.	Dialed call overrides SAC/CF unconditionally only when the call is rerouted to the calling station.
yes	no	ask	**Call Forward Override** on System Parameters screen Call Coverage / Call Forwarding is set to **y**.	Priority button call overrides SAC/CF unconditionally.
yes	no	yes / ask	**All Inside Call** in coverage path on called station screen is set to **n**.	Dialed call overrides SAC/CF unconditionally for active rerouting setting **y**. For rerouting set to **ask**, system displays a message. Coverage is disabled.
yes	no	yes / ask	**All Inside Call** in coverage path on called station screen is set to **n**.	Priority button call overrides SAC/CF unconditionally for active rerouting setting **y**. For rerouting set to **ask**, system displays a message. Coverage is disabled.

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional settings	Notes / Results
yes	no	yes / ask	NA	Priority button call overrides SAC/CF unconditionally. Active rerouting enabled at principal station. (CF all or ECF unconditional are active.)
yes	no	yes / ask	NA	Dialed call or Priority button call overrides SAC/CF. User at called station picks up the call.
yes	no	yes	NA	Dialed call overrides SAC/CF when called station is not busy on any last call appearance.
yes	no	yes	NA	Priority button call overrides SAC/CF when called station has at least one call appearance available.
yes	no	yes	NA	Dialed call or Priority button call overrides SAC/CF at called station with active auto answer. Auto answer is not executed.

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional settings	Notes / Results
yes	no	yes	NA	Dialed call or Priority button call overrides SAC/CF. The Reset Shift Call function is not executed at called station.
yes	no	yes	NA	Dialed call or Priority button call overrides SAC/CF. Overriding precedes station hunting at called station.

Asking for Overriding of SAC/CF

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes / Results
yes	no	ask	**Call Forward Override** on System Parameters screen Call Coverage / Call Forwarding is set to **n**.	Dialed call results in a message displayed at calling station.
yes	no	ask	**Call Forward Override** on System Parameters screen Call Coverage / Call Forwarding is set to **n**.	Active rerouting enabled at principal station. Priority button call results in a message displayed at calling station.

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes / Results
yes	no	yes / ask	**All Inside Call** in coverage path on called station screen is set to **n**.	Rerouting is set to **ask**. Dialed call results in system displaying a message at calling station. Coverage is disabled.
yes	no	ask	NA	Dialed call results in a message displayed at calling station. Called station has restricted last call appearance.There is no impact of this feature when called station is in idle state. Otherwise the called station is busy.
yes	no	ask	NA	Dialed call results in a message displayed at calling station. The called station has at least one last call appearance available.
yes	no	ask	NA	Priority button call results in a message displayed at calling station. The called station has at least one last call appearance available.

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes / Results
yes	no	ask	NA	Dialed call or Priority button call result in a message displayed at calling station.The call is forwarded or rerouted.
yes	no	ask	NA	Dialed call or Priority button call result in a message displayed at calling station. Internal auto answer function is not executed at the called station.

Asking for rerouting with active forwarding

Call by dialing, pressing the dial button or initiating the call from the dial pad.

A message is displayed, informing about the rerouting or overriding. Dialing or pressing any other button leads to the result as follows:

- Dialing 0 or **#**: Override the call forwarding within 9 seconds to ring principal station.
- Dialing 1 or *****: Reject the call forward. You hear an intercept tone.
- No action within 9 seconds: Rerouting to the forwarded-to station.

No Overriding of SAC/CF

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes / Results
yes	no	yes / ask	NA	Dialed call results in no override when Send All Calls is active.
yes	no	yes / ask	NA	Priority button call results in no override when Send All Calls is active.
yes	no	yes / ask	**All Inside Call** in coverage path on called station screen is set to **y**.	Dialed call results in no override when Active rerouting enabled at principal station. Coverage is disabled.
yes	no	yes / ask	**All Inside Call** in coverage path on called station screen is set to **y**.	Priority button call results in no override when Active rerouting enabled at principal station. Coverage is disabled.
yes	no	yes / ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Group calls are enabled.

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes / Results
yes	no	yes / ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Goto Cover is active.
yes	no	yes	NA	Dialed call results in no overriding of SAC/CF when the called station has at least one busy last call appearance.
yes	no	yes	NA	Priority call results in no overriding of SAC/CF when the called station has at least one busy last call appearance.
yes	no	yes	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Do not Dial is active.
yes	no	ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Do not Dial is active.

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes / Results
yes	no	yes	NA	Dialed call or Priority button call results in no overriding of SAC/CF when active rerouting is located in another switch connected through QSIG. The call is rerouted.
NA	NA	NA	NA	Dialed call or Priority button call results in no overriding of SAC/CF when calling station is off-PBX. The call is rerouted.
yes	no	ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF with chained routing active. A message is displayed at the calling station.
yes	no	ask	NA	Dialed call or Priority button call results in no overriding of SAC/CF when Do not Dial is active.

COR of calling station: SAC/CF Override by Dialing / Priority button	COR of called station: SAC/CF Override Protection	Calling station screen: SAC/CF Override	Additional Settings	Notes / Results
NA	NA	NA	NA	Dialed call or Priority button call results in no overriding of SAC/CF for intercom calls enabled at the called station.
NA	NA	NA	NA	Dialed call or Priority button call results in no overriding of SAC/CF for whisper page calls.

The settings on the station screen of the monitoring station are:

- **no** - cannot override rerouting. The station doesn't have the ability to override rerouting.
- **yes** - can override rerouting. The station has the ability to override the rerouting the called station has set, as long as one incoming call appearance is free and the called station allows overriding by its COR settings. If no free call appearance is available or protection is set, the call fails and the user of the monitoring station hears busy tone.
- **ask** - ask whether the user wants to follow the rerouting or override it. When the user of the station can decide whether rerouting should take place or not, a message is sent to the station which displays the active rerouting and the number of the forwarded station. The user of the monitoring station can now follow the rerouting by dialing 1 or #, or by letting the timer which supervises the team button pushes expire, or overriding the active rerouting by dialing 0 or *.

Personal Station Access

Use the Personal Station Access (PSA) feature to allow a user to associate the preferences and permissions of the user telephone with another telephone of the same type.

Detailed description of Personal Station Access

This section provides a detailed description of the Personal Station Access (PSA) feature.

With the PSA feature, users can associate the preferences and the permissions of the user telephone with another telephone of the same type.

Telecommuting

With PSA, different users can use the same group of telephones at different times. For example, several telecommuting users can use the same office on different days of the week. The users use PSA to associate with the office telephone. When a user associates the telephone, the telephone is assigned to that user. For example, the user can originate and receive calls.

At home, a telecommuting user can also use PSA to install a digital communications protocol (DCP) telephone and a DEFINITY Extender. The user can then call into the system, and use PSA to associate the home telephone with the extension that is assigned to the user at the office. When someone calls the user extension, the call rings at the home of the user.

When a user no longer wants to use PSA, the user disassociates from the telephone.

PSA requires a user to enter a security code, from either an onsite or an off-site telephone.

Invalid attempts to use PSA

Invalid attempts to use PSA generate referral calls. If the Security Violation Notification (SVN) feature is enabled, the SVN software logs the invalid attempt. If a user hangs up, or presses the release button, the system does not log the action as an invalid attempt.

Preferences and permissions

The preferences and the permissions that are assigned to the user extension, and that are retained with PSA include:

- The definition of terminal buttons
- Abbreviated dial lists
- Class of Service (COS) permissions
- Class of Restriction (COR) permissions

Extensions that do not have a COS, such as expert agent selection (EAS) agents or hunt groups, cannot use PSA.

Button mapping

PSA functions only on analog, hybrid, and digital communications protocol (DCP) telephones. Many types of DCP telephones exist, with different types and numbers of buttons. If you attempt to associate a DCP telephone or a hybrid telephone with a telephone that has incompatible buttons, button mapping is unpredictable. If you want the user to be able to use the terminal buttons and to have consistent displays, associate stations with terminals of the same type. Telephones and ports on different media servers or switches cannot be associated through PSA. Telephones on different switches, or nodes, within Distributed Communications Systems (DCS) cannot be associated through PSA. The system does not limit the number of stations that can use PSA. However, heavy use of the associate and dissociate functions can have a temporary impact on system performance.

Unanswered calls

When a call goes to coverage from a PSA-disassociated extension, the software sends a message to the coverage point to indicate that the call was unanswered. If the coverage point is a display telephone, the system displays the letter *a* which means "don't answer." If the coverage point is a voice messaging system, the voice messaging system receives an indication from the software that the call was unanswered, and the voice messaging system processes the call as unanswered.

Dissociated telephones

When a user requests to associate a telephone with PSA, any other telephone that uses the extension is automatically dissociated. Users can place emergency calls from a dissociated telephone, if a COR is assigned to dissociated telephones on the Feature-Related System Parameters screen.

PSA allows a dissociate request from a bridged appearance. However, the system dissociates the telephone from which the user issues the PSA command, even if the user is on a bridged appearance of another telephone.

The dissociate function within PSA allows a user to restrict the features that are available at a telephone. When a user uses PSA to dissociate a telephone, the telephone can only be used to:

- Call an attendant
- Accept a terminal translation initialization (TTI) or a PSA request

To enable users to make other types of calls from dissociated telephones, you must establish a COR for the telephones.

For example, assume that extension 4001 and extension 4002 are administered on telephones A and B. On telephone A, user 4001 dials PSA Associate Code, followed by the extension and security code of user 4002, the following events occur:

- Telephone A associates with extension 4002
- Extension 4001 turns to an AWOH extension (X-port)
- Telephone B is not available

When user 4002 dials PSA Dissociate Code on telephone A, the following events occur:

- Telephone A dissociates from extension 4002 and is unavailable
- The dissociation telephone does not restore any previous association with other telephones.
- Extension 4002 dissociates from telephone A and turns to an AWOH

If you again decide to associate these telephones with the same or different extensions, for analog or digital telephones you must use the PSA or TTI feature to associate with an extension and for IP (h.323) phones you login with an extension.

Security

SECURITY ALERT:
Once an extension is associated with a telephone, users of that telephone have the capabilities that are associated with the extension. You must issue a dissociate command from the telephone to ensure that unauthorized users cannot use the telephone. Dissociate the telephones if you use PSA and DCP extenders to permit remote DCP access.

Administering Personal Station Access

The following steps are part of the administration process for the Personal Station Access feature:

- Viewing the user extensions that have the Call Forwarding capabilities active

This section describes:

- Any prerequisites for administering the Personal Station Access feature
- The screens that you use to administer the Personal Station Access feature
- Complete administration for the Personal Station Access feature

Prerequisites for administering Personal Station Access

You must complete the following actions before you can administer the Personal Station Access feature:

- Enable the Personal Station Access feature on your system.
- Create a class of service (COS) that enables your users to use the capabilities associated with the Personal Station Access feature.
- Ensure that Feature Access Codes (FACs) for Call Forwarding and Call Forward Busy/ Don’t Answer are available on your system, if you want users to use an FAC for either of the capabilities.

To create a COS that enables your users to use the Personal Station Access feature:

You can create many classes of service. These classes of service enable many features and capabilities, including those for the Personal Station Access feature. You can create a COS that enables none, some, or all of the capabilities associated with the Personal Station Access feature. However, you can assign only one COS to each user. For more information on COS, see *Administering Avaya Aura™ Communication Manager,* 03-300509.

To ensure that an FAC for PSA is available on your system:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen.

2. Click **Next** until you see the **Personal Station Access (PSA) Associate Code** field (Figure 334: Feature Access Code (FAC) screen on page 1321).

Figure 334: Feature Access Code (FAC) screen

```
change feature-access-codes                                      Page 2 of 7
                            FEATURE ACCESS CODE (FAC)
     Emergency Access to Attendant Access Code:
                     Enhanced EC500 Activation:        Deactivation:
     Extended Call Fwd Activate Busy D/A_  All:        Deactivation:
        Extended Group Call Pickup Access Code:
                Facility Test Calls Access Code:
                             Flash Access Code:
              Group Control Restrict Activation:        Deactivation:
                     Hunt Group Busy Activation:        Deactivation:
                               ISDN Access Code:
                  Last Number Dialed Access Code:
    Leave Word Calling Message Retrieval Lock:
   Leave Word Calling Message Retrieval Unlock:
             Leave Word Calling Send A Message: #66
           Leave Word Calling Cancel A Message: *66
                Malicious Call Trace Activation:        Deactivation:
         Meet-me Conference Access Code Change:
PASTE  (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:        Dissociate Code:
        Per Call CPN Blocking Code Access Code:
      Per Call CPN Unblocking Code Access Code:
                              Posted Messages:
```

3. In the **Personal Station Access (PSA) Associate Code** field, type an FAC that allows a user to associate a telephone.

4. In the **Personal Station Access (PSA) Disssociate Code** field, type an FAC that allows a user to dissociate a telephone.

   To type an FAC in the **Personal Station Access (PSA) Disssociate Code** field, the **Personal Station Access (PSA)** field in the System Parameters Customer-Options screen must be set to **y**.

5. Press **Enter** to save your changes.

Screens for administering Personal Station Access

Screen name	Purpose	Fields
Class of Service	Assign PSA to a Class of Service (COS).	**Personal Station Access**
Feature Access Code (FAC)	Define a Feature Access Code (FAC) to associate and dissociate telephones.	**Personal Station Access (PSA) Associate Code and Dissociate Code**
Feature-Related System Parameters	Specify the Class of Restriction (COR) to apply to calls made from dissociated telephones.	**COR for PSA Dissociated Sets**
	Specify the calling party number or automatic number identification (ANI) for calls that are made from dissociated telephones.	**CPN, ANI for PSA Dissociated Sets**
	Specify that the system record PSA transactions in the history log.	**Record CTA/PSA/TTI Transactions in History Log?**
	The new field **Hot Desking Enhancement Station Lock** on the System-Parameters Features screen controls the feature	**Hot Desking Enhancement Station Lock**
Station	Define the Station Security Code (SSC) for the extension.	**Security Code**

End-user procedures for Personal Station Access

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Personal Station Access (PSA):

- Using the PSA associate command
- Interrupting the PSA command sequence
- Using the PSA dissociate command

Using the PSA associate command

To use the PSA associate command, perform the actions shown in Table 84: PSA associate commands on page 1323.

Table 84: PSA associate commands

Step	User action	System response	Result
1	Dial the Feature Access Code (FAC) for PSA associate.	Dial tone	The request is successful.
		Intercept tone	• The request is unsuccessful, because the request was not made at an analog, a hybrid, or a DCP telephone. • The request is unsuccessful because the telephone is associated with or assigned to a station that does not have PSA permission in its COS.
2	Dial an extension, and then press the pound key (#).	No response	If the user is at a telephone with a display, this pound sign (#) is the last character that the system displays until the PSA sequence is complete.

1 of 2

Table 84: PSA associate commands (continued)

Step	User action	System response	Result
3	Dial the Station Security Code (SSC) for the user extension, and then press the pound key (#).	Confirmation tone	The command sequence is successfully complete. The system queues the request.
		Intercept tone immediately after the confirmation tone.	The request is unsuccessful, because: • Terminal translation initialization (TTI) is not enabled for voice. • Either the dialed extension, or the originating extension, has an add, a change, or a remove action in progress. • You dialed more that 15 digits before you pressed the pound key (#). Issue the PSA request again.
		Intercept tone	The request is unsuccessful because: • The extension and the SSC are incompatible. – The extension is invalid. – The SSC is invalid for the extension. – Both the extension and the SCC are invalid. The Security Violation Notification (SVN) feature logs this unsuccessful use of PSA as an invalid attempt. • The Class of Service (COS) of the extension does not allow PSA. • An extension in one tenant partition cannot be associated with a telephone in another tenant partition.
		Reorder tone	The request is unsuccessful because: • The extension that was entered is in use. • An agent is logged in at the dialed extension. • The system load is too heavy to allow the request to occur. The user can try again later.
			2 of 2

Interrupting the PSA associate command sequence

If you enter incorrect information after you enter the FAC, you can interrupt the command sequence and begin again. To interrupt the command sequence:

1. Press the star key (*) at any time before you press the pound key (#) for the second time.

   The system generates dial tone

2. Dial the extension, but do not dial the FAC again.

SVN does not record the interrupted command sequence as an invalid attempt.

Using the PSA dissociate command

To use the PSA dissociate command,:

- Enter the FAC for PSA dissociate.

  The system responds with:

  — Confirmation tone if the:

    - System successfully dissociates the telephone
    - Telephone was not previously associated

  — Intercept tone, if the COS of the telephone extension does not allow the use of PSA.

Reports for Personal Station Access

The following reports provide information about the Personal Station Access feature:

- None

Considerations for Personal Station Access

This section provides information about how the Personal Station Access (PSA) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Personal Station Access under all conditions. The following considerations apply to Personal Station Access:

- None

Interactions for Personal Station Access

This section provides information about how the Personal Station Access (PSA) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Personal Station Access in any feature configuration.

- Adjunct/Switch Application Interface (ASAI)

  You cannot use PSA on an ASAI link, because ASAI uses a Basic Rate Interface (BRI) port. Do not assign a Class of Service (COS) that allows PSA to an ASAI link.

- Bridged Appearance

  When you issue a PSA dissociate request for the principal telephone, the bridged appearances of the telephone remain active. The bridged appearances remain active if the telephones on which the bridged appearances appear have not been dissociated.

  When a call is made to the principal extension, any of the bridged appearances can alert. If the call cannot alert at a bridged appearance of the principal extension, the system routes the call to the coverage path of the principal extension.

  PSA allows a dissociate request from a bridged appearance. However, the system dissociates the telephone at which the user issues the PSA command, even if the user is on a bridged appearance of another telephone.

- Call Management

  A PSA dissociate request automatically logs out an Automatic Call Distribution (ACD) agent.

- Coverage

  PSA does not change coverage path operations. If a station is dissociated, the system routes calls to coverage, unless the calls are forwarded.

- Property Management System (PMS)

  Do not assign a COS that allows PSA to an extension that is assigned to a room, instead of to a user.

- Save Translations

  PSA commands cannot be run successfully during a save translations operation. When a reset 3 or greater (reset 4, reset 5, and so on) occurs on the system, all associations revert to the state as of the last save translations operation.

- Security Violation Notification (SVN)

  If SVN is active, SVN tracks and reports PSA security violations.

- Tenant Partitioning

  If a telephone is already associated, a user who attempts a PSA associate request at that telephone must specify an extension that is in the same partition as the extension that is already associated with the telephone.

  However, any user in any partition can issue a PSA dissociate request at the telephone, if the COS of the telephone extension allows PSA. After the user successfully dissociates the extension, the user can issue a PSA associate request for an extension in any tenant partition.

Hot Desking interaction with PSA

The Hot Desking Enhancement (HDE) feature displays PSA Login information. You can invoke Personal Station Access (PSA) using H.323 IP telephones. If the Hot Desking Enhancement on page 1514 is activated, the telephone displays a text message to inform you how to log in again after PSA logoff.The message is sent to all telephones, including IP (H.323) telephones, if the **Hot Desking Enhancement Station Lock** field on the Feature-Related System Parameters screen is set to **y**.

The message used for displaying the PSA Login information is a non-call associated message, which gets shown at the top of an IP (H.323) telephone.

The new field **Hot Desking Enhancement Station Lock** on the System-Parameters Features screen controls the feature, as shown in Figure 335:

Figure 335: Hot Desking Enhancement Station Lock on System-Parameters Features screen

```
change system-parameters features                              Page 3 of x
                    FEATURE-RELATED SYSTEM PARAMETERS
TTI/PSA PARAMETERS

  WARNING!  SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE

        Terminal Translation Initialization (TTI) Enabled? y
                TTI State: voice        TTI Security Code: 1234

        Enhanced PSA Location/Display Information Enabled? y
                         Default COR for Dissociated Sets: 1
                            CPN, ANI for Dissociated Sets: 7010
          Unnamed Registrations and PSA for IP Telephones? y
               Customer Telephone Activation(CTA) Enabled? y
 Don't Answer Criteria For Logged Off IP/PSA/TTI Stations? n
                     Hot Desking Enhancement Station Lock? n

EMU PARAMETERS
           EMU Inactivity Interval for Deactivation(hours):

CALL PROCESSING OVERLOAD MITIGATION
           Restrict Calls: stations-first
```

Personalized Ringing

Use the Personalized Ringing feature to hear one of eight ringing patterns for incoming calls. You assign the ringing pattern to each user on your system. The different ringing patterns help users who work in the same area to distinguish their calls from the calls of other users.

Detailed description of Personalized Ringing

This section provides a detailed description of the Personalized Ringing feature.

You can administer Personalized Ringing for each telephone. Either you, or the end user, can administer Personalized Ringing for some programmable telephones.

Ringing patterns

The eight administrable ringing patterns are different combinations of three tones. The eight tone combinations are (in Hertz):

- 750, 750, 750 (standard ringing)
- 1060, 1060, 1060
- 530, 530, 530
- 530, 1060, 1060
- 1060, 1060, 530
- 1060, 530, 530
- 1060, 530, 1060
- 530, 1060, 530

Power failures

The user-specified ringing pattern for some digital telephones is lost when the power fails. The system retains the user-specified ringing pattern for ISDN-BRI telephones when the power fails.

Administering Personalized Ringing

The following steps are part of the administration process for the Personalized Ringing feature:

- Assigning Personalized Ringing to a user telephone

This section describes:

- Any prerequisites for administering the Personalized Ringing feature
- The screens that you use to administer the Personalized Ringing feature
- Complete administration procedures for the Personalized Ringing feature

Prerequisites for administering Personalized Ringing

You must complete the following actions before you can administer the Personalized Ringing feature:

- None

Screens for administering Personalized Ringing

Screen name	Purpose	Fields
Station	Assign Personalized Ringing to a user telephone.	**Personalized Ringing Pattern**

Assigning Personalized Ringing to a user telephone

To assign Personalized Ringing to a user telephone:

1. Type **`change station n`**, where ***n*** is the user telephone to which you want to assign Personalized Ringing. Press **Enter.**

   The system displays the Station screen (Figure 336: Station screen on page 1331).

Figure 336: Station screen

```
change station 1014                                          Page 1 of X
                              STATION

Extension: 1014               Lock Messages? n                    BCC: 0
     Type:                    Security Code:                       TN: 1
     Port:                  Coverage Path 1:                      COR: 1
     Name:                  Coverage Path 2:                      COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                           Message Lamp Ext: 1014
           Speakerphone: 2-way                    Mute button enabled? y
       Display Language? English                    Expansion Module?
                   Model:

 Survivable GK Node Name:                            Media Complex Ext:
                                                          IP Softphone? y
                                                   Remote Office Phone? y
```

2. In the **Personalized Ringing Pattern** field, type one of the valid entries shown in Table 85: Personalized ringing patterns on page 1331.

   Use the following key to the Usage column:

   - L - 530 Hz
   - M - 750 Hz
   - H - 1060 Hz

   For virtual stations, the **Personalized Ringing Pattern** field dictates the ringing pattern on the mapped-to physical telephone.

Table 85: Personalized ringing patterns

Valid entries	Usage
1	MMM (standard ringing)
2	HHH
3	LLL
4	LHH
5	HHL
6	HLL
	1 of 2

Table 85: Personalized ringing patterns (continued)

Valid entries	Usage
7	HLH
8	LHL
	2 of 2

3. Press **Enter** to save your changes.

Interactions for Personalized Ringing

This section provides information about how the Personalized Ringing feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Personalized Ringing in any feature configuration.

- Distinctive Ringing

  With Distinctive Ringing, you can administer the relationship between the number of ring bursts and the call type. The Personal Ringing Pattern that you select is the same ringing pattern that is used in the Distinctive Ringing cycles.

PIN Checking for Private Calls

Use the PIN Checking for Private Calls feature to include three new Feature Access Codes (FACs) providing General, ARS (External) and AAR (Internal) access codes.

For example:

- General operation: *11 12345 04069204130
- External operation: *12 12345 9 04069204130
- Internal operation: *13 12345 04069204130

Detailed description

The PIN Checking for Private Calls feature restricts users from making private calls (internal or external) by forcing them to enter a Personal Identification Number (PIN) code after dialing PIN Feature Access Code. When the PIN is valid, user can dial the destination digits to make a call. The PIN code used for the call is reported in Call Detail Record (CDR) output with a special character P.

The PIN code access feature works in the following way:

1. User dials new Feature Access Code (FAC) administered for this feature.
2. Confirmation tone is played if the FAC dialed by user is valid. On telephone sets supporting displays, user is prompted by message **ENTER PIN**.
3. After user dials an **Assigned PIN Code** and, if the code is accepted, then user gets recall dial tone on the telephone to enter destination digits. **ENTER NUMBER** message is displayed on telephones that support display.
4. When the feature is invoked by a display equipped DCP or H.323 IP telephone, a character * is displayed for each digit of the PIN code dialed.
5. After entering a destination number the private call can be routed.

Note:
This feature is available with Communication Manager Release 5.2 and later only. This feature does not support IP (SIP) telephones at present.

Three examples of Feature Access Codes

1. PIN Checking for Private Calls Access Code: *11
2. PIN Checking for Private Calls Using ARS Access Code: *12

3. PIN Checking for Private Calls Using AAR Access Code: *13

   – To make outgoing calls from the telephone user needs to follow the following order of using PIN Checking for Private Calls Access Code:

PIN_FAC + PIN_CODE + Destination Digits

*11 + 12345 + 36001

The above Access Code can only be used for internal calls.

   – To make external (trunk) calls user needs to use ARS/AAR Access Codes, as shown here:

PIN_FAC + PIN_CODE + Destination Digits

*12 + 12345 + 5400103

PIN_FAC + PIN_CODE + Destination Digits

*13 + 12345 + 5400103

PIN Codes

This feature reuses following functionality provided by Authorization code feature existing in Communication Manager.

1. **Using authorization code, COR assigned to a station or trunk can be overridden**

Each authorization code is assigned a Class of Restriction (COR). When user dials an authorization code, the COR that is assigned to the extension, the attendant console, the incoming trunk group, or the remote access trunk group that is in use for the call is replaced by the COR assigned to the authorization code. The COR that is assigned to the authorization code functions in the same way as the original COR. However, the new COR that is assigned to the authorization code might represent greater or lesser calling privileges than the original COR. All the parameters on COR screen are applicable to COR assigned to the Authorization code. Access to any given facility depends on the restrictions that are associated with the FRL of the authorization code.

PINs used for this new feature are stored in the same table used by authorization codes. So a PIN has the same COR mapping as authorization codes. See Figure 337 on how PINs are administered on the same screen as Authorization codes. There is no way looking at the administration to distinguish whether particular entry is a PIN or an Auth Code. So, if user is assigned with some Auth Code then it can be used instead of a PIN.

Figure 337: Authorization Code Screen

```
 change authorization-code 1234567                              Page 1 of 1
                 Authorization Code - COR Mapping
        NOTE: 1      codes administered. Use 'list' to display all codes

      AC       COR         AC       COR         AC       COR         AC       COR
1234567        1
2345678        2
```

Figure 337 shows administration of a PIN ‘1234567’and an Auth Code ‘2345678’ in same screen. There is no way to distinguish that 1234567 is a PIN and 2345678 is an Auth Code. 2345678 can also be used as a PIN if the COR assigned to that is administered with proper privileges.

2. **Authorization codes length is within 4-13 digit range**

   You can enable the Authorization code feature on System Parameters Customer-Options screen. You can configure the parameters for an Authorization code on Feature-Related System Parameters screen. For this feature the length of the Authorization code administered on Feature-Related System Parameters screen decides the length of PIN codes. Other fields on system-parameters features screen like, **Authorization Code Cancellation**, **Attendant Time Out Flag**, and **Display Authorization Code** are not applicable to PIN codes and this feature.

   For security reasons, Communication Manager software requires that authorization codes must consist of 4 to 13 digits. The number of digits in the codes must be a fixed length for a particular server that is running Communication Manager. You can lengthen the authorization code without deleting and reentering the old codes but you cannot shorten the length unless you delete and reenter the old codes. All authorization codes that are used in the system must be the same length. PINs assigned to users for making private calls are of the same length as authorization codes.

Figure 338: System Parameters Features Screen

```
 display system-parameters features                          Page 4 of 17
                        FEATURE-RELATED SYSTEM PARAMETERS
          Reserved Slots for Attendant Priority Queue: 5
                           Time before Off-hook Alert: 10
               Emergency Access Redirection Extension:
 Number of Emergency Calls Allowed in Attendant Queue: 5
 Maximum Number of Digits for Directed Group Call Pickup:4
               Call Pickup on Intercom Calls? y         Call Pickup Alerting? n
 Temporary Bridged Appearance on Call Pickup? y         Directed Call Pickup? n
                   Extended Group Call Pickup: none

  Deluxe Paging and Call Park Timeout to Originator? n
 Controlled Outward Restriction Intercept Treatment: tone
Controlled Termination Restriction (Do Not Disturb): tone
          Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS          Authorization Code Enabled? y
                                        Authorization Code Length: 7
                             Authorization Code Cancellation Symbol: #
                                          Attendant Time Out Flag? n
                                       Display Authorization Code? y
               Controlled Toll Restriction Replaces: none
```

1. In the **Authorization Code Enabled** field, type **y**.
   This enables the Authorization Codes feature on a system-wide basis.
2. In the **Authorization Code Length** field, type **7**.
   This defines the length of the Authorization Codes users need to enter. To maximize the security of user's system, Avaya recommends making each authorization code the maximum length allowed by the system.
3. In the **Authorization Code Cancellation Symbol** field, leave the default of **#**.
   This is the symbol a caller must dial to cancel the 10-second wait period during which user can enter an authorization code.
4. In the **Attendant Time Out Flag** field, leave the default of **n**.
   This means a call is not to be routed to the attendant if a caller does not dial an authorization code within 10 seconds or dials an invalid authorization code.
5. In the **Display Authorization Code** field, type **n**.
   This prevents the authorization code from displaying on telephone sets thus maximizing security.
6. Press **Enter** to save changes.

Note:
These commands are available only when enabled in the Feature Access Codes screen, as shown in Figure 338.

Feature Access Code screen

Figure 339: Feature Access Codes

```
display feature-access-codes                                  Page 3 of x
                              FEATURE ACCESS CODE (FAC)
             Leave Word Calling Send A Message:
           Leave Word Calling Cancel A Message:
   Limit Number of Concurrent Calls Activation:        Deactivation:
              Malicious Call Trace Activation:        Deactivation:
         Meet-me Conference Access Code Change:

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code: *50    Dissociate Code: #50
        Per Call CPN Blocking Code Access Code:
      Per Call CPN Unblocking Code Access Code:
          PIN Checking for Private Calls Access Code:*11
PIN Checking for Private Calls Using AAR Access Code:*12
PIN Checking for Private Calls Using ARS Access Code:*13
                  Priority Calling Access Code: *66
                           Program Access Code:

       Refresh Terminal Parameters Access Code:
              Remote Send All Calls Activation:        Deactivation:
```

When the Authorization code feature is enabled on the system-parameters features screen, then the feature-access-codes screen displays the three additional fields, as shown in Figure 339.

- **PIN Checking for Private Calls Access Code**
- **PIN Checking for Private Calls Using AAR Access Code**
- **PIN Checking for Private Calls Using ARS Access Code**

Note:

These three fields appears only when the feature is enabled through system-parameters features. If the feature is not enabled, the three fields remain hidden. PIN FACs for example, **11/*12/*13* are visible only when the feature **PIN Checking for Private Calls** is activated in Figure 340.

System parameters screen

Figure 340: PIN Checking for Private Calls - Feature Activation

```
change system-parameters features                              Page 18 of x
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS

                    Direct IP-IP Audio Connections? y
                              IP Audio Hairpinning? n
                           Synchronization over IP? n
CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                   Call Pickup on Intercom Calls? y     Call Pickup Alerting? y
     Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? y
                       Extended Group Call Pickup: simple
                   Enhanced Call Pickup Alerting? y
 Enhanced Call Pickup Delay Timer (sec.) Display: 3   Audible Notifications: 6

                         Display Information with Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? n
               PIN Checking for Private Calls? y
```

You can set the **PIN Checking for Private Calls** field on system-parameters features screen to **y** to enable the feature, as shown in Figure 340.

PIN Checking for Private Calls?

Field description

Valid entries	Usage
y/n	To enable PIN Checking for Private Calls select **y**. To disable the feature select **n**. The default value is **n**.

Feature interactions

Call Detail Recording

The three new Feature Access Codes (FAC) for **`PIN Checking For Private Calls Access Codes`** with AAR and ARS, and the **`PIN Checking For Private Calls`** are stored along with the PIN Code in the Call Detail Record. Also, a condition code “P” is added to distinguish call dialed using PIN FAC calls. The Call Detail Recording feature reuses the code-dial field. This field stores the ARS FAC, AAR FAC, or TAC. This feature replaces these FACs with the PIN FAC.

Port Network Recovery from Control Network Outages

When network fails, IP-connected port networks experience disproportionately long outages from short network disruptions. This feature now provides you using IP connected Port Networks with less downtime in the face of IP network failures.

When there is a network outage, Port Networks do a warm restart rather than a reset to allow faster recovery of service.

The feature also monitors the IPSI-PCD socket in identifying and troubleshooting network related problems.

Detailed description

Improved Port Network Recovery from Control Network Outages

When network fail, IP-connected port networks experience disproportionately long outages from short network disruptions. The enhanced feature now provides you using IP connected Port Networks with less downtime in the face of IP network failures.

The feature lessens the impact of network failures by:

- Improving TCP recovery times that increase the IPSI-PCD socket bounce coverage time from the current 6-8 seconds range for the actual network outage to something closer to 10 seconds. Results vary based on traffic rates.
- Modifying the PKTINT recovery action after a network outage to entail a warm interrupt rather than a **PKTINT application reset** (hardware interrupt)). This prevents H.323 IP telephones from having to re-register and/or have their sockets regenerated. This minimizes recovery time from network outages in the range of 15-60 seconds.

This feature also monitors the IPSI-PCD socket and helps in identifying and troubleshooting network related problems.

The IPSI-PCD socket bounce is developed by improving TCP recovery time that covers typical network outages, up to 10-11 seconds range. In this scenario, uplink and downlink messages are buffered, and operations very quickly return to normal after a network failure. In order to improve recovery time for longer outages, up to the 60 seconds range, the feature introduces the use of a PKTINT warm interrupt rather than a reset. This results in less drastic action being taken to recover links and H.323 IP telephones.

During the network outage, only stable calls already in progress have their bearer connections preserved. A call for which the talk path between the parties in the call has been established is considered stable. Call control is not available during the network outage, and this means that any call in a changing state is most likely not preserved.

Some examples are:

- Calls with dial tone
- Calls in dialing stage
- Calls in ringing stage
- Calls transitioning to/from announcements
- Calls transitioning to/from music-on-hold
- Calls on hold
- Calls in ACD queues
- Calls in vector processing

Further, no change in the state of a preserved call is possible. So, features such as conference or transfer are not available on the preserved calls. Button pushes are not recognized. Invocation of a feature by the user is given denial treatment. In a conference call, if a party in the call drops, the entire call is dropped.

The following are additional improvements:

- Improve TCP Recovery Time
- Increase IPSI Local Buffering to prevent data loss
- Reduce escalation impact between 15 and 60 seconds by using warm interrupt of PKTINT instead of **PKTINT application reset** (hardware interrupt)
- Reduce escalation impact between 60 and 90 seconds by extending PN cold reset action from 60 seconds to 90 seconds
- Reduce ESS **No Service Timer** minimum value from 3 minutes to 2 minutes to reduce your outage in case of prolonged network outage
- List measurements for the PCD-PKTINT socket for improved troubleshooting

With the introduction of a warm interrupt of the PKTINT instead of reset in the 15-60 seconds range, and the optional extension of the PN cold reset from 60 to 120 seconds.

For more information on System parameters screen, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Configuration impacts on availability

Communication Manager reduces the downtime experienced by port networks after a short network outage. H.323 endpoint and application link and socket stability is greatly improved in the sub-60 second range. H.323 endpoints using TTS will not have to regenerate sockets, and H.323 endpoints not using TTS will not have to re-register or have their sockets regenerated.

Survivability

Reducing the minimum ESS No Service Time Out Interval from 3 to 2 minutes improves your overall availability.

Posted Messages

Use the Posted Messages feature to provide callers with a displayed message on the telephone that states why the user is unavailable to take a call.

Detailed description of Posted Messages

This section provides a detailed description of the Posted Messages feature.

The Posted Messages feature is available with Communication Manager Release 1.3 (V11) or later.

A user activates the Posted Messages feature to post a message to his or her telephone. When a person calls that user, the telephone display of the caller shows the posted message for 4 seconds. During those 4 seconds, no incoming alert can appear on the telephone of the caller. After 4 seconds, the telephone display of the caller reverts back to the normal called number and called name.

To use the Posted Messages feature, the telephone of the caller must be able to display messages. Only internal callers can post or view a posted message. Callers from outside your system cannot view a posted message.

Language options

Five languages are available for the Posted Messages feature:

- English
- Italian
- French
- Spanish
- A user-defined language

The 15 fixed messages and the feature button labels are available in English, with predefined Italian, French, and Spanish translations. The administrator cannot change the text of the English, the Italian, the French, or the Spanish fixed messages or feature button labels.

The administrator can translate the fixed messages and feature button labels into a user-defined language. This translation can be any other language that you choose, such as German. The administrator can use only one user-defined language throughout the system.

You can administer the 15 custom messages in English, Italian, French, Spanish, and the user-defined language. The number of available messages equals the number of fixed messages (15), plus the number of custom messages that you administer for each language.

Language translation is automatically achieved between telephones and between systems.For example, telephone A uses English and telephone B uses Italian. User A posts the message "In Meeting." User B calls user A and sees the message "In Riunione" in Italian. If the custom messages are properly administered, the same is true for custom messages.

Messages

User can choose from up to 30 different messages. Of these 30 messages, 15 are *fixed* messages, and 15 are *custom* messages. Each message has a corresponding message number.

While a user selects a Posted Message, his or her telephone is said to be in *selection display mode*. Once the user posts a message, his or her telephone is said to be in *message posting mode*. The message appears on the telephone display of the user. The display of the selected message on the telephone is a visual reminder to the user. The display also indicates the availability of the user to people who might walk into the office.

Telephones that are in message posting mode use a special dial tone when the telephone goes off hook. This special dial tone provides audio feedback to the user. On telephones without a display, this special dial tone is the only indication that the telephone is in message posting mode.

The telephone of the user displays the selected message until:

- The user or someone else deactivates the posted message on the telephone of the user.
- The system resets.If the system resets, the posted message no longer appears on the telephone of the user.

Fixed messages

The numbers for the fixed messages are predefined. You cannot change the numbers or the messages. The following table shows the 15 fixed messages.

Number	Message
01	In Meeting
02	Out To Lunch
03	Away From Desk
04	Do Not Disturb

Number	Message
05	Out All Day
06	On Vacation
07	Gone For The Day
08	Out Sick
09	On Business Trip
10	With Client
11	Working From Home
12	On Leave
13	Back In 5 Minutes
14	Back In 30 Minutes
15	Back In 1 Hour

Note that the Do Not Disturb posted message is independent of the Do Not Disturb feature. Activating or deactivating the Do Not Disturb posted message has no impact on the Do Not Disturb feature.

Custom messages

If you choose to add custom messages, you must start with number 16 and continue in numeric order. Custom messages are specific to each local system. Custom messages in any language cannot exceed 28 characters.

QSIG support

If your system supports QSIG functionality, you can use QSIG to send fixed messages and custom messages to users on other systems. QSIG is a global signaling and control standard for use in private corporate ISDN networks.

The 15 fixed messages are automatically routed to other systems through QSIG. If you want to send custom messages to users on other systems through QSIG, you must:

- Activate QSIG support
- Create the same custom messages on all systems.

  If you do not administer custom messages on the system of the caller, a message does not appear on the telephone display of the caller.

Custom messages must be consistent for all systems and for all translations. The reason is that Posted Messages sends the message number, not the message, to the caller. The system of the caller converts the Posted Messages number into a message.

For example, custom message number 16 on system A is "On Conference Call" and custom message number 16 on system B is "Talking to Boss." If a user on system A posts custom message #16, "On Conference Call" appears on the telephone display of the user. If someone on system B calls the user on system A, Posted Messages sends message number 16 to the caller. The system of the caller converts number 16 into a message. "Talking to Boss" appears on the telephone display of the caller.

Inconsistent administration on custom messages can display unintended results. The system might not display the intended message.

Administering Posted Messages

The following steps are part of the administration process for the Posted Messages feature:

- Defining a Feature Access Code
- Requiring a security code
- Activating QSIG to send custom messages
- Translating Posted Messages
- Translating telephone feature buttons and labels

This section describes:

- Any prerequisites for administering the Posted Messages feature
- The screens that you use to administer the Posted Messages feature
- Complete administration procedures for the Posted Messages feature

Prerequisites for administering Posted Messages

You must complete the following actions before you can administer the Posted Messages feature:

- On the Optional Features screen, ensure that the **G3 Version** field is set to **V11** or later. If this field is not set to **V11** or later, your system is not enabled for the Posted Messages feature. Contact your Avaya representative before you continue with this feature.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

- Click **Next** until you see the **ISDN-BRI Trunks** and the **ISDN-PRI** fields. Ensure that at least one of these fields are set to **y**, depending on what type of trunk you use. These fields indicate that your system can support QSIG to send and receive Posted Messages. Your license file sets the values in the **ISDN-BRI Trunks** and **ISDN-PRI** fields. You cannot manually change these values. If both fields are set to **n**, contact your Avaya representative.
- Click **Next** until you see the **Posted Messages** field. Ensure that the **Posted Messages** field is set to **y**. Your license file sets the value in the **Posted Messages** field. You cannot manually change this value. If the **Posted Messages** field on the Optional Features screen is set to **n**, contact your Avaya representative.
- Click **Next** until you see the QSIG Optional Features screen. Ensure that the following fields are set to **y**:
  - **Basic Call Setup**
  - **Basic Supplementary Services**
  - **Value-Added (VALU)**

  These fields indicate whether your system can support QSIG to send and receive Posted Messages. Your license file sets the values in these fields. You cannot manually change these values. If any of these fields are set to **n**, contact your Avaya representative before you continue with this procedure.

Screens for administering Posted Messages

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 1.3 (V11) or later.	**G3 Version**
	Ensure that your system supports QSIG functionality.	• **ISDN-BRI Trunks** • **ISDN-PRI**
	Ensure that the Posted Messages feature is on.	**Posted Messages**
QSIG Optional Features	Ensure that your system supports QSIG functionality.	• **Basic Call Setup** • **Basic Supplementary Services** • **Value-Added (VALU)**
Feature Access Code (FAC)	Set up a FAC for users to activate and deactivate the Posted Messages feature.	• **Posted Messages Activation** • **Deactivation**

Screen name	Purpose	Fields
Feature-Related System Parameters	Activate QSIG to send custom messages to people on other systems.	**Send Custom Messages Through QSIG**
	Indicate if users who use a FAC must enter a security code. To activate or deactivate Posted Messages.	**Require Security Code**
Station	Set up a security code for the telephone of a user.	**Security Code**
System Posted Messages	Review the 15 fixed messages and, if needed, translate the messages to a user-defined language.	All
Custom Posted Messages	Create or edit up to 15 custom messages in English, Italian, French, Spanish, or a user-defined language.	All
Language Translations	If needed, change the translation of the Posted Messages feature display to a user-defined language.	**Posted Messages**
	If needed, change the translation of the Posted Messages softkey label to a user-defined language.	**PoMsg**
	If needed, change the translation of the Posted Messages button label on the 2420 telephone or the 4620 telephone to a user-defined language.	**Posted MSGs**

Defining a Feature Access Code

To define the two Feature Access Codes (FACs) to activate and deactivate the Posted Messages feature:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Click **Next** until you see the **Posted Messages Activation** field (Figure 341: Feature Access Code (FAC) screen on page 1351).

Figure 341: Feature Access Code (FAC) screen

```
change feature-access-codes                                          Page 3 of 8

                          FEATURE ACCESS CODE (FAC)

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:        Dissociate Code:
        Per Call CPN Blocking Code Access Code:
     Per Call CPN Unblocking Code Access Code:
                  Posted Messages Activation: *29       Deactivation: #29
                Priority Calling Access Code:
                         Program Access Code:
      Refresh Terminal Parameters Access Code:
             Remote Send All Calls Activation:           Deactivation:
              Self Station Display Activation:
                    Send All Calls Activation:           Deactivation:
        Station Firmware Download Access Code:
                     Station Lock Activation:           Deactivation:
     Station Security Code Change Access Code:
             Station User Admin of FBI Assign:                 Remove:
  Station User Button Ring Control Access Code:
            Terminal Dial-Up Test Access Code:
```

3. In the **Posted Messages Activation** field, type a FAC to activate Posted Messages.
4. In the **Deactivation** field, type a FAC to deactivate Posted Messages.
5. Press **Enter** to save your changes.

Requiring a security code

An administrator can require a security code when users use a FAC to activate or deactivate Posted Messages. The requirement for the security code applies to all users. This procedure is optional.

To require users to enter a security code when the users use a FAC to activate or deactivate Posted Messages, complete the following procedures:

- Setting up a security code for the telephone of a user
- Activating the Posted Messages security code

Setting up a security code for the telephone of a user

To set up a security code for the telephone of a user:

1. Type **change station *n***, where ***n*** is the telephone extension of the user. Press **Enter**.

   The system displays the Station screen (Figure 342: Station screen on page 1352).

Figure 342: Station screen

```
change station 1234567                                        Page 1 of 3

                                    STATION

Extension: 1234567                      Lock Messages? n            BCC: 0
     Type: 4606                         Security Code: 86562563      TN: 1
     Port: S00014                  Coverage Path 1:                  COR: 1
     Name: MG IP phone 4606        Coverage Path 2:                  COS: 1
                                   Hunt-to Station:

STATION OPTIONS
              Loss Group: 19           Personalized Ringing Pattern: 1
                                                  Message Lamp Ext: 1234567
           Speakerphone: 2-way                 Mute Button Enabled: y
        Display Language: english
```

2. In the **Security Code** field, type a security code for this telephone.

   The security code can be up to eight digits.
3. Press **Enter** to save your changes.
4. Be sure to share this security code with the user.

Activating the Posted Messages security code

To activate the Posted Messages security code:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.
2. Click **Next** until you see the **Posted Message** area (Figure 343: Feature-Related System Parameters screen on page 1353).

Figure 343: Feature-Related System Parameters screen

```
change system-parameters features                                Page 6 of 12

                          FEATURE-RELATED SYSTEM PARAMETERS

CONFERENCE/TRANSFER

               Abort Transfer? n                  No Dial Tone Conferencing? n
        Transfer Upon Hang-Up? n         Select Line Appearance Conferencing? n
Abort Conference Upon Hang-Up? n                                    Unhold? n
   No Hold Conference Timeout: 60

ANALOG BUSY AUTO CALLBACK
                Without Flash? n


AUDIX ONE-STEP RECORDING
                            Recording Delay Timer (msec): 500
Apply Ready Indication Tone To Which Parties In The Call? all
  Interval For Applying Periodic Alerting Tone (seconds): 15

POSTED MESSAGE
        Require Security Code? y
```

3. Change the **Require Security Code** field to **y**.

   This field appears only if the **Posted Messages** field on the Optional Features screen is set to **y**.

4. Press **Enter** to save your changes.

Activating QSIG to send custom messages

To activate QSIG to send custom messages to users on other systems:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **ISDN Parameters** area (Figure 344: Feature-Related System Parameters screen on page 1354).

Figure 344: Feature-Related System Parameters screen

```
change system-parameters features                                Page7 of 12
                        FEATURE-RELATED SYSTEM PARAMETERS

ISDN PARAMETERS

 Send Non-ISDN Trunk Group Name as Connected Name? n
 Display Connected Name/Number for ISDN DCS Calls? n
       Send ISDN Trunk Group Name on Tandem Calls? n
                 Send Custom Messages Through QSIG? y

                                 QSIG TSC Extension: 6999
 MWI - Number of Digits Per Voice Mail Subscriber: 4

                               National CPN Prefix:
                        International CPN Prefix:
                       Pass Prefixed CPN to ASAI? n
    Unknown Numbers Considered Internal for AUDIX? n
              USNI Calling Name for Outgoing Calls? n
                 Path Replacement with Measurements? y
                    QSIG Path Replacement Extension:
             Path Replace While in Queue/Vectoring? n
```

3. Change the **Send Custom Messages Through QSIG** field to **y**.
4. Press **Enter** to save your changes.

Translating Posted Messages

Translating any fixed or custom message to a user-defined language is optional.

To translate Posted Messages, complete the following procedures:

- Translating fixed messages to a user-defined language
- Creating custom messages

Translating fixed messages to a user-defined language

Fixed messages are available in English, Italian, French, and Spanish. If you want to translate fixed messages into another language, called a user-defined language, complete the following procedure.

To translate fixed messages to a user-defined language:

1. Type **change display-messages posted-message**. Press **Enter**.

   The system displays the System Posted Messages screen (Figure 345: System Posted Messages screen on page 1355).

Figure 345: System Posted Messages screen

```
change display-messages posted-message                          Page 1 of 6

                            SYSTEM POSTED MESSAGES
                       USER DEFINED LANGUAGE TRANSLATIONS

Message  English                        Message  Translation
Number                                  Number
 1.      In Meeting                      1.      ****************************
 2.      Out to Lunch                    2.      ****************************
 3.      Away from Desk                  3.      ****************************
 4.      Do Not Disturb                  4.      ****************************
 5.      Out All Day                     5.      ****************************
 6.      On Vacation                     6.      ****************************
 7.      Gone for the Day                7.      ****************************
 8.      Out Sick                        8.      ****************************
 9.      On Business Trip                9.      ****************************
10.      With Client                    10.      ****************************
11.      Working from Home              11.      ****************************
12.      On Leave                       12.      ****************************
13.      Back in 5 Minutes              13.      ****************************
14.      Back in 30 Minutes             14.      ****************************
15.      Back in 1 Hour                 15.      ****************************
```

2. In the **Translation** fields, type a translation of all fixed messages into the user-defined language.

   Note that the text for the English, the Italian, the French, and the Spanish fixed messages are predefined. You cannot change the text of these translations.

3. Press **Enter** to save your changes.

Creating custom messages

To create custom messages:

1. Type **change display-messages posted-message**. Press **Enter**.

   The system displays the System Posted Messages screen.

2. Click **Next**.

   The system displays the Custom Posted Messages screen for English translations (Figure 346: Custom Posted Messages screen on page 1357).

   The system displays the five Custom Posted Messages screens in the following order:

   - English translations
   - Italian translations
   - French translations
   - Spanish translations
   - User-defined language translations

   In this example, we describe how to create custom messages in English. Use the same instructions to create custom messages in Italian, in French, in Spanish, or in the user-defined language. Ensure that you view the correct screen for the language that you want to use.

   If you first administer custom messages in English, the text of the English custom messages automatically appears on the:

   - Italian translations screen
   - French translations screen
   - Spanish translations screen
   - user-defined language translations screen

Figure 346: Custom Posted Messages screen

```
change display-messages posted-message                          Page 2 of 6

                            CUSTOM POSTED MESSAGES
                             ENGLISH TRANSLATIONS

                                      Message  Translation
                                      Number
                                      16.      ****************************
                                      17.      ****************************
                                      18.      ****************************
                                      19.      ****************************
                                      20.      ****************************
                                      21.      ****************************
                                      22.      ****************************
                                      23.      ****************************
                                      24.      ****************************
                                      25.      ****************************
                                      26.      ****************************
                                      27.      ****************************
                                      28.      ****************************
                                      29.      ****************************
                                      30.      ****************************
```

3. In the **Translation** fields, start with message 16 and type the message in the proper language that you want to create.
4. Continue in numeric order until you create all the custom messages that you want. The maximum number of custom messages is 15.
5. Press **Enter** to save your changes.

Translating telephone feature buttons and labels

This procedure is optional.

To translate telephone feature buttons and labels for Posted Messages to a user-defined language, complete the following procedures:

- Translating the Posted Messages feature display to a user-defined language
- Translating the Posted Messages softkey button label to a user-defined language
- Translating the Posted Messages button label to a user-defined language

Translating the Posted Messages feature display to a user-defined language

To translate the text that appears on the telephone display, when this feature is active, to a user-defined language:

1. Type **change display-messages view-buttons**. Press **Enter**.

   The system displays the Language Translations screen.

2. Click **Next** until you see the **Posted Messages** field (Figure 347: Language Translations screen on page 1358).

Figure 347: Language Translations screen

```
change display-messages view-buttons                          Page 9 of 9

                          LANGUAGE TRANSLATIONS

English                                Translation

1.  Station Lock                       ****************************
2.  License Error                      ****************************
3.  Conference Display                 ****************************
4.  Conf/Trans Toggle-Swap             ****************************
5.  Posted Messages                    ****************************
```

3. In the **Translation** fields, type a translated name for **Posted Messages** into the user-defined language.

   Note that the language translations for the English, the Italian, the French, and the Spanish feature display are predefined. You cannot change the text of these translations.

4. Press **Enter** to save your changes.

Translating the Posted Messages softkey button label to a user-defined language

To translate the Posted Messages softkey button label to a user-defined language:

1. Type **change display-messages softkey-labels**. Press **Enter**.

   The system displays the Language Translations screen (Figure 348: Language Translations screen on page 1359).

Figure 348: Language Translations screen

```
change display-messages softkey-labels                          Page 9 of 9
                            LANGUAGE TRANSLATIONS

English      Translation English      Translation English      Translation
 1. Acct      1. *****   17. Drop     17. *****   33. SAC      33. *****
 2. AD        2. *****   18. Excl     18. *****   34. SFunc    34. *****
 3. AdBsy     3. *****   19. GrpPg    19. *****   35. Spres    35. *****
 4. Admin     4. *****   20. HFAns    20. *****   36. Stats    36. *****
 5. AutCB     5. *****   21. IAuto    21. *****   37. Stop     37. *****
 6. BtnVu     6. *****   22. IDial    22. *****   38. Swap     38. *****
 7. CFrwd     7. *****   23. Inspt    23. *****   39. Timer    39. *****
 8. CnfDs     8. *****   24. Last     24. *****   40. TmDay    40. *****
 9. CnLWC     9. *****   25. LWC      25. *****   41. View     41. *****
10. Cnslt    10. *****   26. Mark     26. *****   42. Wait     42. *****
11. Count    11. *****   27. Pause    27. *****   43. WspAn    43. *****
12. CPark    12. *****   28. PCall    28. *****   44. WspPg    44. *****
13. CPkUp    13. *****   29. PoMsg    29. *****
14. CTime    14. *****   30. Prog     30. *****
15. Dir      15. *****   31. RmBsy    31. *****
16. DPkUp    16. *****   32. RngOf    32. *****
```

2. Locate the **PoMsg** field.
3. In the **Translation** fields, type a translated name for the **PoMsg** softkey button label in the user-defined language. You are limited to five spaces for this translation.

   Note that the language translations for the English, the Italian, the French, and the Spanish softkey button labels are predefined. You cannot change the text of these translations.
4. Press **Enter** to save your changes.

Translating the Posted Messages button label to a user-defined language

The 2420 DCP telephone and the 4620 IP telephone have digital button labels instead of paper labels. If you need to translate the Posted Messages button labels into a user-defined language for these telephones, follow this procedure.

To translate the Posted Messages button label for the 2420 DCP telephone and the 4620 IP telephone to a user-defined language:

1. Type **`change display-messages button-labels`**. Press **Enter**.

   The system displays the Language Translations screen.
2. Click **Next** until you see the **Posted MSGs** field (Figure 349: Language Translations screen on page 1360).

Figure 349: Language Translations screen

```
change display-messages button-labels                          Page 9 of 9

                            LANGUAGE TRANSLATIONS

English                                 Translation
 1. NoAnsAlrt                            1. **********
 2. OffBoardAlarm                        2. **********
 3. PMS Failure                          3. **********
 4. PMS Ptr Alarm                        4. **********
 5. Posted MSGs                          5. **********
 6. Priority Call                        6. **********
 7. QueueCall                            7. **********
 8. QueueTime                            8. **********
 9. Release                              9. **********
10. RemBusyInd                          10. **********
11. ResetAlert                          11. **********
12. Ringer Off                          12. **********
13. Ring Stat                           13. **********
14. RSVN Halt                           14. **********
15. SD                                  15. **
16. SendAllCalls                        16. **********
```

3. In the **Translation** field, type a translated name for the **Posted MSGs** button label into the user-defined language.

   Note that the language translations for the English, the Italian, the French, and the Spanish button labels are predefined. You cannot change the text of these translations.

4. Press **Enter** to save your changes.

End-user procedures for Posted Messages

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Posted Messages:

To activate and deactivate the Posted Messages feature, users can either:

- Dial a Feature Access Code (FAC)
- Press a feature button on the telephone

Users can dial the FAC from:

- Their own telephone
- Another telephone on the same system

- A remote access trunk

A user can dial the Posted Messages FAC from another telephone on the same system, and have the message post on their own telephone. Users must press the feature button on their own telephone to activate or deactivate the Posted Messages feature.

To use a FAC to post a message, users might also have to dial the security code for their telephone. The administrator sets up the system to either require or not require a security code. Ask your administrator if you must dial a security code, and what might be the security code for your telephone.

You cannot use the Posted Messages feature from an attendant console. However, you can the Posted Messages FACs to activate or deactivate this feature for other telephones from an attendant console.

Activating the Posted Messages feature

To activate the Posted Messages feature, the user can complete the following procedures:

- Using a Feature Access Code
- Using the Posted Messages feature button

Using a Feature Access Code

To use a Feature Access Code (FAC) to post a message:

1. Dial the FAC for Posted Messages activation.

   You hear dial tone.

2. Identify your extension:
   - If you dial from your own telephone, press the pound key (#).
   - If you dial from another internal telephone or a remote access trunk, dial your telephone extension. Then press the pound key (#).
3. Identify the security code for your telephone:
   - If you do not have to dial a security code, press the pound key (#).
   - If you have to dial a security code, dial the security code for your telephone. Then press the pound key (#).

     If an error occurs, you hear intercept tone. Press the star key (*) to clear the extension and security code. Repeat from Step 2. If you do not hear intercept tone, continue with Step 4.
4. Dial the 2 digit number of the message that you want to post. Press the pound key (#).

   You hear confirmation tone. The system posts the message to the telephone display after 1 second as long as the:

- Telephone does not receive an incoming call
- User does not press any other button on the telephone

Examples

You want to post a message to your telephone. For the following examples:

- The activation FAC is ***29**.
- Your telephone extension is **1234567**.
- The security code for your telephone, if needed, is **86562563**.
- The message that you want to post to your telephone is message **02**, Out To Lunch.

From	Dial
Your own telephone that requires a security code	***29#86562563#02#**
Your own telephone that does not require a security code	***29##02#**
Another telephone that requires a security code,	***291234567#86562563#02#**
Another telephone that does not require a security code,	***291234567##02#**

Using the Posted Messages feature button

To use the feature button on your telephone to post a message:

1. Press the Posted Messages feature button.

   You can use this method to post a message only to your own telephone.

2. Use of the following methods to select the message that you want to post:
   - Press the Posted Messages feature button to scroll through the available messages. Whenever you press the feature button, the next message appears. To select the message that you want to post, press the pound key (#).
   - Dial the 2 digit number of the message that you want to post. Press the pound key (#).

   You hear confirmation tone. The system posts the message to the telephone display after 1 second as long as the:
   - Telephone does not receive an incoming call
   - User does not press any other button on the telephone

Deactivating the Posted Messages feature

To deactivate the Posted Messages feature, the user can complete the either of following procedures:

- Using a Feature Access Code
- Using the Posted Messages feature button

Using a Feature Access Code

To use a Feature Access Code (FAC) to cancel the Posted Message feature:

1. Dial the FAC for Posted Messages deactivation.
2. Identify your extension:
   - If you dial from your own telephone, just press the pound key (#).
   - If you dial from another internal telephone or a remote access trunk, dial your telephone extension. Then press the pound key (#).
3. Identify the security code for your telephone as follows:
   - If you do not have to dial a security code, press the pound key (#).
   - If you do have to dial a security code, dial the security code for your telephone. Then press the pound key (#).

     If an error occurs, you hear intercept tone. Press the star key (*) to clear the extension and security code. Repeat from Step 2.

     If there is no error, you hear confirmation tone. The telephone returns to the normal mode. The system clears the selected message.

Examples

You want to remove the posted message from your telephone. For the following examples:

- The deactivation FAC is **#29**.
- Your telephone extension is **1234567**.
- The security code for your telephone, if needed, is **86562563**.

From	Dial
Your own telephone that requires a security code	**#29#86562563#**
Your own telephone that does not require a security code	**#29##**

From	Dial
Another telephone that requires a security code,	**#291234567#86562563#**
Another telephone that does not require a security code,	**#291234567##**

Using the Posted Messages feature button

To use the feature button on your telephone to cancel the Posted Message feature:

1. Press the Posted Messages feature button on your telephone.

   You can use this method to cancel a posted message only on your own telephone.

   You hear confirmation tone. The telephone returns to the normal mode. The system clears the selected message.

Considerations for Posted Messages

This section provides information about how the Posted Messages feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Posted Messages under all conditions.

- Performance impact

  Heavy use of the selection display mode might adversely affect system performance. Hardware buffers can overflow when you overuse telephone displays. Telephone hyperactivity checks are usually sufficient to control overuse of the display mode.

- Security

  When a user activates the Posted Messages feature from a remote access trunk, the user must log in as a remote user. When you log in as a remote user, you prevent unauthorized users from activating or deactivating this feature for telephones.

- Serviceability

  In the selection display mode, the telephone might go out of service if the user scrolls through the displays too quickly. Scrolling through the displays too quickly causes the telephone to be reset. Active calls are dropped. When a 2420, a 4620 or a 4630 telephone is out of service, the system clears the call log.

- Time out

  If no activity occurs within 60 seconds of the last action, the telephone automatically exits from the selection display mode. The following events occur:

  – The LED for the feature button goes out. Or on telephones with feature icons, the feature icon changes to the off state.

- The displayed message is cleared.
- The display of any active call is restored.

When the telephone is in the selection display mode, the timer is reset if a user presses:

- The feature button
- The **Next** button
- Any digit key

- Silent ringing

  While a telephone is in the message posting mode, the user hears a burst of ringing, and then the telephone rings silently. Silent ringing removes the ringing disturbance while the user can still answer the incoming call.

Interactions for Posted Messages

This section provides information about how the Posted Messages feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of Posted Messages in any feature configuration.

- Display mode interactions

  The system cancels the selection display mode if one of the following telephone display modes is activated.

  - Normal

    The normal mode displays call related information for the active call appearance. Depending on the type of call, this information can include the name and the number of the calling party or the called party.

    The elapsed time function can be invoked anytime that the display is in Normal mode. The elapsed time feature displays elapsed time in hours, minutes, and seconds.

  - Inspect

    The inspect mode displays call related information for an incoming call when the user is active on a different call appearance. You must reset the mode manually for each call.

  - Stored number

    The stored number mode displays one of the following numbers:

    - The last number that the user dialed
    - The number that is stored in an abbreviated dialing button
    - A number that is stored in an abbreviated dialing list

- A number that is assigned to a button that is administered by the Facility Busy Indication feature

– Date and time

The date and time mode displays the current date and the time of day.

– Integrated directory

The integrated directory mode turns off the touchtone signals. The integrated directory mode then allows a user to use the touchtone buttons to enter the name of a system user. After the user enters a name, the display shows the name and the extension.

Integrated directory mode can also use the Call-Disp button. The Call-Disp button automatically returns the call that the currently displayed message requested, or by the currently displayed name and extension.

– Message retrieval

The message retrieval mode retrieves messages for telephone users. If no messages are stored, the display shows NO MESSAGES. A user can retrieve messages even if the user is active on a call.

Message retrieval mode can use three additional buttons:

- The Next Message button retrieves the next message. When the telephone is in retrieval mode, the telephone displays END OF FILE, PUSH NEXT TO REPEAT.
- The Delete button deletes the message that is currently displayed.
- The Call-Disp button automatically returns the call that the currently displayed message requested, or by the currently displayed name and extension.

– Coverage message retrieval

The coverage message retrieval mode retrieves messages for users who have telephones without a display. You must administer retrieval permission for a user to retrieve messages from another user.

The user does not have to lift the handset to retrieve messages. The user can retrieve messages even if the user is active on a call. Coverage message retrieval mode can use three additional buttons:

- The Next Message button retrieves the next message. When the telephone is in retrieval mode, the telephone displays END OF FILE, PUSH NEXT TO REPEAT.
- The Delete button deletes the message that is currently displayed.
- The Call-Disp button automatically returns the call that the currently displayed message requested, or by the currently displayed name and extension.

- Diverted Calls

If a user diverts a call to a telephone that is in message posting mode, the calling party does not receive the posted message. For example,

– User A posts a message.

  - User B calls user C.
  - The system diverts the call through the Call Coverage or Call Forwarding feature to user A.
  - User B does not receive the posted message from user A.

- Group Extensions, Hunt Groups, Terminating Extension Groups (TEG), intercom groups

  The Posted Messages feature does not apply to calls generated from dialing a group extension. The group member remains available to receive calls, and the calling party does not see the posted message.

  The Posted Messages feature only applies when dialing the group member's own extension.

- No Hold Conference

  No Hold Conference allows a user to automatically conference another party while continuing the conversation on the existing call. The new party is automatically added to the existing call upon answer.

  If the No Hold Conference feature is in process, the user cannot use the Posted Messages feature. If the telephone is in selection display mode, the user cannot use the No Hold Conference feature.

- Personal Station Access/Terminal Translation Initialization (PSA/TTI)

  After PSA/TTI dissociation, the extension of the telephone becomes an X-port extension. If the Posted Messages feature was previously activated for the extension, the Posted Messages feature is deactivated.

  The permanent display for the Posted Messages feature has precedence over the permanent displays for the PSA enhancements feature:

  - if the Posted Messages feature and the Personal Station Access feature are both active
  - when the telephone is PSA-associated

- Transfer

  Under normal conditions, a posted message only appears to a calling party. A posted message does not appear to other parties to whom the call might later be transferred.

  A posted message appears to the telephones of all transferees if both these conditions apply:

  - if a user activates a posted message while the telephone is ringing
  - after the transfer operation is completed

Priority Calling

Use the Priority Calling feature to provide a special type of call alerting between internal telephone users, including the attendant. The called party hears a distinctive ringing when the calling party uses Priority Calling.

Detailed description of Priority Calling

This section provides a detailed description of the Priority Calling feature.

You enable Priority Calling for your system. The Class of Service (COS) that you assign to each user determines whether a user can use Priority Calling.

The following types of calls are always priority calls:

- Call coverage consult
- Automatic callback
- Ringback queuing
- Attendant intrusion
- Security violation notification (SVN)

The system assigns a three-burst ringing-pattern as the default for a Priority Calling call.

The system generates the call waiting ringback tone that a single-line telephone user hears, even if the user is active on a call.

In contrast, the system does not generate the call waiting ringback tone for a multiappearance telephone if no call appearances are idle. Instead, a caller with a multiappearance telephone hears busy tone. The system generates the call waiting ringback tone if the telephone has an idle call appearance, including the call appearance that is reserved for call origination.

Note:

The **VIP Caller** field that is assigned in the Class of Service screen enables automatic priority calling when assigned to the originator of the call. This field might automatically be set to **y** by the ProVision tool (or any other similar software tool) used by Avaya administration personnel. If stations are set to **y**, the call will not follow with coverage to voice mail.You must change the setting to the default **n** to ensure coverage to voice mail.

Administering Priority Calling

The following steps are part of the administration process for the Priority Calling feature:

- Assigning a priority feature button to an attendant console
- Assigning a priority feature button to a telephone

This section describes:

- Any prerequisites for administering the Priority Calling feature
- The screens that you use to administer the Priority Calling feature
- Complete administration procedures for the Priority Calling feature

Prerequisites for administering Priority Calling

You must complete the following actions before you can administer the Priority Calling feature:

- Administer the Feature-Related System Parameters screen to support the Priority Calling feature on your system.
- Create a Class of Service (COS) that allows your users to use Priority Calling.
- Ensure that a Feature Access Code (FAC) for Priority Calling is available on your system.

To administer the Feature-Related System Parameters screen to support the Priority Calling feature on your system:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **Distinctive Audible Alerting** area (Figure 350: Feature-Related System Parameters screen on page 1371).

Figure 350: Feature-Related System Parameters screen

```
display system-parameters features                              Page   5 of 14
                        FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5             Auto Start? n
   Conference Parties with Public Network Trunks: 6               Auto Hold? y
 Conference Parties without Public Network Trunks: 6          Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180         Bridging Tone? n
                  Short Interdigit Timer (seconds): 3        Conference Tone? n
               Unanswered DID Call Timer (seconds):           Intrusion Tone? n
               Line Intercept Tone Timer (seconds): 30     Special Dial Tone? n
                  Long Hold Recall Timer (seconds): 0    Mode Code Interface? y
                       Reset Shift Timer (seconds): 0
    Station Call Transfer Recall Timer (seconds): 0
                               DID Busy Treatment: tone
       Invalid Number Dialed Intercept Treatment: tone
              Allow AAR/ARS Access from DID/DIOD? n
                Allow ANI Restriction on AAR/ARS? n
     Use Trunk COR for Outgoing Trunk Disconnect? n
                 7405ND Numeric Terminal Display? n                  7434ND? y
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                         Attendant Originated Calls: external
   DTMF Tone Feedback Signal to VRU - Connection:          Disconnection:
```

3. In the **Priority** field in the **Distinctive Audible Alerting** area, type **priority** next to the number of rings that you want the system to use for a priority call.

   For virtual stations, the number of rings applies to the mapped-to physical telephone.

4. Press **Enter** to save your changes.

To create a Class of Service (COS) that allows your users to use the Priority Calling feature:

For more information about how to create a COS, see the "Class of Service" feature.

To ensure that a FAC for Priority Calling is available on your system:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Codes (FAC) screen.

2. Click **Next** until you see the **Priority Calling Access Code** field (Figure 351: Feature Access Code (FAC) screen on page 1372).

Figure 351: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page   3 of 7
                              FEATURE ACCESS CODE (FAC)

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code: *98    Dissociate Code: *99
        Per Call CPN Blocking Code Access Code:
     Per Call CPN Unblocking Code Access Code:
                   Posted Messages Activation:        Deactivation:
                Priority Calling Access Code: *76
                         Program Access Code:
      Refresh Terminal Parameters Access Code:
             Remote Send All Calls Activation:        Deactivation:
              Self Station Display Activation: *26
                    Send All Calls Activation:        Deactivation:
        Station Firmware Download Access Code: *36
                     Station Lock Activation:        Deactivation:
     Station Security Code Change Access Code: *47
             Station User Admin of FBI Assign:                  Remove:
  Station User Button Ring Control Access Code:
            Terminal Dial-Up Test Access Code:
```

3. Type the FAC that you want to use for Priority Calling. In this example, the FAC is *76.
4. Press **Enter** to save your changes.

   For more information, see the "Feature Access Code" feature.

Screens for administering Priority Calling

Screen name	Purpose	Fields
Attendant Console	Assign a **priority** feature button to an attendant console.	Any available button field in the **Feature Button Assignments** area
Class of Service	Define a COS that allows Priority Calling.	**Priority Calling**
Feature Access Code (FAC)	Define a FAC for Priority Calling.	**Priority Calling Access Code**

Screen name	Purpose	Fields
Feature-Related System Parameters	Assign the number of rings for a priority call.	**Distinctive Audible Alerting - Priority**
Station (multiappearance)	Assign a **priority** feature button for Priority Calling to a multiappearance telephone.	Any available button field in the **Button Assignments** area

Assigning a priority feature button to an attendant console

To assign a priority feature button to an attendant console:

1. Type **change attendant *n***, where ***n*** is the number of the attendant console to which you want to assign a priority feature button. Press **Enter**.

   The system displays the Attendant Console screen.

2. Click **Next** until you see the **Feature Button Assignments** area (Figure 352: Attendant Console screen on page 1373).

Figure 352: Attendant Console screen

```
change attendant 1                                          Page   3 of   4
                              ATTENDANT CONSOLE

FEATURE BUTTON ASSIGNMENTS

 1: split                                13:
 2:                                      14:
 3:                                      15:
 4:                                      16:
 5:                                      17:
 6: hold                                 18:
 7:                                      19: forced-rel
 8:                                      20:
 9:                                      21:
10:                                      22:
11:                                      23: night-serv
12: priority                             24: pos-busy
```

3. Type **priority** next to the feature button that you want the attendant to use for Priority Calling.
4. Press **Enter** to save your changes.

Assigning a priority feature button to a telephone

To assign a priority feature button to a telephone:

1. Type **change station *n***, where ***n*** is the extension of a multiappearance telephone to which you want to assign a priority feature button. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area (Figure 353: Station screen on page 1374).

Figure 353: Station screen

```
                                   STATION
SITE DATA
      Room:                                          Headset? n
      Jack:                                          Speaker? n
     Cable:                                        Mounting: d
     Floor:                                    Cord Length: 0
  Building:                                      Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          7:
 2: call-appr                          8:
 3: call-appr                          9:
 4: priority                          10:dn-dst
 5:                                   11:goto-cover
 6:                                   12:send-calls Ext:
```

3. Type **priority** next to the button assignment that you want the user to use for Priority Calling.
4. Press **Enter** to save your changes.

End-user procedures for Priority Calling

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. A user can activate Priority Calling before or after the user places a call. This section includes the following end-user procedures for Priority Calling:

To activate Priority Calling before you place a call:

1. Dial the for priority calling Feature Access Code (FAC) and an extension.
2. Press a priority feature button and dial an extension.

To activate Priority Calling after the call starts to ring at the destination:

1. Press the priority feature button.

Considerations for Priority Calling

This section provides information about how the Priority Calling feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Priority Calling under all conditions. The following considerations apply to Priority Calling:

- The Priority Calling feature currently does not work correctly if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.

Interactions for Priority Calling

This section provides information about how the Priority Calling feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Priority Calling in any feature configuration.

- Abbreviated Dialing

  To place a priority call to an extension on an abbreviated dial list, the user must use a button to which both the Feature Access Code (FAC) for Priority Calling and Abbreviated Dialing are assigned.

- Call Coverage

  The system redirects a call to coverage if the user activates Go to Cover for the call. When the call goes to coverage, the call remains a priority call. The covering user hears the priority call ringing pattern.

- Call Forwarding All Calls

  The system forwards priority calls, except callback calls. When the system forwards a call, the call remains a priority call.

- Call Vectoring

  The system generates intercept tone when someone attempts to activate Priority Calling toward a vector directory number (VDN).

- Call Waiting

  A priority call waits on an active single-line telephone, even if Call Waiting is not assigned to the telephone. The user with an active, single-line telephone who receives the call, hears the distinctive priority Call Waiting tone.

- Consult

  A Consult call acts as a priority call and waits at a single-line telephone, even if the telephone does not have Call Waiting Indication assigned.

- Distributed Communications System (DCS)

  With a DCS tandem call to a single-line telephone, the called party does not receive priority ringing, if the caller presses the priority button to activate Priority Calling.

- Last Number Dialed

  A user must use the Last Number Dialed button to place a priority call to the last number dialed. The Last Number Dialed FAC is not valid after a user activates Priority Calling.

  You can administer single-line telephones, for example, 2500-series telephones, so that the system does not provide distinctive ringing. If you administer single-line telephones in this way, the system provides one-burst ringing for priority calls.

Privacy

Use the Privacy feature to protect your call from interruptions.

Privacy supports the following capabilities:

- Data Privacy for voice or data calls

  Prevents voice or data calls from being disturbed by any overriding or ringing features

- Data Restriction for voice or data calls

  Prevents voice or data calls from being disturbed by an overriding or ringing, features or system-generated tones.

- Privacy-Automatic Exclusion

  Automatically prevents other multiappearance users from bridging onto a call

- Manual Exclusion

  Prevents other multiappearance users from bridging onto a call when the recipient of the call presses the exclusion button

Detailed description of Privacy

This section provides a detailed description of the Privacy feature.

Data Privacy

The Data Privacy capability prevents analog data calls from being disturbed by any overriding or ringing features. You administer Data Privacy for each user.

Data Restriction

The Data Restriction capability prevents voice or data calls from being disturbed by any overriding or ringing feature or by system-generated tones. You can administer Data Restriction for either a user or a trunk group. When you administer Data Restriction for a voice telephone, data terminal, or a trunk group, the capability is active for all calls to or from those facilities.

Privacy - Automatic Exclusion

Privacy - Automatic Exclusion allows a user of a multiappearance telephone to keep others with appearances of the same extension from bridging onto an existing call. Automatic exclusion is available as soon as a user answers a call. To turn off automatic exclusion, the user presses the exclusion button.

Privacy - Manual Exclusion

Privacy - Manual Exclusion allows a user of a multiappearance telephone to keep others with appearances of the same extension from bridging onto an existing call. To use manual exclusion, the user presses the exclusion button, either before the user places the call, or when the user is active on the call. If the user presses the exclusion button while others are bridged onto the call, the system drops the other users. To turn off manual exclusion, the user presses the exclusion button.

Administering Privacy

The following steps are part of the administration process for the Privacy feature:

- Administering Privacy for a user
- Activating Data Restriction for a trunk group

This section describes:

- Any prerequisites for administering the Privacy feature
- The screens that you use to administer the Privacy feature
- Complete administration procedures for the Privacy feature

Prerequisites for administering Privacy

You must complete the following actions before you can administer the Privacy feature:

- Ensure that the **Automatic Exclusion** field on the Feature-Related System Parameters screen is set to y.

  To view the Feature-Related System Parameters screen, type **`change system-parameters features`**. Press **Enter**.

- Ensure that the **Data Privacy Access Code** field on the Feature Access Codes (FAC) screen is set to **y**.

  To view the Feature Access Codes (FAC) screen, type **`change feature-access-codes`**. Press **Enter**.

- Ensure that the **Data Privacy** and the **Automatic Exclusion** fields on the Class of Service screen are set to **y**.

  To view the Class of Service screen, type **`change cos`**. Press **Enter**.

Screens for administering Privacy

Screen name	Purpose	Fields
Feature Access Code (FAC)	Set the access code for Data Privacy.	**Data Privacy Access Code**
Feature-Related System Parameters	Activate Privacy-Automatic Exclusion.	**Automatic Exclusion by COS.**
Class of Service	Enable data privacy for a Class of Service (COS).	**Data Privacy**
Station	Administer COS.	**COS**
	Administer an **exclusion** feature button.	Any available button field in the **Button Assignments** area
	Activate Data Restriction.	**Data Restriction?**
Trunk Group - all	Activate Data Restriction.	**Data Restriction?**

Administering Privacy for a user

To administer Privacy for a user:

1. Type **`change station`** ***`n`***, where ***`n`*** is the extension of the user for whom you want to administer Privacy. Press **Enter**.

   The system displays the Station screen (Figure 354: Station screen on page 1380).

Figure 354: Station screen

```
change station                                          Page 1 of X
                              STATION

Extension: 1014               Lock Messages? n                  BCC: 0
     Type:                    Security Code:                     TN: 1
     Port:                  Coverage Path 1:                    COR: 1
     Name:                  Coverage Path 2:                    COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                          Message Lamp Ext: 1014
           Speakerphone: 2-way                   Mute button enabled? y
       Display Language? English                    Expansion Module?
                   Model:

 Survivable GK Node Name:                           Media Complex Ext:
                                                         IP Softphone? y
                                                   Remote Office Phone? y
```

2. In the **COS** field, type the number of the COS that supports Data Privacy.
3. Click **Next** until you see the **Data Restriction?** field (Figure 355: Station screen on page 1381).

Figure 355: Station screen

```
change station                                              Page 2 of X
                                    STATION

FEATURE OPTIONS
           LWC Reception? spe                Auto Select Any Idle Appearance? n
          LWC Activation? y                          Coverage Msg Retrieval? y
  LWC Log External Calls? n                                Auto Answer: none
            CDR Privacy? n                             Data Restriction? y
   Redirect Notification? y                      Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n            Per Station CPN - Send Calling Number? _
       Service Link Mode: as-needed
         Multimedia Mode: basic
    MWI Served User Type: _______                Display Client Redirection? n
         Automatic Moves:
              AUDIX Name:                       Select Last Used Appearance? n
                        _                         Coverage After Forwarding? _
     Recall Rotary Digit? n                         Multimedia Early Answer? n

Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001                          IP Audio Hairpinning? n
```

4. In the **Data Restriction?** field, type **y**.

   If the **Auto Answer** field is set to **all** or **acd**, you must not set the **Data Restriction?** field to **y**.

5. Click **Next** until you see the **Button Assignments** area (Figure 356: Station screen on page 1382).

Figure 356: Station screen

```
change station                                              Page   3 of 4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                            7:disp-chrg
 2: call-appr                            8:
 3: call-appr                            9:
 4:                                     10:
 5:                                     11:exclusion
 6: headset                             12:release
```

6. In the **Button Assignments** area, type **exclusion** next to the feature button number that you want the user to use activate privacy-manual exclusion, and to deactivate both privacy-manual exclusion and privacy-automatic exclusion.
7. Press **Enter** to save your changes.

Activating Data Restriction for a trunk group

To activate Data Restriction for a trunk group:

1. Type **change trunk-group *n***, where ***n*** is the number of the trunk group for which you want to activate Data Restriction.

   The system displays the Trunk Group screen.
2. In the **Data Restriction?** field, type **y**.

   CAUTION:
   Do not change any other fields on this page of the Trunk Group screen without assistance from Avaya or your network service provider.
3. Press **Enter** to save your changes.

End-user procedures for Privacy

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Privacy:

- Using Privacy

To use privacy

1. Dial the Feature Access Code (FAC) for Data Privacy at the beginning of the call to activate Data Privacy.
2. Press the **exclusion** button before or during a call to activate Privacy-Manual Exclusion.
3. Press the **exclusion** button to deactivate Privacy-Manual Exclusion or Privacy-Automatic Exclusion.

Considerations for Privacy

This section provides information about how the Privacy feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Data Privacy under all conditions. The following considerations apply to Privacy:

- Data Privacy applies to both voice and data calls. You can activate Data Privacy on Remote Access calls, but not on other incoming trunk calls. Data Privacy is canceled if a user transfers a call, is added to a conference call, is bridged onto a call, or disconnects from a call. You can activate Data Privacy on calls that originate from attendant consoles.
- For virtual extensions, assign the Data Privacy Class of Service to the mapped-to physical extension.
- Do not administer Data Restrictions for an attendant console.

Interactions for Privacy

This section provides information about how the Privacy feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Privacy in any feature configuration.

- Attendant Call Waiting and Call Waiting Termination

  If Data Privacy is active, Call Waiting is denied.

- Bridged Call Appearance - Single-Line Telephone

  If you activate Data Privacy or assign Data Restriction to a station that is involved in a bridged call and the primary terminal or bridging user attempts to bridge onto the call, this action overrides Data Privacy and Data Restriction.

  When Privacy-Manual Exclusion is active, the system does not allow other users to bridge onto the active call.

- Busy Verification

  Busy Verification cannot be active when Data Privacy is active.

- Call Coverage

  When the principal user bridges onto a call that has gone to coverage, and the call is answered at the coverage pint, the system does not drop the principal user from the call when Privacy-Manual Exclusion is activated.

- Call Pickup

  The system does not drop the called party from the call in the following example:

  — A call is made to user A.

  — User B uses Call Pickup to answer the call.

  — User A bridges onto the call by going off-hook on its call appearance.

  — User B activates Privacy-Manual Exclusion.

- Intercom - Automatic and Dial

  An extension with Data Privacy or Data Restriction active cannot originate an intercom call. The user receives an intercept tone.

- Music-on-Hold Access

  If a user places a call with Data Privacy on hold, the user must withhold Music-on-Hold. This action prevents the transmission of tones that a connected data service might falsely interpret as a data transmission.

- Priority Calls

  If a user activates Data Privacy, Priority Calls are denied on analog telephones. However, Priority Calls appear on the next available line appearance on multiappearance telephones.

- Whisper Paging

  If you administer Data Restriction for a telephone, a data terminal, or a trunk group, the system denies Whisper Paging.

Public Network Call Priority

Use the Public Network Call Priority feature to provide call retention, forced disconnect, intrusion, mode-of-release control, and re-ring to servers on public networks.

Detailed description of Public Network Call Priority

This section provides a detailed description of the Public Network Call Priority feature.

Use the Public Network Call Priority feature to provide call retention, forced disconnect, intrusion, mode-of-release control, and re-ring to servers on public networks. Different countries refer to these functions by different names. Not all functions are available in all countries.

China

Forced disconnect

With forced disconnect, a network operator can disconnect a called party from a local call, and connect the called party to an incoming toll call. Parties who are on the local call hear a warning tone before the network operator disconnects the call. Forced disconnect is allowed only for callers on local single-station calls. The system does not allow forced disconnect for the following type of calls:

- Conference
- Transferred
- Forwarded
- To group users
- Tandem

Mode-of-release control

Mode-of-release control inhibits release of a trunk circuit when a caller goes on-hook, based on call type and direction. Instead of releasing the trunk circuit, the system keeps the circuit active, and reconnects the call if the caller goes off-hook again. Mode-of-release control applies to the following types of incoming or outgoing calls:

- Toll
- Local
- Service

Public Network Call Priority provides three types of mode-of-release control.

- Calling-party control

  When calling-party control is active, the trunk is not released until the caller goes on-hook. For example, if the:

  - Caller goes on-hook, the trunk is released immediately. The called party receives busy tone.
  - Called party goes on-hook, the trunk is not released until the caller goes on-hook, or the
    re-answer timer for outgoing calls expires. The called party can reanswer the call, and talk to the calling party.

    Re-ring occurs for incoming calls to the system with calling-party control. When the called party goes on-hook, the trunk is not released, and the central office (CO) operator can re-ring the called party and reconnect the call.
  - Re-answer timer is activated and expired, the trunk is released on outgoing calls with calling-party control.

- Called-party control

  When called-party control is active, the trunk is not released until the called party goes on-hook.

  - If the called party goes on-hook, the trunk is released immediately, and the caller receives busy tone.
  - If the caller goes on-hook, the trunk is not released until the called party goes on-hook. The caller can go off-hook again to reconnect. No timer is involved with called-party control

- First-party control

  When first-party control is active, the trunk is released immediately regardless of whether the caller or the called party goes on-hook first. The party that is still connected receives busy tone. The default or normal mode-of-release control for the system is first-party control.

Russia

Intrusion

Intrusion allows a network operator to break into a local call and announce an incoming toll call. Intrusion is allowed on local single-line and multiline telephone calls. The system does not allow intrusion for the following types of calls:

- Conference
- On hold
- Toll

Re-ring

Re-ring occurs when a call is interrupted by an operator-assisted incoming call, and the call is kept on hold so that the call can be reconnected to a telephone. When the called party goes on-hook, the network toll operator can re-ring the called party, and reconnect the call.

Spain

Call retention

When a caller makes an emergency call and then hangs up, the call is put on hold. The system does not disconnect the call. When the caller goes back off-hook, the system reconnects the telephone to the emergency call. Call retention works on both analog and digital telephones.

Re-ring

Re-ring occurs when a call is interrupted by an operator-assisted incoming call, and the call is kept on hold so that the call can be reconnected to a telephone. When the called party goes on-hook, the network toll operator can re-ring the called party, and reconnect the call.

Administering Public Network Call Priority

This section describes the screens that you use to administer the Public Network Call Priority feature.

Screens for administering Public Network Call Priority

Screens for China

Screen name	Purpose	Fields
Multifrequency-Signaling-Related System-Parameters	Specify the type of tone that is received from a Chinese central office (CO).	**Incoming Forward Signal Types for group I and group II**
	Specify the type of tone that is sent to a Chinese CO.	**Incoming Backward signal Types for group A and group B**
Trunk Group	Specify country code 18 for China.	**Country**
	Specify the outgoing dial type of mf for China.	**Outgoing Dial Type**
	Specify the incoming dial type of mf for China	**Incoming Dial Type**

Screens for Russia

Screen name	Purpose	Fields
Trunk Group (DID)	Specify country code 15 for Russia.	**Country**
	Specify the protocol type Intol for Russia.	**Protocol Type**
Trunk Group (DIOD)	Specify country code 15 for Russia.	**Country**
	Specify the protocol type Intol for Russia.	**Protocol Type**

Screens for Spain

Screen name	Purpose	Fields
Trunk Group	Specify country code 11 for Spain.	**Country**

Interactions for Public Network Call Priority

This section provides information about how the Public Network Call Priority feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Public Network Call Priority in any feature configuration.

China

Forced disconnect

- Conference

  If the network toll call terminates at a telephone that is involved in a conference, the network does not send the forced disconnect signal.

- Call Forwarding

  The system forwards the forced disconnect signal for calls that are forwarded on-premises, on the network, or off the network.

- Group Users

  The network does not send the forced disconnect signal, if a network toll call terminates to a group user.

- Nonstation Users

  The network does not send the forced disconnect signal, if a network toll call terminates to a nonstation user. Nonstation users include personal attendant, data module., announcement and voice synthesis users.

- Tandem Trunks

  The system does not tandem a forced disconnect signal.

- Transfer

  The network does not send the forced disconnect signal, if a network toll call is transferred.

Mode-of-release control

- Conference

  A call that is involved in a conference is changed to first-party control as the mode-of-release control.

- Forward

  A call that is forwarded on-premises, on the network, or off the network is changed to first-party control as the mode-of-release control.

- Group users, including hunt, trunk, terminating extension group (TEG), CM Messaging, Vector Directory Number (VDN)

  Calls that terminate to group users are changed to first-party control as the mode-of-release control.

- Nonstation users includes personal attendant, data-module, announcement, and users of voice synthesis.

  Calls that terminate to nonstation users are changed to first-party control as the mode-of-release control.

- Tandem Trunks

  The system terminates tandem calls, but the mode-of-release control is changed to first-party control.

- Transfer

  A transferred call is changed to first-party control as the mode-of-release control.

Re-ring

- Conference

  A call that is involved in a conference is changed to first-party control as its mode-of-release control. first-party control calls do not re-ring.

- Call Forwarding

  The system does not forward re-ring signals for calls forwarded on-premises, on the network, or off the network.

- Group users - hunt, trunk, TEG, CM Messaging, and VDN

  The system ignores Re-ring signals that are sent to group users.

- Nonstation user - personal attendant, data-module, announcement, voice synthesis

  The system ignores Re-ring signals that are sent to nonstation users.

- Tandem trunks

  The system does not tandem re-ring signals.

- Transfer

  A transferred call is changed to first-party control as its mode-of-release control. First-party control calls do not re-ring.

Russia

- Announcements

  The system does not allow intrusion and re-ring for an announcement port.

- Abbreviated Ringing and Delayed Ringing

  Abbreviated Ringing and Delayed Ringing characteristics that you assign do not apply to re-ring. Re-ring has its own priority ringing.

- Administered Connections

  Intrusion and re-ring do not apply to Administered Connections.

- Attendant Console

  Intrusion and re-ring do not apply to attendant consoles, or to any call that involves an attendant console.

- Attendant Serial Call

  The system ignores Intrusion and re-ring for an attendant serial call.

- Automatic Callback

  Re-ring takes precedence over automatic callback on busy or no-answer calls.

- Busy Verification and Attendant Intrusion

  While Intrusion or re-ring occurs, Busy Verification and Attendant Intrusion are denied. While Busy Verification or Attendant Intrusion occurs, Intrusion and re-ring are denied.

- Call Coverage

  Re-ring overrides Call Coverage. However, if a station is busy and a coverage destination is free, an incoming toll call rings at the coverage destination instead of intruding on the busy call.

- Call Forwarding

  Intrusion can be used with Call Forwarding. If a station is busy, an incoming toll call is forwarded instead of intruding on the busy call. Re-ring overrides all administered redirection.

- Call Waiting

  If Call Waiting is active, calls are not intruded upon. Call Waiting takes precedence.

- Conference

  The system does not allow intrusion for a call that is involved in a conference.

- Data Calls

  The system does not allow intrusion for telephones that have Data Privacy, Data Restriction, or Data Protection active.

- Distinctive Ringing

  Ringing characteristics that you assign do not apply to re-ring. Re-ring has its own priority ringing.

- Do Not Disturb

  You cannot use intrusion and Do Not Disturb at the same time.

- Emergency Access to the Attendant

  The system does not allow intrusion for an emergency call.

- Hunt Group and Automatic Call Distribution

  If a hunt group queue is not busy, the system places incoming toll calls in the queue. Busy calls are not intruded upon.

- Intercom - Automatic and Dial

  The system does not allow intrusion on any Intercom calls.

- Malicious Call Trace (MCT)

  The system does not allow intrusion on a station that has MCT active.

- Personal Station Access (PSA)

  The system does not allow Intrusion when PSA is in use.

- Pull Transfer

  The system does not allow Intrusion when Pull Transfer is in use.

- Class of Restriction (COR)

  The system does not allow Intrusion, regardless of the COR.

- Ringback Queuing

  Intrusion is allowed with Ringback Queuing.

- Station Hunting

  The system allows Intrusion when Station Hunting is used.

- Tandem Trunks

  The system does not allow Intrusion over trunk groups used as tandem trunks.

Record on Messaging

Use the Record on Messaging feature to record telephone conversations by pressing a single button. The Record on Messaging feature uses CM Messaging to record a telephone conversation. A user needs to press only one feature button on the telephone to activate this feature. Record on Messaging then stores the recorded conversation as a message in the voice mailbox of the user. The system allows Record on Messaging only after a call is answered.

Note:

Some countries, states, and localities have laws that determine if and under what circumstances you can record telephone conversations. Before you administer the Record on Messaging feature, you must understand and comply with these laws.

Detailed description of Record on Messaging

This section provides a detailed description of the Record on Messaging feature.

The Record on Messaging feature is available with Communication Manager Release 1.3 (V11) or later.

- Communication Manager Release 1.3 supports Record on Messaging only when the CM Messaging system is local.
- Communication Manager Release 2.0 and later supports Record on Messaging with a local CM Messaging system or with a remote CM Messaging system. To use a remote CM Messaging system, the person recording the conversation must have Communication Manager Release 2.0 or later.

Feature button

The Record on Messaging feature uses an administered feature button, **audix-rec**. The administrator uses the Station screen to assign this button for each telephone. When you assign the feature button, the system requires you to provide the extension for the CM Messaging hunt group of the user. Users cannot access Record on Messaging on any telephone that does not have an administrable feature button, or on an attendant console.

Language options

Five languages are available for the feature button labels for Record on Messaging:

- English
- Italian
- French
- Spanish
- A user-defined language

The feature button labels for Record on Messaging are available in English, with predefined Italian, French, and Spanish translations. The administrator cannot change the text of the English, the Italian, the French, or the Spanish feature button labels.

The administrator can translate the feature button labels into a user-defined language. This translation can be any other language that you choose, such as German. The administrator can use only one user-defined language throughout the system.

Periodic alerting tone

While CM Messaging records the conversation, all parties on the call might hear a periodic alerting tone. This alerting tone reminds all parties on the call that CM Messaging is recording the conversation. The tone that plays is a zip tone.

You choose the time interval to play the periodic alerting tone. If you set the time interval of the periodic alerting tone to zero, the parties hear no alerting tone.

Ready indication tone

When CM Messaging starts recording the conversation, the system plays a ready indication tone. The tone that plays is a zip tone.

The administrator can set the ready indication tone to play to:

- All the parties on the call.
- The initiator only.

  The "initiator" is the user who activates the Record on Messaging feature.
- None of the parties on the call.

Recording delay timer

When the user presses the **audix-rec** feature button, CM Messaging answers. After CM Messaging answers, the system uses the recording delay timer to wait for CM Messaging to get ready to interpret digits. The system then sends digit 1 to tell CM Messaging to start recording.

The recording delay timer is preset to 500 milliseconds. This delay is sufficient for most recorded conversations. If you have to change this setting, see the section titled "Assigning Record on Messaging Parameters".

Administering Record on Messaging

The following steps are part of the administration process for the AUDIX One-Step Recording feature:

- Assigning Record on Messaging Parameters
- Translating telephone feature buttons and labels
- Assigning the feature button to a telephone
- Changing the characteristics of the zip tone

This section describes:

- Any prerequisites for administering the Record on Messaging feature
- The screens that you use to administer the Record on Messaging feature
- Complete administration procedures for the Record on Messaging feature

Prerequisites for administering Record on Messaging

You must complete the following actions before you can administer the Record on Messaging feature:

- On the Optional Features screen, ensure that the **G3 Version** field is set to **V11** or later. If this field is not set to **V11** or later, your system is not enabled for the AUDIX One-Step Recording feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Record on Messaging

Screen name	Purpose	Fields
Optional Features	Ensure that you have Communication Manager version 1.3 (V11) or later.	**G3 Version**
Feature-Related System Parameters	Set the time interval, in milliseconds, for the recording delay timer.	**Recording Delay Timer (msec)**
	Assign who on the call can hear the ready indication tone.	**Apply Ready Indication Tone To Which Parties In The Call**
	Set the time interval, in seconds, for the periodic alerting tone.	**Interval For Applying Periodic Alerting Tone (seconds)**
Language Translations	If needed, change the translation of the **audix-rec** feature button to a user-defined language.	**Audix Recording**
	If needed, change the translation of the **Audix Record** button label to a user-defined language.	**Audix Record**
Station	Assign the **audix-rec** feature button, and associate the hunt group extension of the user.	**Button Assignments**

Assigning Record on Messaging Parameters

To assign the recording delay timer, the ready indication tone, and the periodic alerting tone:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **AUDIX One-step Recording** area (Figure 357: Feature-Related System Parameters screen on page 1397).

Figure 357: Feature-Related System Parameters screen

```
change system-parameters features                                Page 6 of 12

                        FEATURE-RELATED SYSTEM PARAMETERS

CONFERENCE/TRANSFER

               Abort Transfer? n                  No Dial Tone Conferencing? n
        Transfer Upon Hang-Up? n        Select Line Appearance Conferencing? n
Abort Conference Upon Hang-Up? n                                    Unhold? n
   No Hold Conference Timeout: 60

ANALOG BUSY AUTO CALLBACK
                Without Flash? n


AUDIX ONE-STEP RECORDING
                            Recording Delay Timer (msec): 500
Apply Ready Indication Tone To Which Parties In The Call? all
  Interval For Applying Periodic Alerting Tone (seconds): 15
```

3. If you need to change the time between when CM Messaging answers and when CM Messaging starts recording, change the value in the **Recording Delay Timer (msec)** field. The time is measured in milliseconds in increments of 100. The default setting is 500 milliseconds.

   After CM Messaging starts recording, Communication Manager must filter out the CM Messaging tone. The user must wait longer than the Recording Delay Timer setting before the user notices that recording has started.

4. In the **Apply Ready Indication Tone To Which Parties In The Call** field, type one of the following values. These values indicate who hears the ready indication tone:

   - If you want all parties on the call to hear the ready indication tone, leave the default set to **all**. The screen displays the **Interval For Applying Periodic Alerting Tone (seconds)** field.
   - If you want only the initiator to hear the ready indication tone, right-click the field and select **initiator**. The screen does not display the **Interval For Applying Periodic Alerting Tone (seconds)** field.
   - If you want no one on the call to hear the ready indication tone, right-click the field and select **none**. The screen does not display the **Interval For Applying Periodic Alerting Tone (seconds)** field.

5. In the **Interval For Applying Periodic Alerting Tone (seconds)** field, type a value between **0** and **60** seconds. This value indicates how often all parties on the call hear the periodic alerting tone.

   The default value is **15** seconds. If you set the value to **0**, no one on the call hears the periodic alerting tone.

6. Press **Enter** to save your changes.

Translating telephone feature buttons and labels

To translate telephone feature buttons and labels for Record on Messaging to a user-defined language, you must complete the following procedures:

- Translating the Record on Messaging text that appears on a telephone display to a user-defined language
- Translating the Record on Messaging button label to a user-defined language

Translating the Record on Messaging text that appears on a telephone display to a user-defined language

To translate the text that appears on your telephone display, when this feature is recording, to a user-defined language:

1. Type **`change display-messages view-buttons`**. Press **Enter**.

   The system displays the Language Translations screen.

2. Click **Next** until you see the **Audix Recording** field (Figure 358: Language Translations screen on page 1398).

Figure 358: Language Translations screen

```
change display-messages view-buttons                          Page 9 of 9

                          LANGUAGE TRANSLATIONS

English                                Translation

1.  Station Lock                       ****************************
2.  License Error                      ****************************
3.  Conference Display                 ****************************
4.  Conf/Trans Toggle-Swap             ****************************
5.  Posted Messages                    ****************************
6.  Audix Recording                    ****************************
```

3. In the **Translation** field, type a translated name for **Audix Recording** into the user-defined language.

   Note that the language translations for the English, the Italian, the French, and the Spanish feature display are predefined. You cannot change the text for these translations.

4. Press **Enter** to save your changes.

Translating the Record on Messaging button label to a user-defined language

The 2420 DCP telephone and the 4620 IP telephone have digital button labels instead of paper labels. If you need to translate the AUDIX One-Step Recording button labels into a user-defined language for these telephones, follow this procedure.

To translate the AUDIX One-Step Recording button label for the 2420 DCP telephone and the 4620 IP telephone to a user-defined language:

1. Type **`change display-messages button-labels`**. Press **Enter**.

   The system displays the Language Translations screen.

2. Click **Next** until you see the **Audix Record** field (Figure 359: Language Translations screen on page 1399).

Figure 359: Language Translations screen

```
change display-messages button-labels                          Page 9 of 9

                            LANGUAGE TRANSLATIONS

English                                  Translation

 1. Alternate FRL                         1. *************
 2. ANI Request                           2. *************
 3. Assist                                3. **********
 4. ASVN Halt                             4. *************
 5. AttQueueCall                          5. *************
 6. AttQueueTime                          6. *************
 7. Audix Record                          7. *************
 8. Auto Callback                         8. *************
 9. Auto Chk Halt                         9. *************
10. AutoIC                               10. *******
11. Auto In                              11. **********
12. AutoWakeAlarm                        12. *************
13. Auto Wakeup                          13. *************
14. AuxWork                              14. ********
15. Busy                                 15. *****
```

3. In the **Translation** field, type a translated name for the **Audix Record** button label into the user-defined language.

   Note that the language translations for the English, the Italian, the French, and the Spanish feature buttons are predefined. You cannot change the text for these translations.

4. Press **Enter** to save your changes.

Assigning the feature button to a telephone

To assign the **audix-rec** feature button to an individual telephone:

1. Type **`change station n`**, where ***n*** is the extension of the telephone. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Button Assignments** area (Figure 360: Station screen on page 1400).

Figure 360: Station screen

```
change station 9876                                          Page 3 of 3

                                    STATION

 SITE DATA
      Room:                                      Headset? n
      Jack:                                      Speaker? n
     Cable:                                     Mounting: d
     Floor:                                   Cord Length: 0
  Building:                                     Set Color:



ABBREVIATED DIALING
     List1:                List2:                List3:

BUTTON ASSIGNMENTS
 1. call-appr                          6.
 2. call-appr                          7.
 3. call-appr                          8.
 4. audix-rec  Ext: 9800               9.
 5.                                   10.
```

3. Right-click a button field that is not assigned to see a list of button names. Select **audix-rec** from the list.

   The screen displays an **Ext** field.

4. In the **Ext** field, type the CM Messaging hunt group extension of the user.
5. Press **Enter** to save your changes.

Changing the characteristics of the zip tone

When the Record on Messaging feature is recording a conversation, the tone that a user hears is a zip tone. By default, a zip tone plays at a frequency of 480 Hz for 500 milliseconds, followed by silence.

If you need to change the characteristics of the zip tone, the screen that you use depends on what version of Communication Manager you have.

To change the characteristics of the zip tone if you have Communication Manager Release 2.0 (V12) or later:

1. Type **`change tone-generation`**. Press **Enter**.

   The system displays the Tone Generation screen.

2. Click **Next** until you see either:

   - An existing Tone Generation Customized Tones screen for the zip tone

     If a screen already exists for the zip tone, the word **zip** appears in the **Tone Name** field.

   - A blank Tone Generation Customized Tones screen (Figure 361: Tone Generation Customized Tones screen on page 1402).

Figure 361: Tone Generation Customized Tones screen

```
change tone-generation                                          Page 4 of 21

                        TONE GENERATION CUSTOMIZED TONES

     Tone Name           Cadence          Tone
                          Step      (Frequency/Level)
                            1:
                            2:
                            3:
                            4:
                            5:
                            6:
                            7:
                            8:
                            9:
                           10:
                           11:
                           12:
                           13:
                           14:
                           15:
```

If a screen already exists for the zip tone, skip the next step and go to Step 4.

3. Right-click the **Tone Name** field to see a list of options. Select **zip** from the list.
4. Right-click the **Cadence Step 1** field to see a list of options. Select a tone frequency and level combination from the list.

   The screen displays a **Duration (msec)** field.
5. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to play.
6. Right-click the **Cadence Step 2** field to see a list of options. Select **silence** from the list.

   The screen displays a **Duration (msec)** field.
7. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to remain silent after the system plays the tone.
8. Press **Enter** to save your changes.

To change the characteristics of the zip tone if you have Communication Manager Release 1.3 (V11) or earlier:

1. Type **`change system-parameters country-options`**. Press **Enter**.

   The system displays the System Parameters Country-Options screen.
2. Click **Next** until you see either:

- An existing System Parameters Country-Options screen for the zip tone

  If a screen already exists for the zip tone, the word **zip** appears in the **Tone Name** field.

- A blank System Parameters Country-Options screen (Figure 362: System Parameters Country-Options screen on page 1403).

Figure 362: System Parameters Country-Options screen

```
change system-parameters country-options                        Page 7 of 24

                      SYSTEM PARAMETERS COUNTRY-OPTIONS

     Tone Name           Cadence          Tone
                          Step      (Frequency/Level)
                            1:
                            2:
                            3:
                            4:
                            5:
                            6:
                            7:
                            8:
                            9:
                           10:
                           11:
                           12:
                           13:
                           14:
                           15:
```

If a screen already exists for the zip tone, skip the next step and go to Step 4.

3. Right-click the **Tone Name** field to see a list of options. Select **zip** from the list.
4. Right-click the **Cadence Step 1** field to see a list of options. Select a tone frequency and level combination from the list.

   The screen displays a **Duration (msec)** field.
5. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to play.
6. Right-click the **Cadence Step 2** field to see a list of options. Select **silence** from the list.

   The screen displays a **Duration (msec)** field.
7. In the **Duration (msec)** field, type the number of milliseconds for which you want the zip tone to remain silent after the system plays the tone.
8. Press **Enter** to save your changes.

End-user procedures for Record on Messaging

End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for the Record on Messaging feature.

Recording a conversation

The user who wants to record the conversation is called the "initiator."

Note:
This procedure assumes that the initiator understands and complies with any country, state, and local laws concerning if you can record telephone conversations.

1. A user announces to the other parties on the call that he or she wants to record the conversation.
2. This user gets permission from the parties, and presses the **audix-rec** button to record the conversation.

   When the initiator presses the **audix-rec** button, the LED for the **audix-rec** button flashes. After a few seconds, the telephone displays of all internal users on the call change to **Conference**. The number of parties on the call increases by one. The LED on the telephone of the initiator stays on, and no longer flashes. This light indicates that CM Messaging is ready to record.

   CM Messaging starts to record the conversation. The system plays the ready indication tone to indicate that recording is started. Only the initiator hears any CM Messaging announcements.
3. To stop the recording at any time, the initiator can press the **audix-rec** button again. The LED on the telephone of the initiator goes out. The number of parties on the call decreases by one. The call remains active. The initiator can press the **audix-rec** button to start and stop recording the same conversation any number of times. Each time creates a separate recorded message.

   If the initiator hangs up while CM Messaging is recording the conversation, the recording ends. If the call is originally a two-party call and the other party hangs up, the recording ends. If the call is originally a multiple-party conference call and someone other than the initiator hangs up, the recording continues.

   When the recording ends, the system saves the recorded conversation in the voice mailbox of the initiator as a new voice mail message.

Considerations for Record on Messaging

This section provides information about how the Record on Messaging feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Record on Messaging under all conditions. The following considerations apply to the Record on Messaging feature:

- Capacity constraints and feature limitations

  Record on Messaging has the following capacity constraints and feature limitations:

  - Only one simultaneous CM Messaging recording is allowed for each call.
  - The **audix-rec** feature button works as a toggle button. When the button is active, the button is associated with only one call. A user cannot use the **audix-rec** feature button on two calls simultaneously.
  - Attendant consoles do not have an **audix-rec** feature button. Attendants cannot use the Record on Messaging feature.
  - Service observers who are actively involved in service observing cannot use the Record on Messaging feature.

- Denial scenarios

  The Record on Messaging feature is denied, and the feature button flutters, if a user presses the **audix-rec** button when:

  - No call is active on the telephone
  - The user is still dialing digits
  - The connection to CM Messaging is not operating
  - All CM Messaging ports are busy
  - The number of parties on the call reaches the administered maximum
  - Another party on the call is already recording the conversation with AUDIX One-Step Recording
  - The user starts the recording from a bridged call appearance
  - Service observers are actively involved in service observing
  - The incoming or outgoing call is ringing and is not answered

- Security

  Some countries, states, and localities have laws that determine if and under what circumstances you can record telephone conversations. Before you administer the Record on Messaging feature, you must understand and comply with these laws.

- Serviceability

  This feature depends on CM Messaging to function. The administrator is responsible for properly administering CM Messaging. CM Messaging must work for the telephone user before the administrator applies this feature to the telephone. Specifically, the administrator needs to set the appropriate **Mailbox Size** and **Voice Mail Message Maximum Length** on CM Messaging for the user.

  The **audix-rec** button requires the extension of the CM Messaging hunt group of the user. The administrator must type the correct extension on the Station screen.

Interactions for Record on Messaging

This section provides information about how the Record on Messaging feature interacts with other features in your system. Use this information to ensure that you receive the maximum benefits of Record on Messaging in any feature configuration. The following interactions apply to the Record on Messaging feature:

- Bridged Call Appearance
  - A user cannot activate or deactivate the **audix-rec** feature button from a bridged call appearance.
  - If the administrator sets the ready indication tone to play to all parties, parties on bridged call appearances hear the tone. If the administrator sets the ready indication tone to play to the initiator only, parties on bridged call appearances do not hear the tone.
- Call Park

  When Record on Messaging is active on a call, the system does not allow the user to park the call. If the user attempts to park the call, the call appearance LED flutters.

  When a call is parked, the system does not allow the user to activate Record on Messaging. If the user attempts to activate Record on Messaging, the feature button LED flutters.
- Conference

  When the recording request is in process, the LED is flashing. If anyone attempts to conference in another party, Record on Messaging stops. The LED goes out.

  When the recording starts, the LED is on but not flashing. Any party on the call can conference in another party. The recording continues.

  If Record on Messaging is in progress on two separate calls, the system does not allow the user to conference the two calls together.

- Coverage Answer Group

  An answer group contains up to eight members who act as a coverage point for another user. For example, if several attendants are responsible to answer redirected calls from a department, assign all attendants to an answer group. The administrator assigns a group number to the answer group. That group number appears in the coverage path of that department. All telephones in an answer group ring simultaneously. Any member of the group can answer the call.

  When a member of a Coverage Answer Group answers a call, any of the parties on the call can press the **audix-rec** button to record the conversation. The system stores the recorded message in the voice mailbox of the party who answers the call.

- Drop Last

  After CM Messaging starts to record, the initiator becomes the control party. If the initiator presses the **Drop** button, Record on Messaging stops and the LED goes out. If other parties on the call press the **Drop** button, the system denies the request.

- Group Paging that uses a speakerphone

  With Group Paging, users can make an announcement over a group of digital speakerphones. Neither the group members who receive a page, nor the originator of the page, can use Record on Messaging to record the conversation. If anyone on the call presses the **audix-rec** button, the system ignores the request. The LED flutters.

- Hunt Group

  If a member of a hunt group answers a call, the parties on the call can use Record on Messaging to record the conversation. The system stores the recorded message in the voice mailbox of the party who answers the call.

- Hunt Group queueing

  Users cannot activate Record on Messaging when the following conditions apply.

  — The queue is enabled for the CM Messaging hunt group

  — All the CM Messaging ports are busy

- Meet-me Conference

  Parties on a Meet-me Conference can use Record on Messaging. Conference parties can selectively use the Display and Drop feature to drop the Record on Messaging hunt group extension from the call. The LED goes out.

- Mode Code interface

  Voice mail connections through the Mode Code interface rely on digits that are sent over analog ports. The Record on Messaging feature does not work with a Mode Code connection.

- Terminating Extension Group (TEG)

  Neither group members who receive TEG calls, nor the originators of TEG calls, can use Record on Messaging to record the conversation. If anyone on the call presses the **audix-rec** button, the system denies the request. The LED flutters.

- Transfer

  When the recording request is in process, the LED is flashing. If anyone attempts to transfer the call to another party, Record on Messaging stops. The LED goes out.

  When the recording starts, the LED is on but not flashing. Any party on the call can transfer the call to another party.

  — If the initiator transfers the call, recording automatically stops after the transfer.

  — If another party on the call transfers the call, recording continues.

  If Record on Messaging is in progress on two separate calls, the system does not allow a user to transfer one call to the other.

- Vector Directory Number (VDN)

  When a call is answered through a VDN, any of the parties on the call can press the **audix-rec** button to record the conversation.

- Whisper Page

  With Whisper Page, no parties on the call can use Record on Messaging to record the conversation. If anyone on the call presses the **audix-rec** button, the system denies the request. The LED flutters.

Troubleshooting Record on Messaging

This section lists the known or common problems that users might experience with the Record on Messaging feature.

Problem	Possible cause	Action
The user does not have the **audix-rec** button on the telephone.	The **audix-rec** button is not assigned to the telephone of the user.	Use the **`change station`** ***`n`*** command, where ***`n`*** is the extension of the telephone, to add the **audix-rec** button.
	The telephone of the user does not support buttons that can be administered.	This user cannot access the Record on Messaging feature.
The user hears a beep every few seconds during recording.	The alerting tone interval is set too low.	Set the alerting tone interval to a number that is between 15 and 60.

Problem	Possible cause	Action
Nothing happens when the user presses the **audix-rec** button. The button light flutters.	The user was not on an active call.	Inform the user that the **audix-rec** button only works if the user is on an active call.
	The connection to CM Messaging is not operating.	Ensure that CM Messaging is operating correctly. If not, the user must wait for the system to reestablish the connection.
	The LAN connection between the CM Messaging server and the Communication Manager server is not operating.	Ensure that CM Messaging is operating correctly. If not, the user must wait for the system to reestablish the connection.
	All the CM Messaging ports are busy.	The user must wait for a CM Messaging port to be released.
	Another person on the call is already using the AUDIX One-Step Recording feature to record the conversation.	The user cannot record the conversation if someone else on the call is already using this feature.
	The user attempted to start the Record on Messaging feature from a bridged call appearance.	The user cannot record the conversation from a bridged call appearance.
	Remote CM Messaging is configured for Communication Manager Release 1.3.	• Move the voice mail service of the user to a local CM Messaging, or • Upgrade the user to Communication Manager Release 2.0 or later.
The user does not hear a beep during recording.	The ready indication tone is set to play to only the initiator, or to no one.	Set the ready indication tone to **all**.
	The alerting tone interval is set to zero.	Set the alerting tone interval to a number between 15 and 60.
	The zip tone is set to **silence** instead of to a frequency and duration.	Reset the characteristics of the zip tone.
After the green LED is steady and the recording starts, the user hears a CM Messaging announcement.	If configured with CM Messaging, ARIA TUI might be turned on. The Recording Delay Timer is not set high enough.	Set the Recording Delay Timer to a higher number.

Recorded Telephone Dictation Access

Use the Recorded Telephone Dictation Access feature to access dictation equipment.

Detailed description of Recorded Telephone Dictation Access

This section provides a detailed description of the Recorded Telephone Dictation Access feature.

Use the Recorded Telephone Dictation Access feature to access dictation equipment. Users can access the feature from any onsite or off-site telephone, and can use incoming tie trunks to access the feature.

A user enters a Feature Access Code (FAC) or an extension to access the feature. A user can enter commands by key or by voice to control the start and stop functions. A user can enter commands by key to control other functions, such as initial activation.

Recorded Telephone Dictation Access cannot be used with Automatic Route Selection (ARS) or Conference.

For more information, see the following features:

- "Audible Message Waiting"
- "Announcements"
- "Voice Message Retrieval"

Administering Recorded Telephone Dictation Access

The following steps are part of the administration process for the Recorded Telephone Dictation Access feature:

- Assigning manual signaling button to a multiple-call appearance telephone user

This section describes:

- Any prerequisites for administering the Recorded Telephone Dictation Access feature
- The screens that you use to administer the Recorded Telephone Dictation Access feature

- Complete administration for the Recorded Telephone Dictation Access feature

Screens for administering Recorded Telephone Dictation Access

Screen name	Purpose	Fields
Station	Assign a **signal** button to a user telephone, and specify the extension that rings when the user presses the button.	Any available button field in the **Button Assignments** area

Assigning manual signaling button to a multiple-call appearance telephone user

To assign a manual signaling button to a multiple-call appearance telephone user:

1. Type **`change station n`** where ***n*** is the extension to which you want to assign a signaling button. Press **Enter**.

   The system displays the Station screen for the extension that you requested.

2. Click **next** until you see the **Button Assignments** area (Figure 363: Station screen on page 1413).

Figure 363: Station screen

```
change station 32006                                        Page   3 of   4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1: personal 1         List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                              5: signal     Ext:
 2: call-appr                              6:
 3: call-appr                              7:
 4:                                        8:
```

3. Type **signal** next to the number of the button that you want the user to use for manual signaling.

   When you type **signal** next to the button number the system displays an **Ext:** field.

4. Type the extension of the recipient of the signal in the **Ext:** field.
5. Press **Enter** to save your changes.

Interactions for Recorded Telephone Dictation Access

This section provides information about how the Recorded Telephone Dictation Access feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of the Recorded Telephone Dictation Access feature.

- Automatic Route Selection (ARS)

  You cannot use ARS to access Recorded Telephone Dictation Access.

- Conference

  You cannot use Conference and Recorded Telephone Dictation Access at the same time.

Remote Access

Use the Remote Access feature to access and use the system from the public network.

Detailed description of Remote Access

This section provides a detailed description of the Remote Access feature.

SECURITY ALERT:
Avaya has designed the Remote Access feature incorporated in this product, when properly administered by the customer, to enable the customer to minimize the ability of unauthorized people to gain access to the network. It is the responsibility of you to take the appropriate steps to properly implement the features, evaluate and administer the various restriction levels, protect access codes, and distribute the access codes only to people whom you advise of the sensitive nature of the access information. Instruct each authorized user to use access codes properly.

In rare instances, unauthorized individuals use the Remote Access feature to make connections to a telecommunications network. In such an event, applicable tariffs require that you pay all network charges for traffic. Avaya cannot be responsible for such charges, and does not make any allowance or give any credit for charges that result from unauthorized access.

The Remote Access caller must access your system from the public network and use a touch tone telephone or equivalent equipment. When a user uses Remote Access, the system does not have access to the calling number, because the calling number is outside the system. Thus, some features and capabilities, such as Ringback Queuing and Automatic Callback, cannot be used on a Remote Access call. Also, the user cannot use any feature that requires recall dial tone, such as, the Hold and Transfer features, from the remote location.

Remote Access provides users with access to the system and system features from the public network. Uses can use Remote Access to make business calls from home or use the Recorded Telephone Dictation Access to dictate a letter. An authorized user can also access system features from any onsite extension.

With Remote Access, you can dial into the system over direct inward dialing (DID), central office (CO), foreign exchange (FX), or 800 service trunks. When a call comes in on a trunk group that is dedicated to Remote Access, the system routes the call to the Remote Access extension that you assigned. If DID is provided, and the Remote Access extension is within the range of numbers that can be accessed by DID, the system uses DID for Remote Access.

You can administer your system so that a user must enter a barrier cod, an authorization code, or both to use Remote Access.

Use barrier codes to secure and define calling privileges through the Class of Restriction (COR) that you administer to users and trunk groups. You can administer as many as 10 barrier codes. Each barrier codes has a different COR and Class of Service (COS). Barrier codes can be from 4 to 7 digits, but all barrier codes that you define must be the same length.

Night Service

You can administer your system to provide attendant-assisted calling during the day, and then Remote Access when the system is in Night Service.

Security

To ensure system security, you can permanently disable the Remote Access feature if you do not intend to use the feature. If you permanently disable Remote Access, you must contact your Avaya representative to activate this feature again.

CAUTION:
Your attempt to disable the Remote Access feature is lost if the server that runs Communication Manager is rebooted without saving translations. Therefore, you must run a **`save translation`** command after you permanently disable the Remote Access feature.

The system provides several ways to secure your system when you use the Remote Access feature:

- The **`status remote-access`** command
- Barrier codes
- Authorization codes
- Alternate Facility Restrictions Levels (AFRLs)
- COR
- Logoff Notification

Status remote-access

You can check the status of the Remote Access feature and the barrier codes. The **`status remote-access`** command displays information that can help you determine when and why the system denied remote access to a user, or why the system blocked a barrier code.

When you type the **`status remote-access`** command, the system displays the:

- Remote Access status:
  - Not administered
  - Enabled
  - Disabled
  - Disabled following detection of a security violation
- Date and time that Remote Access was last modified
- Barrier code information:
  - The date that the code was administered, reactivated, or modified
  - The expiration date
  - The number of calls that can be placed with the code
  - The number of calls that were placed with the code
  - Active or expired status
  - The date and the reason that a code expired

For a detailed description of the **`status remote-access`** command and display, see the *BCS Products Security Handbook*.

Barrier codes

Remote Access has inherent risks, such as large-scale unauthorized long distance use of your telecommunications facilities. To increase the security of your system, use a 7-digit barrier code, and administer expiration dates and access limits for each of the 10 barrier codes that are available to you. If your system has more than 10 Remote Access users, the users must share barrier codes. A barrier code automatically expires if the expiration date or the number of accesses exceeds the limits that you set. You can administer the system to limit:

- The length of time that an access code remains valid
- The number of times that an access code can be used
- Both the length of time that an access code remains valid and the number of times that an access code can be used

When you no longer need a barrier code, remove the code from the system.

If you administer barrier codes, a special answer-back tone causes a calling modem to leave dial mode. Sometimes a modem dialer is used to gain access with Remote Access. When a dialer of a modem is used to gain access with Remote Access, the special answer-back tone cancels echo suppressors on the network. The cancellation of echo suppressors in the network prevents dual-tone multifrequency (DTMF) tones from breaking dial tone from Communication Manager.

Use the **`status remote-access`** command to view the status of a Remote Access barrier code.

Call Detail Recording (CDR) does not track the use of barrier codes.

Authorization codes

You can administer authorization codes to manage access to your system. You can then use Call Detail Recording to track the use of authorization codes. Use the following guidelines to manage the use of authorization codes.

- Assign authorization codes that:
  - Are random, nonconsecutive, and unpredictable
  - Are the maximum code length that the system allows
  - Are unique to each person who uses an authorization code
  - Have the minimum level of calling permissions that a user requires
- Change codes frequently, at least quarterly.
- Delete codes when the codes are no longer needed.
- Delete codes when a user leaves the company, or changes job assignments.
- Use CDR reports to monitor and analyze the use of the codes.

Alternate Facility Restriction Levels

Consider the use of Alternate Facility Restriction Levels (AFRLs) instead of Facility Restriction Levels (FRLs) after normal business hours to restrict where calls can be made over your facilities. Do not restrict callers from summoning emergency services after normal business hours.

Class of Restriction

The COR of an authorization code supersedes the COR of a barrier code.

- Time of Day Routing is controlled by the time-of-day entries in the COR or by the partition.
- Toll Restriction and Analysis is controlled by COR.
- Trunk Access Code (TAC) interacts with toll restriction. You can translate Communication Manager so that users can use ARS to make toll calls, without the need for a TAC.

For additional steps to secure your system, and to obtain security information on a regular basis, see the *Avaya Toll Fraud and Security Handbook*.

Logoff Notification

Use Logoff Notification when you enable Remote Access for your system, but your users are not actively using Remote Access. Logoff Notification notifies you when you log off the system that Remote Access is enabled.

Logoff Notification alerts you to an unauthorized activation of the Remote Access feature. Logoff Notification is administered by login ID.

Administering Remote Access

The following steps are part of the administration process for the Remote Access feature:

- Administering the Remote Access screen
- Assigning authorization codes
- Administering Remote Access for Night Service

This section describes:

- Any prerequisites for administering the Remote Access feature
- The screens that you use to administer the Remote Access feature
- Complete administration procedures for the Remote Access feature

Prerequisites for administering Remote Access

You must complete the following actions before you can administer the Remote Access feature:

- None

Screens for administering Remote Access

Screen name	Purpose	Fields
Authorization Code - COR Mapping	Assign pairs of authorization codes and Classes of Restriction (CORs).	• **AC** • **COR**
Feature-Related System Parameters	Assign the length of the authorization codes.	**Authorization Code Length**
Optional Features	Enable authorization codes.	**Authorization Codes?**

Screen name	Purpose	Fields
Remote Access	Enable Remote Access.	All
	Disable Remote Access	**Permanently Disable?**
Trunk Groups • CO • DID • FX • ISDN-BRI • ISDN-PRI • WATS	Assign Remote Access for Night Service.	• **Incoming Destination** • **Night Services**

Administering the Remote Access screen

To administer Remote Access, you must complete the following procedures:

- Enabling Remote Access
- Disabling Remote Access

Enabling Remote Access

To Enable Remote Access:

1. Type **`change remote-access`**. Press **Enter**.

   The system displays the Remote Access screen (Figure 364: Remote Access screen on page 1421).

Figure 364: Remote Access screen

```
change remote-access

                                REMOTE ACCESS
   Remote Access Extension: ________              Barrier Code Length:____
Authorization Code Required? y              Remote Access Dial Tone: n

     Barrier      COR  TN  COS   Expiration    No. of     Calls
      Code        COR  TN  COS      Date       Calls      Used
   1:________     1__  1_  1__   __/__/__      ______     ______
   2:________     1__  1_  1__   __/__/__      ______     ______
   3:________     1__  1_  1__   __/__/__      ______     ______
   4:________     1__  1_  1__   __/__/__      ______     ______
   5:________     1__  1_  1__   __/__/__      ______     ______
   6:________     1__  1_  1__   __/__/__      ______     ______
   7:________     1__  1_  1__   __/__/__      ______     ______
   8:________     1__  1_  1__   __/__/__      ______     ______
   9:________     1__  1_  1__   __/__/__      ______     ______
  10:_______      1__  1_  1__   __/__/__      ______     ______

Permanently Disable? __ Disable Following A Security Violation? y
(NOTE:  You must logoff to effect permanent disabling of Remote Access)
```

2. In the **Authorization Code Required** field, perform one of the following actions:
   - If you want a user to enter an authorization code to use Remote Access, type **y**.
   - If you do not want a user to enter an authorization code when the user uses Remote Access, type **n**.

   The **Calls Used** field is a display-only field that shows the number of calls that are placed with the corresponding barrier code. The system increments this field whenever a barrier code is successfully used to access the Remote Access feature.
3. In the **Barrier Code** field, perform one of the following actions:
   - Type a barrier code.

     The number that you type in the **Barrier Code Length** field determines the number of digits that you type in this field.
   - If the **Barrier Code Length** field is blank, you must type **none** in the first **Barrier Code** field.

   You can assign 10 barrier codes to your system. You cannot assign duplicate barrier codes.
4. In the **Barrier Code Length** field, type the length of the barrier codes that you want to use in your system. Valid entries are the numbers **4** through **7**. You can also leave this field blank.

5. In the **COR** field, type the COR number that is associated with the barrier code. The barrier code defines the call restriction features.
6. In the **COS** field, type the COS number that is associated with the barrier code. The barrier code defines access permissions for Call Processing features. Valid entries are the numbers **0** to **15**.
7. In the **Disable Following a Security Violation** field, perform one of the following actions:
   - If you want the system to disable the Remote Access feature when the system detects a remote access security violation, type **y**.
   - If you do not want the system to disable the Remote Access feature when the system detects a remote access security violation, type **n**.

   The system displays the **Disable Following a Security Violation** field when the **SVN Authorization Code Violation Notification Enabled** field on the Security-Related System Parameters screen is set to **y**.
8. In the **Expiration Date** field, type the date that you want the barrier code to expire. You must type a date that is greater than the current date. You can also leave the field blank.

   If you assign an expiration date, the system displays a warning message on the System Copyright screen 7 days before the expiration date of the barrier code. If you want to extend the expiration date, change the date in this field.
9. In the **No. of Calls** field, type the number of times that users can use the barrier code for Remote Access. Valid entries are the numbers **1** to **9999**.
10. In the **Permanently Disable?** field, type **n**.
11. In the **Remote Access Dial Tone** field, perform one of the following actions:
    - If you want the system to provide a Remote Access dial tone prompt, type **y**.
    - If you do not want the system to provide a Remote Access dial tone prompt, type **n**.

    SECURITY ALERT:
    To maintain system security, Avaya recommends that you set this field to **n.**

    The system displays this field only when the **Authorization Code Required** field is set to **y**.
12. In the **Remote Access Extension** field, perform one of the following actions:
    - If no barrier codes exist, leave the field blank.
    - If barrier codes exist, type the Remote Access extension.

    The remote access extension is used like a DID extension. Only one DID extension can be assigned as the Remote Access extension. Calls to the Remote Access extension are treated the same as calls on the remote access trunk.
13. In the **TN** field, type the Tenant Partition number. Valid entries are the numbers **1** to **100**.
14. Press **Enter** to save your changes.

Disabling Remote Access

To disable Remote Access:

1. Type **change remote-access**. Press **Enter**.

   The system displays the Remote Access screen (Figure 364: Remote Access screen on page 1421).

2. In the **Permanently Disable?** field, type **n**.
3. Press **Enter** to save your changes.

Assigning authorization codes

Prerequisites

You must complete the following actions before you can assign authorization codes:

- Ensure that authorization codes are enabled on the Optional Features screen.
- Administer the authorization code parameters on the Feature-Related System Parameters screen.

To ensure that authorization codes are enabled on the Optional Features screen:

- On the Optional Features screen, ensure that the **Authorization Codes?** field is set to **y.** If the **Authorization Codes?** field is set to **n**, your system is not enabled for authorization codes. Contact your Avaya representative before you continue with this procedure

  To view the Optional Features screen, type **display system-parameters customer-options**. Press **Enter**.

To administer the authorization code parameters on the Feature-Related System Parameters screen:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen (Figure 365: Feature-Related System Parameters screen on page 1424).

Figure 365: Feature-Related System Parameters screen

```
change system-parameters features                                    page 3
                     FEATURE-RELATED SYSTEM PARAMETERS
                      Reserved Slots for Attendant Priority Queue: 5_
                                      Time Before Off-Hook Alert: 10__
                           Emergency Access Redirection Extension: ________
             Number of Emergency Calls Allowed in Attendant Queue: __
                                          Call Pickup Alerting? n
                      Temporary Bridged Appearance on Call Pickup? y
                                   Call Pickup on Intercom Calls? y
                                          Directed Call Pickup? n
                                     Extended Group Call Pickup: flexible
                Deluxe Paging and Call Park Timeout to Originator? n
    Controlled Outward Restriction Intercept Treatment: tone
   Controlled Termination Restriction (Do Not Disturb): tone
            Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS           Authorization Code Enabled? y
                                         Authorization Code Length: 7
                           Authorization Code Cancellation Symbol? #
                                            Attendant Time Out Flag? n
                                     Display Authorization Code? _
                 Controlled Toll Restriction Replaces: station-station
          Controlled Toll Restriction Intercept Treatment: extension     3000
```

2. In the **Authorization Codes Enabled?** field, perform one of the following actions:
   - If you want the users to use authorization codes, type **y**.
   - If you do not want the users to use authorization codes, type **n**.

   You can administer this field only if the **Authorization Codes?** field on the Optional Features screen is set to **y**.

   SECURITY ALERT:
   To maintain system security, Avaya recommends that you set the **Authorization Codes Enabled?** field to **y**.

3. In the **Authorization Code Length** field, type the length of the authorization codes. Authorization codes must be between 4 and 13 digits long.

   The system displays this field only if the **Authorization Codes Enabled?** field is set to **y**.

   SECURITY ALERT:
   To maintain system security, Avaya recommends that you use the maximum length for the authorization code.

4. In the **Authorization Code Cancellation Symbol** field, perform one of the following actions:

- If both the main server and the tandem server are the same type of server, type a pound sign (#).
- If an Avaya System 85 or a DIMENSION is involved, type the number **1**.

A user dials the authorization code cancellation symbol to cancel the 10-second wait period, during which the user can enter an authorization code

The system displays this field only when the **Authorization Codes Enabled?** field is set to **y**.

5. In the **Attendant Time Out Flag** field, perform one of the following actions:
   - If you want the system to route a call to the attendant if a user does not dial an authorization code within the 10-second wait period, or if a user dials an invalid authorization code, type **y**.
   - If you do not want the system to generate an intercept tone if a user does not dial an authorization code within the 10-second wait period, or if a user dials an invalid authorization code, type **n**.

   The system displays this field only when the **Authorization Codes Enabled?** field is set to **y**.
6. In the **Display Authorization Code?** field, perform one of the following actions:
   - If you want the system to display the authorization code as the user dials the authorization code, type **y**.
   - If you do not want the system to display the authorization code as the user dials the authorization code, type **n**.

   This field applies only to digital communication protocol (DCP) telephones. The field does not apply to ISDN-BRI or hybrid sets.

   SECURITY ALERT:
   To enhance the security of your system, Avaya recommends that you set the **Display Authorization Code?** field to **n**.
7. Press **Enter** to save your changes.

To assign authorization codes:

1. Type **`change authorization-code`**. Press **Enter**.

   The system displays the Authorization Code - COR Mapping screen (Figure 366: Authorization Code - COR Mapping screen on page 1426).

Figure 366: Authorization Code - COR Mapping screen

```
change authorization-code                                          Page 1 of 1
                        Authorization Code - COR Mapping
      Note:    XX codes administered.  Use "list" to display all codes.
     AC    COR   AC    COR   AC    COR   AC    COR   AC    COR   AC    COR

    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
    _______ __  _______ __  _______ __  _______ __  _______ __  _______ __
```

The **Number of Codes Administered** field is a display-only field. This field contains the number of authorization codes that you administered on the Authorization Code - COR Mapping screen. The system limits the number of authorization codes that you can administer. To determine the number of authorization codes that you can administer, type **`display capacity`**.

2. In the **AC** field, type the length of the authorization codes. Authorization codes must be between 4 and 13 digits long.

   The number of digits that you type in this field must be the number of digits that you assigned to the **Authorization Code Length** field on the Feature-Related System Parameters screen.

3. In the **COR** field, type the Class of Restriction (COR) that the system uses when a user enters the associated authorization code.

4. Press **Enter** to save your changes.

Administering Remote Access for Night Service

To administer Remote Access for Night Service:

1. Type **`change trunk-group`** ***`n`***, where ***`n`*** is the number of the trunk group for which you want to administer Remote Access for Night Service. Press **Enter**.

   The system displays the Trunk Group screen.

2. In the **Incoming Destination** field, type **attd**.

   The system displays the **Incoming Destination** field, when the **Direction** field is set to **incoming** or **two-way**.

3. In the **Night Service** field, type the Remote Access extension.
4. Press **Enter** to save your changes.

End-user procedures for Remote Access

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Remote Access:

- Accessing the attendant

To access the attendant:

1. Enter the Remote Access extension.
2. Enter the barrier code.
3. Enter the attendant access code.

Reports for Remote Access

The following reports provide information about the Remote Access feature:

- None.

Considerations for Remote Access

This section provides information about how the Remote Access feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Remote Access under all conditions. The following considerations apply to Remote Access:

- After the baud of a digital-terminal data module (DTDM) is changed from 9600 to 1200, the DTDM cannot be accessed by Remote Access until an internal call is made to the DTDM.

Interactions for Remote Access

This section provides information about how the Remote Access feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Remote Access in any feature configuration.

- Authorization Codes

  When a Remote Access caller dials the assigned Remote Access extension and connects to the system, the system can request the caller to dial an authorization code in addition to a barrier code. Dial tone between the barrier code and authorization code is optional. Calling privileges that are associated with the Class of Restriction (COR) that is assigned to the authorization code supersede the calling privileges that are assigned to the barrier code.

- Call Detail Recording (CDR)

  CDR tracks the use of authorization codes. CDR does not track the use of barrier codes.

- Class of Restriction (COR)

  COR restrictions do not block access to the Remote Access feature.

- Night Service

  You can specify the Remote Access extension as the Night Service extension on incoming,
  non-direct inward dialing (DID) trunk groups.

Restriction - Controlled

Use the Restriction - Controlled feature to allow a user with console permission to:

- Activate and deactivate specific restrictions for an individual user or an attendant
- Activate and deactivate specific restrictions for all users or attendants who have a specific Class of Restriction (COR)

Detailed description of Restriction - Controlled

This section provides a detailed description of the Restriction - Controlled feature.

With Restriction - Controlled, a user with console permissions can:

- Activate and deactivate specific restrictions for an individual user or an attendant
- Activate and deactivate specific restrictions for all users or attendants who have a specific Class of Restriction (COR)

Use Restriction - Controlled to administer the following restrictions:

- Outward

  The user cannot place calls to the public network.

- Total

  The user cannot place or receive calls, with the following exceptions:

  - Calls to a remote-access extension
  - Terminating-trunk transmission tests
  - Emergency Access to Attendant calls

- Termination

  The user cannot receive any calls. The system:

  - Routes incoming calls to the attendant
  - Redirects calls to the Call Coverage path
  - Uses Restriction - Controlled intercept treatment

- Station-to-Station

  The user cannot place or receive station-to-station calls.

Administering Restriction - Controlled

This section describes the screens that you use to administer the Restriction - Controlled feature.

Screens for administering Restriction - Controlled

Screen name	Purpose	Fields
Feature Access Code (FAC)	Specify the Feature Access Codes (FACs) for Restriction - Controlled.	• **User Control Restrict Activation and Deactivation** • **Group Control Restrict Activation and Deactivation**
Feature-Related System Parameters	Specify the type of intercept treatment that the system uses for Restriction - Controlled.	• **Controlled Outward Restriction Intercept Treatment** • **Controlled Termination Restriction (Do Not Disturb)** • **Controlled Station-to-Station Restriction**

End-user procedures for Restriction - Controlled

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Restriction - Controlled:

- Activating Restriction - Controlled

Activating Restriction - Controlled

To activate Restriction - Controlled:

1. Dial the Feature Access Code (FAC) that allows you to apply Restriction - Controlled to an extension or an attendant group.
2. Dial the number for the type of restriction that you want:
   - **1** for outward
   - **2** for total
   - **3** for termination
   - **4** for station-to-station
3. Perform one of the following actions:
   - If you want to apply Restriction Controlled to an individual extension, dial the extension.
   - If you want to apply Restriction Controlled to all users and attendant who are assigned a certain Class of Restriction (COR), dial the number of the class of restriction (COR).

Reports for Restriction - Controlled

The following reports provide information about the Restriction - Controlled feature:

- None

Considerations for Restriction - Controlled

This section provides information about how the Restriction - Controlled feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Restriction - Controlled under all conditions. The following considerations apply to Restriction - Controlled:

- All telephones with the same COR are affected by a group restriction. When a call is placed, the system checks both the individual and the group restrictions.

Interactions for Restriction - Controlled

This section provides information about how the Restriction - Controlled feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Restriction - Controlled in any feature configuration.

- Call Coverage

  The system does not check controlled restrictions for covering users.

- Call Forwarding

  The system checks the controlled restrictions for the forwarded-to extension, when Call Forwarding All Calls is active.

- Class of Restriction (COR)

  The system checks the COR when a call is authorized.

- Priority Call

  If a user activates priority calling before the user dials another extension, the calling user receives intercept tone. The user receives the intercept tone whether you set **Controlled Station to Station Restriction** field on the Feature-Related System Parameters form to **y** or **n**.

- Uniform Call Distribution (UCD)

  The system does not apply Restriction - Controlled to calls that are dialed through the Uniform Dial Plan (UDP).

Ringing - Abbreviated and Delayed

Use the Ringing - Abbreviated and Delayed feature to assign one of four ring types to each call appearance on a telephone. The ring type that you assign to a call appearance is automatically assigned to each of the bridged call appearances of each call appearance.

Detailed description of Ringing - Abbreviated and Delayed

This section provides a detailed description of the Ringing - Abbreviated and Delayed feature.

The Ringing - Abbreviated and Delayed feature has two categories of ringing:

- Ringing that alerts consistently and does not change:
  - Ringing, in which the lamp flashes and audible ringing occurs
  - Silent ringing, in which the lamp flashes and audible ringing does not occur
- Ringing that transitions from one ringing state to another:
  - Abbreviated ringing, in which ringing continues for the number of cycles that you specify with the automatic abbreviated transition interval or the delayed transition interval, and then changes to silent alerting
  - Delayed ringing, in which visual alerting continues for the number of cycles that you specify with the automatic abbreviated transition interval or the delayed transition interval, and then changes to ringing

When you administer the Station screen of a user, you can assign an abbreviated dial button of that user to another user. The user of the Station screen that you administer must have a telephone with call appearances that have either abbreviated or delayed ringing. When a call alerts at one of those call appearances, the user presses the button. When the user presses the button, the system forces an immediate transition from ringing to silence, or from silence to ringing.

The Ringing - Abbreviated and Delayed feature is most useful in bridging situations in which some users want to:

- Have a call audibly alert as soon as the call arrives
- Be audibly notified if the call is unanswered within a specified number of rings
- Stop the audible alerting if the call is unanswered by the called party, and the user cannot answer the call

You specify the types of ringing on the Station screen of each user in your system. You can assign one of the following ring types to each telephone line button.

- Abbreviated Ring

  A call rings the telephone until the automatic or the manual automatic abbreviated transition or the delayed transition occurs. After the transition, the call silently alerts at the telephone.

- Delayed Ring

  A call silently alerts the telephone until the automatic or the manual abbreviated transition or the delayed transition occurs. After the transition, the call rings at the telephone.

- No Ring

  A call silently alerts the telephone and does not transition.

- Ring

  A call rings at the telephone and does not transition.

When a user presses the abbreviated-ring button on the telephone, the system performs an abbreviated transition or a delayed transition for all calls at the extension. Calls to other extensions that alert at the telephone are unaffected.

Administering Ringing - Abbreviated and Delayed

The following steps are part of the administration process for the Ringing - Abbreviated and Delayed feature:

- Assigning ring control to a user
- Assigning an abbreviated ringing button to a user

This section describes:

- Any prerequisites for administering the Ringing - Abbreviated and Delayed feature
- The screens that you use to administer the Ringing - Abbreviated and Delayed feature
- Complete administration procedures for the Ringing - Abbreviated and Delayed feature

Prerequisites for administering Ringing - Abbreviated and Delayed

You must complete the following actions before you can administer the Ringing - Abbreviated and Delayed feature:

- Assign the number of rings before a transition

To assign the number of rings before a transition:

1. Type **change system-parameters features**. Press **Enter**.

   The system displays the Figure 367: Feature-Related System Parameters on page 1435).

Figure 367: Feature-Related System Parameters

```
change system-parameters features                                    page 1
                        FEATURE-RELATED SYSTEM PARAMETERS
                           Self Station Display Enabled? n
                                Trunk-to-Trunk Transfer? none
 Automatic Callback - No Answer Timeout Interval (rings): 4_
                    Call Park Timeout Interval (minutes): 10
    Off-Premises Tone Detect Timeout Interval (seconds): 20_
                              AAR/ARS Dial Tone Required? y
                                      Music/Tone On Hold: music    Port: _____
          Music (or Silence) On Transferred Trunk Calls: all
                    DID/Tie/ISDN/SIP Intercept Treatment: attd

 Internal Auto-Answer of Attd-Extended/Transferred Calls? y
              Automatic Circuit Assurance (ACA) Enabled? y
                                      ACA Referral Calls: local
                                ACA Referral Destination: ________
            ACA Short Holding Time Originating Extension: ______
             ACA Long Holding Time Originating Extension: ______
         Abbreviated Dial Programming by Assigned Lists:
    Auto Abbreviated/Delayed Transition Interval(rings):
                  Protocol for Caller ID Analog Terminals: Bellcore
 Display Calling Number for Room to Room Caller ID Calls?
```

2. In the **Auto Abbreviated/Delayed Transition Interval (rings)** field, type the number of rings before the system performs an automatic abbreviated transition or delayed transition for a call. You can type a number from **1** to **16**.
3. Press **Enter** to save your changes.

Screens for administering Ringing - Abbreviated and Delayed

Screen name	Purpose	Fields
Feature-Related System Parameters	Assign the number of rings before the system performs an automatic abbreviated transition or a delayed transition for a call.	**Auto Abbreviated/Delayed Transition Interval (rings)**

Screen name	Purpose	Fields
Station	Allow a user to select ringing for call appearances.	**Per Button Ring Control**
	Assign an **abrv-ring** button to a user.	Any available button field in the **Feature Buttons** area

Assigning ring control to a user

To assign ring control to a user:

1. Type **`change station n`**, where ***n*** is the number of the extension to which you want to assign ring control for a user. Press **Enter**.

   The system displays the Station screen.

2. Click **Next** until you see the **Per Button Ring Control** field (Figure 368: Station screen on page 1436).

Figure 368: Station screen

```
change station 75001                                          Page 2 of 4

                                    STATION

FEATURE OPTIONS
           LWC Reception? spe                Auto Select Any Idle Appearance? n
          LWC Activation? y                          Coverage Msg Retrieval? y
  LWC Log External Calls? n                                Auto Answer: none
              CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n            Per Station CPN - Send Calling Number? _
       Service Link Mode: as-needed
         Multimedia Mode: basic
    MWI Served User Type: ______                 Display Client Redirection? n
         Automatic Moves:
              AUDIX Name:                       Select Last Used Appearance? n
                                                  Coverage After Forwarding? _
     Recall Rotary Digit? n                         Multimedia Early Answer? n

Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001                          IP Audio Hairpinning? n
```

3. In the **Per Button Ring Control** field, perform one of the following actions:
   - Type **y** if you:
     - Want users to select ringing individually for each call appearance, bridged call appearance, or analog bridged call appearance on the telephone, and
     - Want to enable the automatic abbreviated and delayed ring transition for each call appearance on the telephone, and
     - Do not want the system to automatically move the line selection to a silently alerting call, unless that call was audibly ringing earlier
   - Type **n** if you want:
     - Calls on call-appr buttons to always ring the telephone, and
     - The value in the **Bridged Call Alerting** field of the Station screen to control whether calls ring on the brdg-appr or the abrdg-appr buttons, and
     - The system to move the line selection to a silently alerting call, if no call is audibly ringing the telephone
4. Press **Enter** to save your changes.

Assigning an abbreviated ringing button to a user

To assign an abbreviated and delayed feature button to a user:

1. Type **`change station n`**, where ***n*** is the number of the extension to which you want to assign an abbreviated and delayed feature button for a user. Press **Enter**.

   The system displays the Station screen.
2. Click **Next** until you see the **Button Assignments** area (Figure 369: Station screen on page 1438).

Figure 369: Station screen

```
change station 32009                                        Page 3 of 4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          7:
 2: call-appr                          8:
 3: call-appr                          9:
 4: abrv-ring  Ext:                   10:
 5:                                   11:
 6: headset                           12: release
```

3. Type **abrv-ring** next to the button that you want the user to use to cause a call that rings to transition from ringing to silence, or silence to ringing.

   When you type **abrv-ring** next to the button, the system displays an **Ext:** field.

4. (Optional) In the **Ext:** field, type the extension of the other user to whom you want to assign the abbreviated ringing button.
5. Press **Enter** to save your changes.

Reports for Ringing - Abbreviated and Delayed

The following reports provide information about the Ringing - Abbreviated and Delayed feature:

- None

Considerations for Ringing - Abbreviated and Delayed

This section provides information about how the Ringing - Abbreviated and Delayed feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Ringing - Abbreviated and Delayed under all conditions. The following considerations apply to Ringing - Abbreviated and Delayed:

- You cannot assign Ringing - Abbreviated and Delayed to an attendant console.
- You can assign the Ringing - Abbreviated and Delayed feature to analog telephones. However, because analog telephones cannot visually alert, a user can unexpectedly answer an incoming call, when the user intends to originate a call.

Interactions for Ringing - Abbreviated and Delayed

This section provides information about how the Ringing - Abbreviated and Delayed feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Ringing - Abbreviated and Delayed in any feature configuration.

- Call Coverage

  If the number-of-rings interval for coverage is shorter than the automatic transition interval, the system redirects the call to coverage before the system audibly alerts a call appearance that has delayed ringing. However, the system continues to increment the timer for the automatic transition interval, in case no coverage point is available, and the call continues to alert at the telephone.

  When a call is immediately redirected to coverage, the Ringing - Abbreviated and Delayed ringing has no effect on the system processes.

- Call Forwarding - Busy/Don’t Answer

  When the system forwards a call because no one answers the call in the specified interval, the call stops alerting at the telephone. The Ringing - Abbreviated and Delayed feature does not affect the manner in which the system processes the call. However, the system continues to increment the timer for the automatic transition interval, in case forwarding fails, and the call continues to alert at the telephone.

  If the interval for call forward don’t answer is shorter than the interval for automatic transition, the system redirects the call to the forwarded-to extension before the call rings at a telephone that has a ring type of delayed ringing.

- Call Vectoring - Expert Agent Selection - Logical Agents

  Calls that the system routes to a logical agent use the translations for the Ringing - Abbreviated and Delayed feature of the telephone that the agent uses.

- Data Extension Calls

  Data Extension calls are unaffected by the ring values. The calls continue to be directed according to the way that you administered bridged call alerting.

- Hospitality Features - Do Not Disturb

  The Do Not Disturb feature takes precedence over the Ringing - Abbreviated and Delayed feature in blocking ringing to the telephone.

- Integrated Services Digital Network (ISDN) - World Class Basic Rate Interface (BRI)

  Several of the protocol variations that the World Class BRI feature supports do not allow the messaging that is required for control of a telephone ringer by the Ringing - Abbreviated and Delayed feature. If the protocol variations do not permit the required messaging for the telephone ringer, the system rings the call at the telephone, and does not transition the ring.

- Multiappearance Preselection and Preference

  If the **Per Button Ring Control** field on the Station screen is set to **n**, the system automatically selects any call that alerts at a telephone. The call can alert in a manner other than ringing.

  If the **Per Button Ring Control** field on the Station screen is set to **y**, the system automatically selects any call that rings at a telephone.

- Off-Premises Station (OPS) and Off-Premises Extension (OPX) lines

  You must use a ring type of **ring** for OPS and OPX lines.

- Personal Central Office Line (PCOL) calls

  Ring values do not affect the processing of PCOL calls. PCOL calls continue to be directed according to the way that you administer bridged call alerting.

- Redirection Notification

  If you enable Redirection Notification, telephones receive redirection notification only if the alerting button, or the first call appearance, has an assigned ring value of **ring** or **abrv-ring**.

- Terminating Extension Group (TEG) calls

  Ring values do not affect the processing of TEG calls. TEG calls continue to be directed according to the way that you administer bridged call alerting.

- Voice mail systems

  Voice mail systems might look for ringing that is applied to a port to trigger call answer. Ring-type translations that are inappropriately set for ports that serve a voice mail system, can result in undesirable operation of the adjunct.

Security Violation Notification

Use the Security Violation Notification (SVN) feature to notify a designated referral point about a possible security violation. A designated referral point can be an attendant console, a display-equipped telephone, or a telephone without a display for SVN referral calls with announcements.

The system monitors and reports on the following types of security violations:

- Login violations
- Remote access barrier code violations
- Authorization code violations
- Station security code violations

Communication Manager provides the option to log a major alarm if a security violation occurs involves an Avaya services login ID. Avaya is responsible for retiring the alarm.

Detailed description of Security Violation Notification

This section provides a detailed description of the Security Violation Notification (SVN) feature:

- Security violation thresholds and notification
- Sequence of events
- Reporting
- SVN - halt buttons
- SVN Referral Call With Announcement
- Dealing with Security Violations

To effectively monitor the security of your system, you must know how often both valid and invalid attempts at system entry are normally made. A significant increase in such attempts can mean the system is being compromised.

Note:
Avaya recommends that you print and clear the security violation measurement reports at least once a month. In a busy system, you must print security-violation measurement reports often.

Security violation thresholds and notification

For example, you might determine that during a 40 hour week, the normal condition is for users to submit about 1,000 valid barrier codes and 150 invalid barrier codes. That is, about 3.75 invalid barrier codes submitted per hour.

With this information, you might decide to declare that a security violation occurs during any hour in which eight invalid barrier codes are submitted. If you know that during an 8-hour period, about 30 invalid codes are submitted, you might set the threshold to count a security violation when 40 invalid codes are submitted within eight hours.

You can administer SVN to place a referral call to the location of your choice whenever the established thresholds are reached. All SVN referral calls are priority calls.

Invalid attempts accumulate at different rates for login, authorization-code, remote-access, and station-security code depending on feature usage and the number of users on a server. For this reason, you administer thresholds separately for each type of violation.

Sequence of events

The following sequence of events occurs when an SVN is enabled and a detects a security violation:

1. The number of invalid attempts that are permitted in a specified time interval is exceeded.
2. An SVN referral call (with announcements, if assigned) is placed to a designated point, and SVN provides an audit trail that contains information about each attempt to access server that is running Communication Manager.
3. SVN disables a login ID or remote access following the security violation.
4. The login ID or remote access remains disabled until someone with an authorized login ID, with the correct permissions reenables it.

Reporting

The system reports information about security violations in the following ways:

- In real time. You can use the **`monitor security-violations`** command to monitor security violations as they may be occurring. Enter this command, and then the type of security violation you want to monitor (logins, remote-access, authorization-codes, or station-security-codes).

- On an immediate basis. When a security violation occurs, the system sends a priority call to a designated referral point (attendant console or phone). Thus, there is some chance of apprehending the violator during the attempted violation.

  Upon notification, you can request the Security Violations Status Reports, which show details of the last 16 security violations of each type. The Barrier Code and Authorization Code reports, also include the calling party number from which the attempt was made, where available.

- On a historical basis. The number of security violations of each type and other security measurements, are collected and displayed in the Security Violations Summary and Detail reports. These reports show summary information since the counters were reset by the **`clear measurements security-violations`** command or since system initialization. These reports do not show all aspects of the individual security violations.

SVN - halt buttons

You can administer buttons for the notification extension to stop notification calls. However, this might pose a security risk. Do not use these buttons if you do not really need them.

To find out what svn - halt buttons exist in the system, type **`display svn-button-location`**. Press **Enter**.

SVN Referral Call with Announcement

The SVN Referral Call with Announcement option can provide a recorded message with the referral call identifying the type of violation. You can use Call Forwarding, Call Coverage, or Call Vector Time-of-Day Routing to route to an extension or a number off the media server or switch. SVN referral calls with announcements terminate to a point that is either on or off the switch.

Use of other means to route SVN referral calls to alternate destinations are not supported at this time. An attempt to use an alternate method to route SVN referral calls might result in a failure to receive the call or to hear the announcement.

Dealing with Security Violations

When a security violation occurs, you can disable the login ID or the remote access privileges of the user who commits the violation.

Disabling a login ID

To disable a login for one of your users:

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Type **disable login *n***, where ***n*** is the login ID of the user. Press **Enter**.

Enabling a login ID

To enable a login ID:

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Type **enable login *n***, where ***n*** is the login ID of the user. Press **Enter.**

Enabling remote access

To enable remote access:

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Type **enable remote-access**. Press **Enter**.

Disabling remote access

To disable remote access:

1. Log in to Communication Manager with a login ID that has the correct permissions.
2. Type **disable remote-access.** Press **Enter**.

Administering Security Violation Notification

The following steps are part of the administration process for the Security Violation Notification (SVN) feature:

- Setting up Security Violation Notification

This section describes:

- Any prerequisites for administering the Security Violation Notification (SVN) feature
- The screens that you use to administer the Security Violation Notification (SVN) feature
- Complete administration procedures for the Security Violation Notification (SVN) feature

Prerequisites for administering Security Violation Notification

- None

Screens for administering Security Violation Notification

Screen name	Purpose	Fields
Login Administration	Set up security violation notification.	**Disable Following A Security Violation**
Security-Related-System Parameters	Set up security violation notification.	• **SVN Login Violation Notification** • **Originating Extension** • **Referral Destination** • **Login Threshold** • **Time Interval**
Remote Access	Set up security violation notification.	**Disable Following A Security Violation**
Station	Set up security button assignments.	Any available button field in the **Button Assignments** area

Setting up Security Violation Notification

To set up Security Violations Notification:

1. Type **`change system-parameters security`.** Press **Enter.**

   The system displays the Security-Related System Parameters screen (Figure 370: Security Related System Parameters screen on page 1446).

Figure 370: Security Related System Parameters screen

```
change system-parameters security                                Page 1 of 2

                     SECURITY-RELATED SYSTEM PARAMETERS

SECURITY VIOLATION NOTIFICATION PARAMETERS

  SVN Login Violation Notification Enabled? y
        Originating Extension: 3040_ Referral Destination: attd_
              Login Threshold: 3_           Time Interval: 0:03
       Announcement Extension: ________

  SVN Remote Access Violation Notification Enabled? y
        Originating Extension: 2719_ Referral Destination: 2720_
       Barrier Code Threshold: 3            Time Interval: 0:03
       Announcement Extension: ________

  SVN Authorization Code Violation Notification Enabled? y
        Originating Extension: 3030_ Referral Destination: 3031_
 Authorization Code Threshold: 3            Time Interval: 0:03
       Announcement Extension: ________
```

2. In the **SVN Login Violation Notification Enabled** field, type **y**.

   This action sets Security Violation Notification login violation notification.

   Note:
   If you are not using Security Violation Notification for logins, type **n** in the **SVN Login Violation Notification Enabled** field and go to Step 11.

3. In the **Originating Extension** field, type **3040**.

   This becomes the phone extension for the purpose of originating and identifying SVN referral calls for login security violations.

4. In the **Referral Destination** field, type **attd** to send all calls to the attendant.

   This is the extension of the telephone that receives the referral call when a security violation occurs.

5. In the **Login Threshold field**, type **3**.

   This is the minimum number of login attempts that are permitted before a referral call is made. More than 3 attempts causes a security violation notification.

6. In the **Time Interval** field, type **0:03**.

   This the time interval in which the threshold, or number of violations, must occur.

7. Press **Enter** to save your changes.

8. (Optional) Type **change login** ***nnnn***, where ***nnnn*** is your login ID.

   The system displays the Login Administration screen (Login Administration screen on page 1447).

Figure 371: Login Administration screen

```
add login                                                    Page 1 of 2
                              LOGIN ADMINISTRATION

               Password of Login Making Change:

           LOGIN BEING ADMINISTERED
                            Login's Name:xxxxxxx
                              Login Type:
                           Service Level:
    Disable Following a Security Violation?
                                                  Access to INADS Port? _

          LOGIN'S PASSWORD INFORMATION
                         Login's Password:
                  Reenter Login's Password:
        Password Aging Cycle Length (Days):

        LOGOFF NOTIFICATION
          Facility Test Call Notification?     Acknowledgment Required?
               Remote Access Notification?     Acknowledgment Required?

ACCESS SECURITY GATEWAY PARAMETERS
Access Security Gateway?
```

9. (Optional) In the **Disable Following A Security Violation** field, type **y**.

   This disables a login following detection of a login security violation for the login you are administering.

10. Press **Enter** to save your changes.

Note:
If you are not using Remote Access, go to Step 14.

11. (Optional) Type **change remote-access**. Press **Enter**.

    The system displays the Remote Access screen (Figure 372: Remote Access screen on page 1448).

Figure 372: Remote Access screen

```
                                REMOTE ACCESS
   Remote Access Extension_________          Barrier Code Length____
Authorization Code Required? y                  Remote Access Dial Tone: n

Barrier Code    COR  TN  COS    Expiration Date   No. of Calls    Calls Used
1:_________     1__  1_  1__    __/__/__         ______          ______
2:_________     1__  1_  1__    __/__/__         ______          ______
3:_________     1__  1_  1__    __/__/__         ______          ______
4:_________     1__  1_  1__    __/__/__         ______          ______
5:_________     1__  1_  1__    __/__/__         ______          ______
6:_________     1__  1_  1__    __/__/__         ______          ______
7:_________     1__  1_  1__    __/__/__         ______          ______
8:_________     1__  1_  1__    __/__/__         ______          ______
9:_________     1__  1_  1__    __/__/__         ______          ______
10:________     1__  1_  1__    __/__/__         ______          ______

Permanently Disable? __ Disable Following A Security Violation? y
(NOTE:  You must logoff to effect permanent disabling of Remote Access)
```

12. (Optional) In the **Disable Following A Security Violation** field, type **y**.

    This disables remote access following detection of a remote access security violation.

13. (Optional) Press **Enter** to save your changes.

14. Type **change station *n***, where ***n*** is the station that you want to assign to the notification halt button. Press **Enter**.

    The system displays the Station screen.

15. Click **Next** until you see the **Button Assignments** area (Figure 373: Station screen on page 1449).

Figure 373: Station screen

```
                                                              Page 3 of 4
                                      STATION
     SITE DATA
          Room: _______                                  Headset? n
          Jack: ___                                      Speaker? n
         Cable: ___                                     Mounting: d
         Floor: _______                             Cord Length: 0_
      Building: _______                               Set Color: _____


ABBREVIATED DIALING
     List1: ________          List2: _________          List3: _________

BUTTON ASSIGNMENTS
 1: asvn-halt                          4: ________
 2: ________                           5: ________
 3: ________
```

16. In the **Button Assignments** area, type one of the following values:
    - **asvn-halt** - The Authorization Code Security Violation Notification call is activated when an authorization code security violation is detected. This applies only if you are using authorization codes.
    - **lsvn-halt** - The Login Security Violation Notification call is activated a referral call when a login security violation is detected.
    - **rsvn-halt** - The Remote Access Barrier Code Security Violation Notification call is activated as a call referral. This applies only if you are using Remote Access barrier codes.
    - **ssvn-halt** - The Station Code Security Violation Notification call is activated when a station code security violation is detected. This applies only if you are using station codes.

    Note:
    Any of the above four security violations causes the system to place a notification call to the designated telephone. The call continues to ring until answered. To stop notification of any further violations, press the button associated with the type of violation.
17. Press **Enter** to save your changes.

Reports for Security Violation Notification

The following reports provide information about the Security Violation Notification feature:

- The Security Violations Status Report shows details of the last sixteen violations of each type. The Barrier Code and Authorization Code reports also include the calling party number from which the attempt was made, if that number is available.

For detailed information on these reports and the associated commands, see *Avaya Aura™ Communication Manager Reports*, 555-233-505.

Considerations for Security Violation Notification

This section provides information about how the Security Violation Notification feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Security Violation Notification under all conditions. The following considerations apply to Security Violation Notification:

- You may administer only one referral destination per system for each type of violation.
- Use caution when you administer bridged appearances for stations that are used as SVN referral destinations. SVN referral calls terminating to bridged appearances *must* be accompanied by an announcement message or *must* route to bridge appearances equipped with a display module. SVN referral calls that do not have an announcement and terminate to a bridged appearance that does not have a display to provide an indication of the nature of the call.
- An authorization code violation with remote access generates two SVNs. One displays authorization code violation and the second SVN displays barrier code violation, even though the correct barrier code was input. These two displays help you determine that the violation took place in the context of a remote access attempt, and not an attempt to place an outgoing call to an ARS trunk.

Interactions for Security Violation Notification

This section provides information about how the Security Violation Notification feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Security Violation Notification in any feature configuration.

- Call Coverage, Call Forwarding, and Call Pickup

  These features are supported for SVN only if you use recorded announcements.

- Centralized Attendant Services (CAS)

  CAS attendants cannot receive SNV referral calls from branch locations.
- Distributed Communications System (DCS)

  SVN does not support referral calls across a DCS network.

Separation of Bearer and Signaling

Use the Separation of Bearer and Signaling feature to reduce the costs of private leased lines. The Separation of Bearer and Signaling (SBS) feature provides a feature set similar to Distributed Communications Service Plus (DCS+). The SBS feature uses the Public Switched Telephone Network (PSTN) for bearer (voice) element, and QSIG private network signaling over a low-cost IP Network for the signaling element of calls. SBS is available only with Communication Manager.

Detailed description of Separation of Bearer and Signaling

This section provides a detailed description of the Separation of Bearer and Signaling (SBS) feature.

SBS provides a low-cost, virtual private network (VPN) over IP trunks with the high voice quality that is expected of the PSTN. By using SBS, you can save on the costs of private leased lines.

The Separation of Bearer and Signaling (SBS) feature provides a Distributed Communications Service Plus (DCS+)-like feature set using the Public Switched Telephone Network (PSTN) for the bearer (voice) element, and QSIG private network signaling over a low-cost IP Network for the signaling element of calls.With SBS Distributed Communication System Plus (DCS+), you can replace an expensive VPN service if you need Dial Plan Expansion (DPE) functionality. Therefore, you can get enhanced signaling without private leased lines. DCS does not work with 6-digit or 7-digit dial plans. Although QSIG works with 6-digit or 7-digit dial plans, QSIG does not work over VPNs. These VPNs include SDN from AT&T or V-Net from MCI.

SBS also provides a transport mechanism for application data, and other enhanced functionality in locations where ISDN trunking is unavailable or expensive.

The SBS feature supports:

- QSIG private network signaling over a low-cost, IP-based network
- Voice calls, or bearer traffic, over the PSTN
- Correct association between QSIG feature signaling information and each voice call.

You must always use Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or Uniform Dial Plan (UDP) to originate an SBS call. You cannot use a Trunk Access Code (TAC) or a Dial Access Code to originate an SBS call.

Note:

This SBS feature is strictly a proprietary Communication Manager implementation and does not operate with non-Communication Manager systems. There is no known industry standard that supports Separated Bearer and Signaling calls.

When a user dials a call that is routed to an SBS trunk, two different and separate calls originate. One call carries the signaling portion of the call and the other carries the bearer portion of the call. The following is a high level description of a point to point SBS call.

Call originated

- A signaling call is setup between the SBS Originating Node and the SBS Terminating Node (SETUP and Call PROCEEDING messages).
- An initial SETUP message is sent which has the final destination extension number as the *called party*.

Complete Number constructed

- The SBS Terminating Node selects a new extension type, SBS Extension, to use for the duration of the call setup. This new extension type indicates that the call was received on an SBS trunk group.
- The SBS Terminating Node, using the *public unknown-numbering* table, constructs a Complete Number (area/city/extension) for the SBS extension.
- The SBS Terminating Node then adds its country code to the Complete Number and sends this entire number (country code/area/city/extension) to the SBS Originating Node (INFO message).
- This new number allows the SBS Originating Node to establish the bearer call to the SBS Terminating Node.

Complete Number launched to SBS Terminating Node

- The SBS Originating Node receives the Complete Number from the SBS Terminating Node and compares the country code in the Complete Number to its own country code.
- If the country codes match, the SBS Originating Node discards the country code.

  or

  If the country codes do not match, the SBS Originating Node adds its International Access Code to the Complete Number.
- The SBS Originating Node uses Automatic Route Selection (ARS) to launch a call to the SBS Terminating Node using the Complete Number. ARS is always used to launch the bearer call. ARS uses normal call routing (ARS analysis to pattern/preference) to complete the call. Through the use of digit conversion, for example, the call can be routed using AAR and a private network.

Call completed

- The SBS Terminating Node receives the bearer call to the SBS Extension.
- The SBS Terminating Node determines which SBS signaling call is currently using this particular SBS Extension. The SBS Terminating Node provides a unique ID over the signaling call (INFO message) to the SBS Originating Node.

- The SBS Originating Node passes the unique ID back to the SBS Terminating Node, through DTMF digits over the bearer call.
- The SBS Terminating Node uses the DTMF unique ID to verify that the bearer call is the "correct" call to associate with the signaling call.
- Once the SBS Terminating Node has associated the signaling and bearer call it completes the call to the called party and returns an ALERTING message to the SBS Originating Node on the SBS signaling call.

Signaling for the SBS signaling call is the same as existing H.323 trunks using QSIG signaling with two exceptions. First, the SETUP and CALL PROCEEDING messages will contain Null Caps. Second, at least two INFO messages will be sent from the SBS Terminating Node to the SBS Originating Node. The INFO messages indicate the number to route the SBS bearer call to, and then the unique ID to signal on the SBS bearer call. These INFO messages are sent after the CALL PROCEEDING, and before ALERTING. They are encoded in a standard fashion, containing a Called Party Number - Information Element (IE).

Typical Call Connections

Four typical call connections are presented here.

- Point to Point call represents an SBS call between two Communication Manager systems. See Figure 374: Point to Point SBS Call Connections on page 1456.
- Tandem SBS trunk call represents an SBS call between two Communication Manager systems (A to C) with an intervening Communication Manager system in between. The SBS signaling link tandems through the intervening (B) node. The SBS bearer call is direct from node A to node C. See Figure 375: Tandem SBS Call Connections on page 1456.
- An SBS trunk interworked to a non-SBS trunk represents a call between two Communication Manager systems (A to C) with SBS functionality available only between nodes A and B. This call is interworked from SBS to a non-SBS QSIG trunk group at node B. See Figure 376: SBS to non-SBS QSIG Call Connections on page 1457.
- A non-SBS trunk interworked to an SBS trunk represents a call between two Communication Manager systems (A to C) with SBS functionality only available between nodes B and C. This call is interworked from non-SBS QSIG trunk group to SBS at node B. See Figure 377: PRI Non-SBS to SBS Call Connections on page 1458.

Figure 374: Point to Point SBS Call Connections

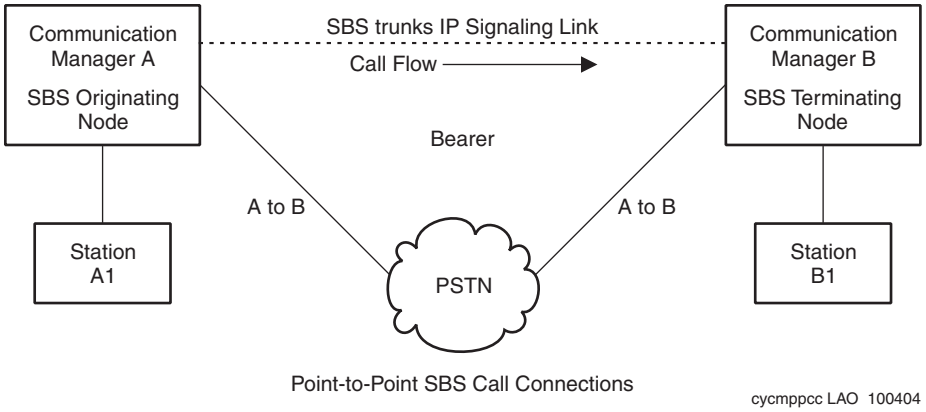


Figure 375: Tandem SBS Call Connections

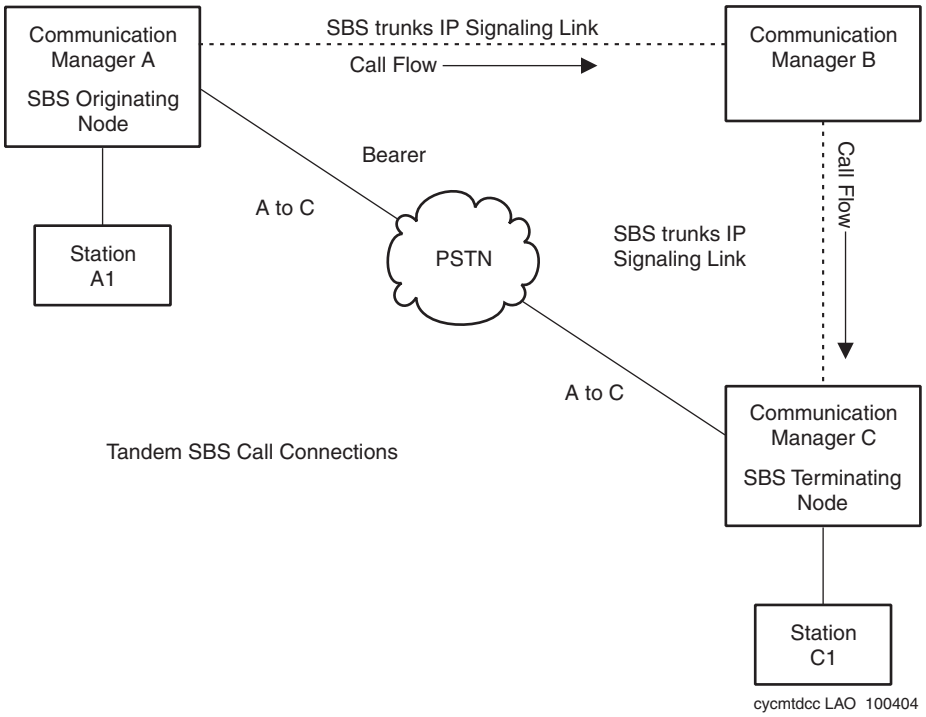


Figure 376: SBS to non-SBS QSIG Call Connections

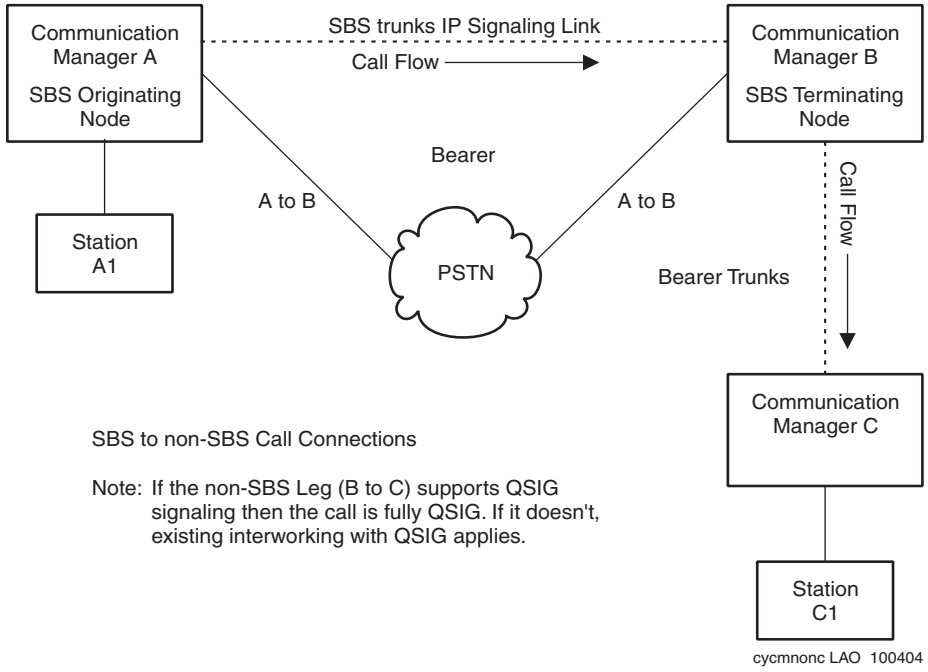
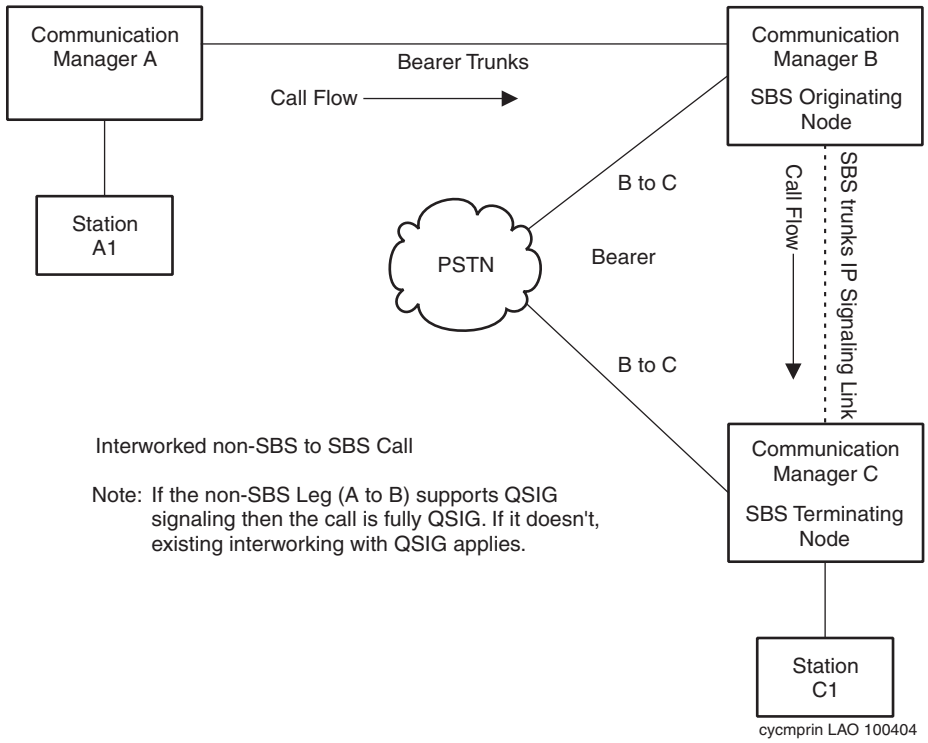


Figure 377: PRI Non-SBS to SBS Call Connections



Typical Call Setup

The following is a step-by-step description of a typical call.

1. An originating node user goes off hook and dials a terminating node user. The user can dial whatever number of digits are required to reach the terminating user. The originating call may be routed using Uniform Dial Plan (UDP), Automatic Route Selection (ARS), Automatic Alternate Routing (AAR), or a combination of these steering mechanisms.

   Note:
   The call might first route over a non-SBS trunk to an SBS Interworking Node that then routes the call to an SBS trunk. In this case, the SBS Interworking Node, not the originating Node, serves as the SBS Originating Node for this call.

2. Whichever routing mechanism is invoked (UDP/ARS/AAR), the call eventually routes to an H.323 IP trunk group. The call is translated to use QSIG signaling and specified in administration as an SBS trunk group with an SBS signaling group. The QSIG and SBS signaling group identification is the signaling portion of the call. This signaling portion is active for the duration of the call. A translation field identifies the SBS trunk group as reserved for SBS use. The signaling group associated with the SBS trunk group also has specific SBS translation. Apart from these fields, the SBS trunk group and signaling group are translated as a standard IP trunk group with standard QSIG signaling.
3. The SBS Terminating Node receives the signaling call. The SBS Terminating Node knows the call is an SBS call because it arrives on an SBS trunk group. The SBS Terminating Node determines that the called party in the signaling call SETUP message routes to a local extension or a non-SBS trunk. However, the Terminating Node temporarily refrains from terminating the call. Instead, the SBS Terminating Node allocates an SBS Extension to use for the duration of call setup. SBS Extension is a new type of Administered Without Hardware (AWOH) extension that is administered at all nodes that terminate SBS calls.
4. The SBS Terminating Node checks the *isdn public/unknown numbering* table. Upon finding a match for the SBS Extension, the SBS Terminating Node maps the number to a national (public network) Complete Number, including area/city code if applicable. The SBS Terminating Node also determines the local Country Code from the Feature Related System Parameters screen and adds it to the number created from the **ISDN Numbering-Public/Unknown** *screen.* The resulting number includes Country Code/Area/City/SBS Extension.
5. The SBS Terminating Node then sends the Complete Number to the SBS Originating Node on the SBS Signaling call. This is the number that the SBS Originating Node uses to route the bearer call.
6. The SBS Originating Node receives the Complete Number. The SBS Originating Node compares the Country Code received to the Country Code that the SBS Originating Node is located in. If the Country Codes are the same, the SBS Originating Node deletes the Country Code from the received number. If the Country Codes are different, the SBS Originating Node adds its SBS International Access Code (from *the* Feature Related System Parameters screen) to the received number.
7. The SBS Originating Node uses ARS to route on the Complete Number, which may have been modified. The Origination Node then launches the SBS bearer call to the routed-to bearer trunk.
8. The SBS Originating Node associates the signaling and bearer calls internally.
9. The bearer call arrives at the SBS Terminating Node. The SBS Terminating Node determines that the call is for an SBS Extension and *immediately answers* the call.

10. The SBS Terminating Node then sends a message to the SBS Originating Node on the signaling call that contains a unique three digit ID. This ID is created by the SBS Terminating Node from the internal call identification. This unique ID is reserved for the duration of the call. The SBS Terminating Node uses this unique ID to determine which bearer call is associated with the SBS signaling call in the event of multiple simultaneous calls to the SBS extension at the SBS Terminating Node. Examples of multiple simultaneous calls to the SBS extension include misdirected PSTN calls, telemarketing calls, and so on
11. The SBS Originating Node then sends the unique ID through DTMF tones, on the bearer call, towards the SBS Terminating Node. The originating user does not hear the DTMF tones.
12. After receiving the unique ID, the SBS Terminating Node associates the proper bearer and signaling calls. The SBS Terminating Node completes the call to the original destination (local extension or non-SBS trunk).
13. The SBS Terminating Node releases the SBS Extension.
14. When the called party is ringing, the SBS Terminating Node sends an ALERTING message to the SBS Originating node on the SBS signaling call.
15. When the called party answers, the SBS Terminating Node sends a CONNECT message to the SBS Originating Node on the SBS signaling call.
16. When either the calling party at the originating node or the called party at the terminating node hang up, both the bearer and signaling call are idled.

Tandem SBS calls

Separation of bearer and signaling calls can be tandemed through Communication Manager systems. Either the SBS signaling call or the SBS bearer call can tandem.

When SBS calls tandem through a intervening system you cannot use status commands to determine what bearer call is associated with what signaling call. SBS signaling and bearer calls cannot be associated at tandem nodes.

Tandem SBS bearer call

While the SBS feature is intended to use the Public Switched Telephone Network (PSTN) for transport of the bearer call there is nothing to preclude the use of private point to point (Tie Trunk) facilities to establish the bearer call. The SBS bearer call may also use traditional H.323 IP trunks. When IP trunks are used for transport of the SBS bearer call, appropriate user expectations as to voice quality need to be set.

When private point to point facilities are used to transport the SBS bearer call, all feature transparency and name information is obtained from the associated SBS signaling call. This is true even if the bearer call is transported on facilities capable of providing feature transparency (PRI).

You must administer appropriate steering of extension numbers at intervening nodes to ensure proper routing of tandem bearer calls.

Tandem SBS signaling call

SBS signaling calls can tandem through intervening nodes but those nodes must be Communication Manager systems, equipped with release 1.3 or later. Unlike SBS bearer calls, tandem SBS signaling calls must be carried on SBS trunks for all segments of the call. For more information, see Tandem SBS Call Connections on page 1456.

You must administer appropriate steering of extension numbers at intervening nodes to insure proper routing of tandem bearer calls.

Interworked SBS calls

The SBS Interworking Node is the switch where either:

- an incoming SBS trunk call is routed to a non-SBS trunk (Figure 376: SBS to non-SBS QSIG Call Connections on page 1457),

  or

- an incoming non-SBS trunk call is routed to an SBS trunk (Figure 377: PRI Non-SBS to SBS Call Connections on page 1458).

The SBS Interworking Node is either the SBS Originating Node or the SBS Terminating Node.

- The SBS Interworking Node is the SBS Originating Node when a non-SBS trunk is interworked to an SBS trunk.
- The SBS Interworking Node will be the SBS Terminating Node when an SBS trunk is interworked to a non-SBS trunk.

Feature interworking on SBS calls is supported only to the degree that Communication Manager currently interworks public/private protocols to/from QSIG signaling.

Administering Separation of Bearer and Signaling

The following steps are part of the administration process for the Separation of Bearer and Signaling feature:

- Administering Local Country Code and International Access Code
- Administering SBS trunks and trunk groups
- Administering routing for SBS

- Administering SBS extensions
- Verifying system capacities

This section describes:

- Any prerequisites for administering the Separation of Bearer and Signaling feature
- The screens that you use to administer the Separation of Bearer and Signaling feature
- Complete administration procedures for the Separation of Bearer and Signaling feature

Prerequisites for administering Separation of Bearer and Signaling

You must complete the following actions before you can administer the Separation of Bearer and Signaling feature:

Verify that the system is running Communication Manager Release 1.3 or later. Release 1.3 or later is required on all nodes that participate in SBS calls. The nodes can be originating, tandem, and terminating.

Verify features on the **Optional Features screen** by the following procedure:

1. In a SAT session, type **`display system-parameters customer-options`** and press **Enter**.

   The system displays the **Optional Features screen**.
2. Scroll through the **Optional Features** screens to find the **Maximum Administered IP Trunks** field. This field must be greater than 1 and include enough trunks for SBS trunk group use.
3. Scroll through the screens to find the **IP Trunks?** field.
4. Set the **IP Trunks?** field to **y**.
5. Scroll through the screens to find the **QSIG Optional Features screen**.
6. Set the **Basic Call Setup?** field to **y**
7. Set the **Basic Supplementary Services?** field to **y**.
8. Press **Enter** to save your changes.

Note:
Other QSIG options might need to be activated, depending on your feature functionality requirements.

Verify port and SBS trunk capacities.

- SBS Extensions count against the pool of available ports in the same manner as Administered Without Hardware (AWOH) extensions.

- Consider whether SBS trunks that you add to an existing system increase traffic on the PSTN trunks. SBS trunk group members count against the pool of available IP trunks. SBS bearer calls usually use the same trunks as normal local and/or toll PSTN calls. For implementation of the SBS feature, you might have to increase the quantity of trunks to the PSTN.

Screens for administering Separation of Bearer and Signaling

Screen name	Purpose	Fields
Dial Plan Analysis	Define the dial plan for SBS calls on the local system.	**All**
Feature-Related System Parameters	Specify a valid country code for the SBS signaling trunk groups.	**Local Country Code**
	Specify the access code that the private switched telephone network (PSTN) requires to route calls out of the country.	**International Access Code**
ISDN Numbering - Public/Unknown	Specify information for call processing to create a "complete number" for the SBS extension when this system is the SBS Terminating Node in an SBS call.	**All**
Route Pattern	Set the **TSC** field to **y** on the route pattern that SBS signaling calls are directed to.	**TSC**
Signaling Group	Enable SBS for a signaling group.	**Group Type** **Max number of NCA TSC** **SBS** **Trunk Group for NCA TSC** **Trunk Group for Channel Selection** **Supplementary Service Protocol** **Near-end /Far-end Listen Ports**

Screen name	Purpose	Fields
Station	Specify the SBS extension.	**SBS Extension** **Type** **Port**
Stations	List assigned SBS extensions	Ext Type
System Capacity	Verify trunk and station maximums for the system.	Trunk Ports IP Trunks Station and Trunk Ports Extensions Stations Records Stations without Ports Station and Trunk Ports
Trunk Group	Enable SBS for a trunk group; add members to the SBS trunk group.	Group Type Carrier Medium Carrier Medium Supplementary Service Protocol **SBS** **NCA-TSC Trunk Member** **Send Name** Send Calling Number Send Connected Number (add members) All

Administering Local Country Code and International Access Code

Administer the Local Country Code and International Access Code at both the SBS Originating and SBS Terminating Nodes using the Feature-Related System Parameters screen.

To administer Local Country Code and International Access Code:

1. Type **`change system-parameters features`**. Press **Enter**.

   The system displays the Feature-Related System Parameters screen.

2. Click **Next** until you see the **International Calling Routing Parameters** fields (Figure 378: Feature-Related System Parameters screen on page 1465).

Figure 378: Feature-Related System Parameters screen

```
change system-parameters features                              Page   x of  x
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS

   CPN/ANI/ICLID Replacement for Restricted Calls:
  CPN/ANI/ICLID Replacement for Unavailable Calls:

INTERNATIONAL CALLING ROUTING PARAMETERS

               Local Country Code: 1
        International Access Code: 011
```

3. In the **Local Country Code** field, enter the three-digit country code for this node. In the United States this field is populated with **1**.
4. In the **International Access Code** field, enter the access code required by the Public Switched Telephone Network (PSTN) to route calls out of the country.
5. Press **Enter** to save your changes.

Administering SBS trunks and trunk groups

You must administer the H.323 IP trunks, equipped with QSIG signaling, between nodes. These trunks are the signaling portion of SBS calls and are specifically translated as SBS trunks in their trunk group and signaling group administration forms. The number of SBS trunk group members must be engineered for the expected SBS traffic volume.

You must administer the trunks to the local PSTN from each node. These trunks do not have any unique SBS related administration.

Note:

While these trunks are intended to be circuit switched PSTN trunks, there is nothing in the SBS feature operation that precludes the use of other trunks. For example, a second choice for bearer calls may be IP trunks. Note that voice quality might be affected if you use trunks other than PSTN quality circuit switched trunks.

SBS trunk groups are added in three steps. First, create the trunk group and populate the first two administration screens. Second, create the SBS signaling group. Third, add the trunk members to the SBS trunk group. All of these tasks are performed in a SAT session.

Creating the SBS trunk group

To create the SBS trunk group:

1. Type **add trunk-group *n*** where ***n*** is the number of the trunk group. Press **Enter**.

   The system displays the **Trunk Group** screen.
2. Click **Next** until you see the **Trunk Parameters** section.
3. Set the **Group Type** field to **ISDN**.
4. Set the **Carrier Medium** field to **IP**.
5. Set the **Dial Access?** field to **n**.
6. The **Supplementary Service Protocol** is always set to **b**.
7. Click **Next** until you see the **Trunk Features** section.
8. Set the **SBS** field to **y** (default is **n**).

   Note:
   The **SBS** field can only be set to **y** if all the following are true:
   - **Carrier Medium** field is set to **IP**,
   - **Dial Access** field is set **n**,
   - **Supplementary Services Protocol** field is set to **b, and**
   - **Local Country Code** and **International Access Code** fields are administered on the Features Related System Parameters screen.

     The **Send Name, Send Calling Number,** and **Send Connected Number** fields must be set to **y** for the SBS trunk group to enable these capabilities on SBS calls.
9. Set the **NCA-TSC Trunk Member** field to one member of the SBS trunk group.
10. Set the **Send Name** field to **y**.
11. Set the **Send Calling Number** to **y**.
12. Set the **Send Connected Number** to **y**.
13. Press **Enter** to save your changes.

Creating a signaling group

To create a signaling group:

1. Type **add signaling-group *n*** where ***n*** is the signaling group number. Press **Enter**.

   The system displays the Signaling Group screen (Figure 379: Signaling Group screen on page 1467).

Figure 379: Signaling Group screen

```
add signaling-group 52
                                SIGNALING GROUP

 Group Number: 52                 Group Type: h.323
                            Remote Office? n          Max number of NCA TSC: 5
                                      SBS? y           Max number of CA TSC: 0
                                                    Trunk Group for NCA TSC: 52
       Trunk Group for Channel Selection: 52
         TSC Supplementary Service Protocol: b


        Near-end Node Name: hc_clan3          Far-end Node Name: fido_clan1
     Near-end Listen Port: 6067             Far-end Listen Port: 6067
                                         Far-end Network Region:
              LRQ Required? n             Calls Share IP Signaling Connection? y
              RRQ Required? n
                                             Bypass If IP Threshold Exceeded? n

            DTMF over IP: out-of-band         Direct IP-IP Audio Connections? y
                                                    IP Audio Hairpinning? y
                                              Interworking Message: PROGress


Command:
```

2. Make sure the **Group Type** field is set to **H.323**
3. Set the **Max number of NCA TSC** field to a number greater than zero.

   Non Call Associated Temporary Signaling Connections (NCA TSC) are used to establish connections and pass messages for features like Message Waiting Indication (MWI) activation and deactivation. QSIG protocol establishes and releases the NCA TSC for each MWI session.

   When a TSC is established between two Communication Manager systems it sends the message it was established for. The TSC then stays up until there have been a few minutes of inactivity. Depending on traffic, this TSC can be used for multiple messages.

   A TSC that is established between a Communication Manager system and a messaging system will be taken down after the initial message is sent.
4. Set the **SBS** field to **y**.

   This field only appears when the **Group Type** field is set to **H.323**.
5. Set the **Trunk Group for NCA TSC** field to same number as the SBS trunk group.
6. Set the **Trunk Group for Channel Selection** field to the same number as the SBS trunk group.

7. Always set the **TSC Supplementary Service Protocol** field to **b**.
8. Set the **Near-end /Far-end Listen Ports** fields to equal the far-end value on the distant switch. The near-end value on the distant switch must match the far-end value on this near-end switch.

   Note:
   A signaling group that is used for SBS trunks cannot be used for non-SBS trunk groups. The **Near** and **Far-end Node Names** are defined using the change node-names ip administration form.
9. Press **Enter** to save your changes.

Adding trunk group members to SBS trunk group

To add trunk group members to the SBS signaling trunk group:

1. Type **`change trunk-group n`** where ***n*** is the trunk group number. Press **Enter**.

   The system displays the **Trunk Group** screen.
2. Click **Next** until you see the **Group Member Assignments** section.
3. Add trunk group members to the numbered **Group Member Assignments**. This signaling group is used only for SBS signaling.

   Note:
   A signaling group cannot be used for both SBS and non-SBS trunk groups. A SBS trunk group cannot be associated with a signaling group that is connected to a Remote Office.
4. Press **Enter** to save your changes.

   Note:
   Like standard IP trunks the initial input for the *Port* field should be *IP.* Once the form has been successfully submitted the actual port information will be shown.

Administering routing for SBS

Routing at each node occurs through AAR, ARS, and UDP. Calls to nodes using SBS trunking are initially steered to the SBS trunk group for the target (terminating) node. When the SBS Terminating Node returns a complete number to the SBS Originating Node the bearer call is established using ARS and the call is transported over standard bearer facilities (not the SBS trunk group). The bearer always originates through ARS but the complete number may be modified and passed to other routing capabilities (AAR or UDP) and sent through private facilities.

To create a route pattern:

1. In a SAT session, type **`change route-pattern n`** where ***n*** is the number of the route pattern. Press **Enter**.

   The system displays the **Route pattern screen** (Figure 380: Route pattern screen on page 1469).

2. *Set the **TSC** field to* **y** for the route pattern to which the SBS signaling calls are directed.

   If the **TSC** field is set to **n**, Message Waiting Indication (MWI) messages will fail and the voice messaging system will not able to light or retire message waiting lamps on individual stations.

Figure 380: Route pattern screen

```
display route-pattern 52                                        Page   1 of   3
                           Pattern Number: 52

    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                              Dgts                                  Intw
 1: 52   0                                                           n    user
 2:                                                                  n    user
 3:                                                                  n    user
 4:                                                                  n    user
 5:                                                                  n    user
 6:                                                                  n    user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature BAND  No. Numbering LAR
    0 1 2 3 4 W     Request                                   Dgts Format
                                                           Subaddress
 1: y y y y y n   y  none      rest                                      none
 2: y y y y y n   n            rest                                      none
 3: y y y y y n   n            rest                                      none
 4: y y y y y n   n            rest                                      none
 5: y y y y y n   n            rest                                      none
 6: y y y y y n   n            rest                                      none
```

3. Press **Enter** to save your changes.

Administering SBS extensions

The SBS Extension is an extension type that is translated at each SBS Terminating Node. Each SBS Extension must be Direct Inward Dial/Direct Dial In (DID/DDI) accessible at the SBS Terminating Node it is administered on. However, if the bearer call arrives at the SBS Terminating Node through other than PSTN DID/DDI trunks, for example private Tie Trunks, the SBS feature does not require that the SBS Terminating Node have physical DID/DDI trunks. You must allocate sufficient SBS Extensions for the expected SBS traffic volume.

Note:
SBS Extensions are only in use for the duration of call setup, not for the entire duration of the SBS call.

The SBS Extension type emulates a station with three call appearances. You cannot assign a coverage path or station hunting for an SBS Extension.

To add an SBS station extension:

1. In a SAT session, type **add station *nnnnnnn*** where ***nnnnnnn*** is a valid extension that is DID/DDI accessible. Press **Enter**.

   The system displays the **Station screen** (Figure 381: Station screen on page 1470).

Figure 381: Station screen

```
add station 694102
                                    STATION

Extension: 694102                                              BCC: 0
     Type: SBS                                                  TN: 1
     Port: X                                                   COR: 1
     Name: SBS TEST EXTENSION                                  COS: 1


Command:
```

2. Set the **Type** field to **sbs**.

   The **Port** field sets automatically to **X** when **Type** is set to **SBS**.
3. Type the name of the extension in the free form **Name** field.
4. Type the tenant number in the **TN** field. SBS Extensions may be partitioned through the Tenant Partitioning feature.
5. Type in the Class of Restriction number in the **COR** field.
6. Type in the Class of Service number in the **COS** field.
7. Press **Enter** to save your changes.

Note:

SBS extensions are not real extensions. SBS extensions should not be entered in fields, not other administration forms, where Communication Manager administration expects a real extension. Calls to the SBS extension will fail if you enter SBS extensions on administration forms. Also, such non-SBS usage could disrupt completion of incoming SBS calls (that is, if an SBS Extension was not available when needed due to misuse). Examples of fields where an SBS Extension should **not** be administered include:

- Hunt group member
- Point in a coverage path
- Cover Answer Group member
- Termination Extension Group member
- Hunt-to extension in Station Hunting
- Extension tracked by a Facility Busy Indicator button

This list is not exhaustive.

Administering SBS extensions

You must define the dial plan on the local system and map the SBS extensions to complete numbers.

Defining the dial plan

To define the dial plan on the local system:

1. Type **`change dialplan analysis`** and press **Enter**.

   The system displays the **Dial Plan Analysis Table** screen (Dial Plan Analysis Table screen on page 1472).

2. Type in the appropriate extensions lengths according to your dial plan.

In the example below the first digit of 2, 3, 6 and 7 are defined as extensions of various lengths (1 digit through 7 digits). SBS Extensions for this system are 6-digit extension numbers. See Station screen on page 1470.

Figure 382: Dial Plan Analysis Table screen

```
change dialplan analysis                                    Page   1 of   3
                            DIAL PLAN ANALYSIS TABLE
                                                          Percent Full:    6

      Dialed  Total  Call      Dialed  Total  Call      Dialed  Total  Call
      String  Length Type      String  Length Type      String  Length Type
        00      2    attd        6       6    ext         #       2    fac
        01      4    fac         7       5    ext
        1       3    dac         8       1    fac
        2       1    ext         9       4    fac
        2       2    ext         9       5    ext
        2       3    ext         *0      2    fac
        2       4    ext         *1      2    fac
        2       5    ext         *2      2    fac
        2       6    ext         *3      2    fac
        2       7    ext         *4
2    fac
        32      7    ext         *5      2    fac
        37      7    ext         *6      2    fac
        39      7    ext         *7      2    fac
        4       1    fac         *8      2    fac
        6       5    ext         *9      2    fac
```

3. Press **Enter** to save your changes.

Mapping SBS Extensions to complete numbers

You must map SBS Extensions to a complete number, that is, area/city/SBS extension, at each SBS Terminating Node. This complete number is then sent to the SBS Originating Node where ARS establishes the bearer call.

Use the **ISDN Numbering - Public/Unknown Format** screen to create a "complete number" for the SBS extension when this system is the SBS Terminating Node in an SBS call.

To administer SBS extensions:

1. Type **`change isdn public-unknown-numbering`** and press **Enter.**

   The system displays the **ISDN Numbering - Public/Unknown Format** screen (Figure 383: ISDN public-unknown format on page 1473).

Figure 383: ISDN public-unknown format

```
display isdn public-unknown-numbering                          Page   1 of   8

                     ISDN NUMBERING - PUBLIC/UNKNOWN FORMAT
                                    Total                                  Total
Ext  Ext     Trk       CPN           CPN Ext Ext     Trk       CPN           CPN
Len  Code    Grp(s)    Prefix        Len Len Code    Grp(s)    Prefix        Len

 5   9                 30337         10
 6   6                 3033          10
 6   69                3034          10
```

2. Type in the **Ext Len** (extension length) of the extensions in your dial plan.
3. Type in the **Ext Code** (extension code) for each extension.
4. Type in the **CPN Prefix** for each extension.
5. Press **Enter** to save your changes.

When a SBS call is received, and routes to a local endpoint or non-SBS trunk, an SBS extension is allocated for use during call setup. For example, if the extension was 694102, call processing would index the *public-unknown-numbering* table for the best match to the extension using the *Ext Code* column.

For the translations shown in Figure 383: ISDN public-unknown format on page 1473, the best match is the 6 digit entry for Extension Code 69. Call processing takes the associated CPN prefix entry (3034) and pre-pends it to the extension to make a Complete Number, 3034694102. Call processing then pre-pends the local country code found on Figure 378: Feature-Related System Parameters screen on page 1465 to the number, 13034694102.

This complete number is sent to the SBS Originating Node on the SBS trunk that is originating the call.

Note:

The Complete Number that is sent to the SBS Originating Node must be DID/DDI accessible at the SBS Terminating Node. The SBS Originating Node uses its international access code to dial the Complete Number if the local country code provided differs from the local country code of the SBS Originating Node. See Figure 378: Feature-Related System Parameters screen on page 1465.

Verifying system capacities

SBS Extensions and trunks count against the pool of available ports and trunks. You must consider whether SBS trunks that you add to an existing system increase traffic on the PSTN trunks. SBS trunk group members count against the pool of available IP trunks. SBS bearer calls usually use the same trunks as normal local and/or toll PSTN calls. Implementation of the SBS feature might require that you increase the quantity of trunks to the PSTN.

To verify the used, available and system limits for SBS trunks:

1. In a SAT session, type **`display capacities`** and press **Enter**.

   The system displays the **System Capacity** screen (Figure 384: System Capacity screen: Voice Terminals on page 1474).

Figure 384: System Capacity screen: Voice Terminals

```
display capacity                                          Page   7 of  10
                                SYSTEM CAPACITY

                                                                    System
                                                  Used Available    Limit
                                                 ----------------------

                  VOICE TERMINALS
                     Station Button Memory (units):    2 %    98 %  17496000
                                    Station Records:   1488   34487*   36000
                  Stations (includes BRI stations):     774     -        -
                                 Stations With Port:    734
                              Stations Without Port:     40
                                    Other Stations:     714     -        -
                                         TTI Ports:       0     -        -
                                Auto Moves Stations:      0     5000     5000
                           Administered IP SoftPhones:    48     2752     2800
                      ISDN BRI Endpoint And Trunk Ports:    53     6947     7000
                    IP Trunks (included in 'Trunk ports'):    98      902     1000
         Remote Office Trunks (included in 'Trunk ports'):     0     1000     1000
                   SBS Trunks (included in 'Trunk ports'):     5      995     1000
              '*'  Availability reduced by the number of administered VDNs
```

2. Scroll through the **System Capacity** screens until you see the **Voice Terminals** fields.
3. Verify the **Used**, **Available**, and **System Limit** capacities for the **SBS Trunks** field.

   SBS Trunks count against the system maximums for the following trunk ports fields:

   - **Maximum ports** field (**Optional Features** screen)
   - **Trunk Ports** field (**System Capacity** screen)

- **IP Trunks** field (**System Capacity** screen)
- **Station and Trunk Ports** field (**System Capacity** screen)

To verify the used, available and system limits for SBS stations:

1. Scroll through the **System Capacity** screens until you see the **Total Subscribed Ports** fields (Figure 385: System Capacity screen: Total Subscribed Ports on page 1475).

Figure 385: System Capacity screen: Total Subscribed Ports

```
display capacity                                          Page   8 of  10
                            SYSTEM CAPACITY

                 TOTAL SUBSCRIBED PORTS
                                                                  System
                                                Used Available    Limit
                                               ----------------------
                          Station and Trunk Ports:   1134   18866    20000
                                      SBS Stations:      9     491      500
                                 Radio Controllers:      0       0        0
                                Wireless Terminals:      0       0        0
                                  XMOBILE Stations:      0       0        0
                                           EC500:        0
                                            DECT:        0
                                             PHS:        0
       SYSTEM-WIDE REGISTRATION COUNTS
                                            Currently                System
                                            Registered  Available    Limit
                                            ------------------------------
                                IP Stations:       489       4511     5000
                        IP Attendant Consoles:       0          1        1
                       Remote Office Stations:       0       1000     1000
```

2. Verify the **Used**, **Available**, and **System Limit** capacities for the **SBS Stations** field.

   SBS Stations count against the system maximums for the following trunk ports and stations fields:

   - **Maximum Ports** field (**Optional Features** screen)
   - **Extensions** field (**System Capacity** screen)
   - **Stations Records** field (**System Capacity** screen)
   - **Stations without ports** field (**System Capacity** screen)
   - **Station and Trunk Ports** field (**System Capacity** screen)
3. Press **Enter** and logoff the SAT session.

Considerations for Separation of Bearer and Signaling

This section provides information about how the Separation of Bearer and Signaling (SBS) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Separation of Bearer and Signaling under all conditions. The following considerations apply to Separation of Bearer and Signaling:

- Call Detail Recording (CDR)

  CDR functionality records the calling and the called number information, and the start and end times of each measured call. You administer this CDR functionality on a trunk-group basis within Communication Manager. At the end of a call, the information is made available to an adjunct server for functions such as costing, reports, and traffic analysis.

  In the case of an SBS call, the data that is gathered and made available to the adjunct server does not change. However, since each trunk group that is involved in an SBS call can be administered to generate CDR reports, the system can generate two CDR records for each SBS call. The system generates one record for the SBS signaling call, and one record for the SBS bearer call. You cannot link the separate SBS signaling and bearer CDR records.

  Since the signaling and bearer CDR records cannot be linked, you might prefer to measure only the bearer calls. The service provider is more likely to bill for the bearer calls. However, note that the SBS bearer call is always answered by the SBS extension, even though the actual called party does not answer the SBS call. The parties on the SBS bearer call are not the actual originating and terminating parties. The parties on the SBS bearer calls are "dummy" users, who are internal to Communication Manager for the sole purpose of originating and terminating the bearer call.

- Call Management System (CMS) and Basic Call Management System (BCMS)

  You can administer the following entities to be measured for CMS or BCMS:

  - A trunk group
  - A Vector Directory Number (VDN)

– A hunt group

An SBS call can generate two separate CMS or BCMS records. The system can generate one record for the SBS signaling call, and one record for the SBS bearer call.

CMS and BCMS measure the SBS bearer call only if the bearer trunk group is administered to be measured. CMS and BCMS measure only the trunk bearer seize events and idle events.

The SBS signaling call is measured if the SBS signaling group is administered to be measured, or an endpoint on the SBS call is a measured object. A measured object can be an agent in a hunt group that is administered to be measured. The measured events on the SBS signaling call include not only the trunk signaling seize events and idled events, but also any endpoint events, such as agent hold.

The SBS signaling and bearer calls generate separate CMS or BCMS records with different Universal Call IDs (UCIDs). You cannot link these separate records.

- Calling Party—Delay in Call Setup Time

  When originating an SBS call, the calling party might perceive a delay in call setup time compared to non-separated calls. This delay is caused by several factors. First, the SBS bearer call cannot be initiated until after the SBS signaling call initiates and a number to route the SBS bearer call to is received from the SBS Terminating Node. Then, the establishment of this SBS bearer call may be noticeably delayed relative to a non-SBS call, depending upon the type of bearer trunk selected and its trunk signaling protocol. Finally, DTMF digits must be sent over the SBS bearer call, so that the SBS Terminating Node can identify the correct bearer call, which also adds delay.

  The exact amount of these delays depends upon several variables such as the amount of congestion in the IP network used for the SBS signaling call and the type of bearer trunk used for the SBS bearer call.

  Given a fairly un-congested data network, SBS calls add approximately 1.5 seconds to the call setup time as perceived by the originating user. The SBS delay of approximately does not affect the originating user in any profound way. This delay is relative to a non-separated call over the same type of trunk as used for the SBS bearer call.

  The time before the originator hears audible ringback may approach 10 seconds for a bearer trunk that is slow to outpulse digits (rotary). However, a non-separated call using the same bearer trunk would result in a delay of approximately 8.5 seconds before audible ringback is heard. Some bearer trunks can outpulse digits quickly. An example of message oriented signaling trunks is ISDN. For these types of bearers, the SBS induced delay is a majority of the overall delay until the originator hears audible ringback.

  The *called* party will perceive no delays relative to non-separated calls. All setup, validation, and association of SBS signaling and bearer calls occur before alerting of the called party.

- Feature Information Displays

  SBS call display feature information such as Name and Number, call transfer or forward indication and transfer-to or forward-to party information is the same as QSIG calls. SBS call displays are driven exclusively by translations and signaling on the SBS trunk, and not by translations/signaling on the associated bearer trunk.

Interactions for Separation of Bearer and Signaling

This section provides information about how the Separation of Bearer and Signaling (SBS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Separation of Bearer and Signaling in any feature configuration.

Overview of SBS interactions

SBS provides a separated trunk call. Many types of trunks can be used to carry the bearer portion of the separated call. Thus, SBS affects many Communication Manager features. Almost any feature that can interact with a trunk call can interact with SBS.

This section describes features that might interact with SBS calls. Other features might also interact with SBS in a minor way.

You must understand how SBS calls are configured internally to understand why certain features can work with SBS calls, and others cannot. This general understanding also helps you to accurately predict whether a feature that is not included in this section can successfully work with an SBS call.

Two important facts about the internal configuration of an SBS call are:

- SBS bearer and SBS signaling calls are tracked internally as separate calls for the life of the SBS call. Separate call records are created internally for each call to:
  - Allow the SBS bearer call to be carried over almost any type of trunk
  - Use the standard call establishment and tear-down code for that trunk type

  The system cannot use the standard code if the bearer trunk is somehow "buried" as a nonstandard party in a "merged" signaling and bearer call record.
- The endpoint users are parties on the SBS signaling call, and not on the SBS bearer call. In other words, the SBS signaling call controls the call. Endpoint user activity drives QSIG signaling only if a QSIG trunk is a party on the call. Therefore, the SBS signaling call must control the call. A QSIG trunk is guaranteed only if the endpoint user is associated with the SBS trunk. A QSIG trunk is not guaranteed if the endpoint user is associated with the bearer trunk.

Understanding potential interactions

Based on these two facts about the internal configuration of an SBS call, the following general observations about feature interactions with SBS calls can be made.

- Most features work with SBS

  A significant number of the features that can interact with an SBS call work as those features do with any other QSIG trunk call.

- Delay applies to all SBS calls

  For features that do work with SBS calls, the standard SBS delay applies. However, some of the following feature interaction descriptions do not specifically mention SBS delay.

- Call status

  Any query or report that is related to an endpoint user on an SBS call indicates the call ID of the SBS signaling call, and the trunk ID of the signaling trunk, but not the bearer trunk. For example, a **status station** command that is issued against a telephone on an SBS call shows the telephone that is connected to an SBS trunk.

- Feature signaling interworks to and from SBS signaling calls

  Any feature information that is interworked from a non-SBS leg of a call to an SBS leg of a call is transported on the SBS signaling call, and not on the SBS bearer call. Likewise, any feature information that is interworked from an SBS leg of a call to a non-SBS leg of a call is taken from the SBS signaling call, and not from the SBS bearer call.

- Two records per SBS call

  Any feature that reports or records status for a call can create two different reports or records for a single SBS call. The feature can create one report or record for the signaling trunk, and a second report or record for the bearer trunk. For example, with Call Detail Recording (CDR), the number of reports or records depends on whether both trunks groups are administered to produce call detail records.

- Bearer trunk signaling features

  Features that require signaling over a non-QSIG type of trunk do not work with SBS calls. The endpoint users are not parties on the SBS bearer call. Therefore, user activity cannot drive any feature signaling on the bearer call. Similarly, any feature signaling that is received on the bearer call cannot drive any notification or displays to the endpoint user. For example, public or private network-specific (non-QSIG) Malicious Call Trace (MCT) network notification and Advice of Charge (AOC) display functionality do not work with SBS calls.

- Bearer trunk user features

  Features that are related to the SBS bearer call and require activation or acknowledgement from an endpoint user do not work with SBS calls. Such features do not work with SBS calls because the endpoint user is not a party on the bearer call. For example, queuing of the SBS bearer call does not work because the real originating party is not on the bearer call.

- Early-answer features

  Features that require early answer do not work with SBS calls. Such features do not work with SBS calls because when the signaling call is answered, the bearer call is not started. When the bearer call is first answered, the call is for the SBS extension at the terminating node. For example, authorization code collection on incoming calls and direct calls to remote access does not work with SBS calls.

- Network features that send tones when the bearer call answers do not work

  Network features that send tones when the bearer call answers do not work with SBS. When the bearer call is answered, the call is for the SBS extension. The final telephone user is not on the call to hear the tones. For example, the user does not hear the dual-tone multifrequency (DTMF) notification when a network call is eligible to be transferred, such as with Take-back and Transfer.

General system features and SBS

- Media processor resources are not used by the SBS trunks. SBS trunks carry only SBS signaling calls. SBS bearer calls require media processor resources if IP trunks are used.

  Voice quality can degrade if you use IP trunks for bearer calls.

- Shuffling and hairpinning work with SBS bearer calls if you use IP trunks. The SBS bearer call originates with the same "shufflable endpoint" characteristics as the originator.
- The system obtains the contents of the Incoming Call Identification (ICI) display for an SBS call from the SBS signaling call, and not from the bearer call.
- The system uses the Class of Restriction (COR) of the SBS call originator to set up the SBS bearer call.
- The system routes the SBS signaling and bearer calls separately. Use caution when you administer Toll Restriction, Toll Analysis, and Toll/Code restriction so that you do not block calls that should be allowed.
- The Class of Service (COS) Trunk-to-Trunk Transfer permission affects the transfer of SBS trunk calls in the same way as for non-SBS trunk calls.
- SBS calls follow the Station Hunting of the originally called party.
- When Tenant Partitioning is active in an enterprise, existing Tenant Partitioning rules apply to endpoints, SBS extensions, SBS trunk groups, and the bearer trunk groups that are involved in any SBS call.

- SBS works with Dial Plan Expansion of 6-digit or 7-digit extensions.
- Standard Malicious Call Trace (MCT) on an incoming SBS call records the bearer trunk call.

Attendant interactions with SBS

Attendant features that do not work with SBS

- Attendant Control of Trunk Group Access does not work with an SBS Trunk Group.
- Centralized Attendant Service (CAS) does not work over SBS trunks, since CAS requires release link trunks (RLT). However, you can use CAS to direct an incoming SBS call to a centralized attendant over an RLT. Likewise, a centralized attendant can extend a call over an RLT, that the system then routes to an SBS trunk.

Attendant features that work with SBS

- Attendant Direct Extension Selection (DXS) can be used to originate an SBS call that uses Uniform Dial Plan (UDP).
- Attendant Intrusion can be used to intrude on an SBS call.
- Attendant Recall works with an SBS call
- Attendant Return Call and Serial Calling work with an incoming SBS call.
- Attendant transfer is applicable to an SBS call.
- An incoming SBS call can be parked, and is subject to Call Park Time-out to the Attendant.
- An SBS call can be a party in an attendant conference.
- An SBS call can be directed to an individual attendant access number.
- Inter-PBX attendant service works with SBS trunks.
- Incoming SBS calls follow attendant Night Service.
- Incoming SBS calls hear Recorded Announcements in the attendant queue.
- You can use Trunk Answer Any Station (TAAS) to answer an incoming SBS call.
- The Trunk Identification by Attendant feature identifies the SBS trunk group member.
- An SBS call can be held with Two-Party Hold on Console.
- Attendant Vectoring can receive and redirect attendant-directed calls over SBS trunks.

Adjunct Switch Applications Interface interactions with SBS

- When you use Call Classification after Answer, do not use SBS to route calls. Do not use SBS because the Call Classifier must be on the bearer trunk, and the SBS-invoked DTMF signaling that is sent on the bearer trunk causes interferences.
- Adjunct Switch Applications Interface (ASAI) Phantom call, such as DEFINITY Anywhere, can originate or receive an SBS call.
- ASAI Selective Listening works on an SBS trunk party on a call.
- ASAI Send DTMF works on a connected SBS call.
- ASAI Single Step Conference can add another station onto a call with an SBS call.
- ASAI Provided Dial-Ahead Digits work when the incoming call is an SBS call.
- Any ASAI user data, Universal Call ID, or both that are currently transported or interworked over QSIG trunks, are sent on the SBS signaling call.
- Any II Digits that are received in the SETUP message to the incoming SBS Signaling call are tandemed with the SBS signaling call when an SBS call is received and subsequently tandemed over an SBS trunk.
- The information that is provided in response to an ASAI Value Query indicates whether an SBS trunk or an associated bearer trunk is idle or busy. The response is based on the UID in the query message and whether the response was for the signaling or the bearer trunk.
- For ASAI Event Reports, Communication Manager reports the Call ID and the Trunk ID of the SBS trunk. ASAI provides the Trunk ID of the associated bearer trunk to the ASAI Event Reports and Adjunct Route message.

CM Messaging and Octel voice mail adjuncts interactions with SBS

- Centralized voice mail with Interswitch Mode Codes does not interwork with SBS trunks. For that application, the tie trunks between the servers that run Communication Manager cannot use the QSIG protocol. While those tie trunks might be used for SBS bearer calls, SBS is likely not implemented when this methodology is used.
- Leave Word Calling with Message Wait Indicator over QSIG (QSIG LWC MSI) uses SBS to support Digital Line Emulation integration for centralized voice mail.
- SBS supports centralized CM Messaging from a served user switch.
- Where an Octel Serenade is connected to Communication Manager with QSIG, the server that runs Communication Manager is the SBS terminating node. This SBS terminating node interworks to the Serenade, since the Serenade does not support SBS.

Call Center interactions with SBS

Automatic Call Distribution interactions with SBS

- Look Ahead Interflow (LAI) might not function correctly on an SBS call, because of the SBS call setup delay. If the SBS delays are a problem, you might use Non Call Associated (NCA) Temporary Signaling Connection (TSC) instead of LAI to poll by Best Service Routing (BSR).
- Normal SBS call setup delays affect calls if Outbound Calling is done from a Call Center, and the call uses SBS to call another Communication Manager system. Outbound Calling over SBS trunks must not use Call Classification. Outbound Calling will have interference from the DTMF signaling that is invoked by SBS and sent to identify the correct bearer call at the terminating end.
- Dialed Number Information Service (DNIS) and Original Dial Number Delivery service from a service provider can deliver an SBS bearer call to an SBS extension in an SBS terminating node.
- When an incoming Automatic Call Distribution (ACD) call arrives by way of an SBS trunk, transfers by an agent to another agent or to an application work properly.
- An incoming SBS call can hear any announcements that are associated with the Call Center.
- The Agent Assist functionality works when the incoming call arrives over SBS.
- Displays at the agent terminals function correctly when the incoming call arrives over SBS. This includes Vector Collected digits.
- Multiple Call Handling works when arriving calls are incoming SBS calls.
- An incoming SBS call that receives Redirect on No Answer (RONA) works correctly.
- SBS calls that receive intraflow, interflow, or hunt group night service treatment are routed in the same way as a non-SBS call.
- Any ISDN call data, R2MFC call data, or both ISDN and R2MFC data that is currently interworked to or from a QSIG trunk is sent on (retrieved from) the SBS signaling call at the SBS interworking node. Such call data includes calling party number, II Digits, CINFO digits, and so on.
- Call Center data that is currently transported on QSIG trunks is sent on the SBS signaling call.
- When an ACD call is transferred to an agent through an SBS trunk connection on another system that runs Communication Manager, all associated call information that is currently transported on a QSIG trunk is sent on the SBS signaling call.
- All types of Service Observing functions work on SBS calls in the same way as for non-SBS calls.

Best Service Routing interactions with SBS

- Polling by Best Service Routing (BSR) can use SBS signaling facilities when the NCA-TSC version of BSR Polling is used, and adequate resources are available. The non-NCA-TSC version of BSR Polling might not work because of the SBS call setup delays.
- BSR interflow over SBS trunks, including incoming call data forwarding and Enhanced Information Forwarding, are supported.

Vectors interactions with SBS

- Routing on Automatic Number Identification (ANI) by a vector can use SBS to route an outgoing call. For an incoming SBS call, the Routing on ANI functionality uses the ANI from the SBS signaling call.
- Correct routing over SBS trunks works when a vector step exists for routing on ANI or II digits, or a route-to number step, and interflow is invoked.
- Post-Connect in-band DTMF signaling for Call Prompting collect steps and Auto Attendant functionality both work with SBS.
- When CINFO Digit Routing occurs, and the call is routed over an SBS trunk, the information is tandemed with the call.
- Vector Routing Tables can use SBS trunks to route calls.
- Incoming SBS calls still provide VDN of Origin announcements (VOA) and displays to the agent who answers the call.
- VDN Return Destination works with SBS calls.

Networking-related interactions with SBS

Networking features or capabilities that do not work with SBS

- Authorization codes cannot be collected on an incoming SBS signaling call or on an SBS bearer call. Such codes might be required to administer of the incoming trunk group or because of insufficient Facilities Restriction Level (FRL) on a tandem call. Authorization codes cannot be collected on incoming SBS signaling calls for two reasons:
    - The SBS bearer call is not established at the time that the system usually prompts for and signals an authorization code.
    - The originating endpoint user is not a party on the SBS bearer call.

- When the bearer call is transported through Message Oriented Signaling trunks ISDN, information in the SBS bearer call D-channel is not displayed to the end users. The information is not displayed because the signaling in the SBS signaling call overwrites the information.
- User information in the SBS bearer leg of the call is ignored.
- Australian Malicious Call Trace (MCT) cannot be invoked on an SBS call because:
  - End-user activity drives feature signaling only on the SBS signaling call, and not on the SBS bearer call
  - An SBS trunk does not support the Australia public network protocol

  The normal MCT feature within Communication Manager records the call as usual.
- ETSI MCT cannot be invoked on an SBS call because:
  - End-user activity drives feature signaling only on the SBS signaling call, and not on the SBS bearer call
  - An SBS trunk does not support ETSI protocol

  The normal MCT feature within Communication Manager records the call as usual.
- Calling Line ID Prefix information is ignored when the information is transported in conjunction with an associated bearer trunk.
- Advice of Charge (AOC) information that is received on an SBS bearer call is not displayed to the end user. However, AOC information is conveyed to the CDR port for the SBS bearer call record. Only SBS trunk information affects end-user displays.
- ETSI Network Call Deflection (NCD) does not work with an SBS call. For SBS, the signaling that controls the call is in the SBS signaling call on the QSIG interface. NCD, however, requires an ETSI interface that is available only on SBS bearer calls.
- ETSI Network Call Transfer (NCT) does not work with an SBS call. For SBS, the signaling that controls the call is in the SBS Signaling call on a QSIG interface. NCT, however, requires an ETSI interface that is available only on the SBS bearer call.
- Direct SBS calling into Remote Access does not work. Barrier Codes cannot be collected for SBS calls to Remote Access because the SBS bearer call has not yet been established when such tones are prompted for or expected. However, an SBS call can invoke Remote Access by means of a vector collect or a route-to command.
- SBS does not support Wideband Switching (NxDSO).
- Russian Incoming ANI with a button does *not* display the ANI that is received in the SBS bearer call. The system displays to the end user only the ANI that is received on the SBS signaling call.
- Trunk Flash to get recall dial tone from a central office (CO) does not work. End-user activity drives signaling on the SBS signaling call only, and not on the SBS bearer call. QSIG Call Transfer functionality can be used instead.

- R2 MultiFrequency Compelled (MFC) Intercept treatment must drop the SBS bearer and SBS signaling calls, and does so by applying the appropriate treatment to the call originator based on what is received on the R2 MFC bearer call.

Networking features or capabilities that work with SBS

- When authorization codes are required to access the SBS trunk, authorization codes can be collected. The reason is that authorization codes are collected locally before the outgoing trunk is seized.
- Calling Party Number (CPN) restriction can be administered for and signaled on both the SBS signaling and SBS bearer calls. However, end-user displays, including any restrictions, are populated from information that is carried in the SBS signaling call, and not from information in the SBS bearer call.
- At an SBS Interworking node, DCS and DCS+ signaling on the non-SBS portion of the call is interworked to and from the SBS signaling call, to the extent that DCS-QSIG interworking currently applies.
- A DCS trunk can be used as the bearer trunk on an SBS call. However, any DCS signaling information received on the Bearer call is overridden by the QSIG signaling information received on the SBS signaling call.
- User information that is received on an SBS signaling call by an SBS tandem node, or received on a non-SBS trunk by an SBS interworking node, is sent on the SBS signaling call, per current tandeming or interworking procedures on QSIG trunks.
- Temporary Signaling Connection (TSC) messages can be sent over an SBS trunk.
- Look Ahead Routing can be used with both SBS signaling and SBS bearer calls, if such calls start on ISDN trunks.
- In regions where Feature Plus (F+) is offered, SBS calls can use the pseudo-DID functionality of F+. Then, you do not need to obtain direct inward dialing (DID) or DDI numbers from a service provider. You must administer SBS extensions at the SBS terminating node, but these numbers do not need to correspond with real DID or DDI numbers. CPN prefix administration at the SBS terminating node must map the SBS extension to a number that is a national complete number,. Except, the SBS extension portion is not recognized by the PSTN. ARS at the SBS originating node must route this number to a route pattern preference that supports F+. The "No. Dgts SubAddress" administration for this preference must indicate the length of the SBS extension at the SBS terminating node. This number is the number of digits that are extracted from right to left, and sent in the Calling Party Subaddress Information Element. Administration for this preference must also delete the SBS extension digits, and insert the Listed Directory

Number (LDN) extension of the SBS terminating node in its place. The SBS bearer call is routed to the LDN at the SBS terminating node. F+ functionality at the SBS terminating node then routes the call to the SBS extension that is passed in the Subaddress IE, instead of to the attendant. Multiple route patterns are needed at the SBS originating node, if the SBS terminating node uses SBS extensions of various lengths.

SBS extensions that are used with F+ cannot be longer than 5 digits, because F+ is not included in Dial Plan Expansion.

- QSIG MSI messages are sent in the SBS Signaling link. The system ignores any messages that are in the SBS bearer call.
- QSIG Call Completion works with SBS calls.

  Both the original call and the "call-back call" incur separate SBS delays if the call uses SBS trunks.
- QSIG Call Transfer works with SBS calls.

  Both the original call and the second call to the transferred-to party incur separate SBS delays if the call uses SBS trunks.
- QSIG Diversion, forward switch and reroute, works with SBS calls.

  Both the original call and the second call, to the forwarded-to party, incur separate SBS delays if the call uses SBS trunks.
- QSIG Path Replacement works with SBS calls.

  The entire SBS call, both the SBS signaling call and the associated SBS bearer call, are replaced. All separate calls, the original call, the call to the transferred-to party, and then the path replacement call, incur separate SBS delays if the calls use SBS trunks.
- QSIG Enhanced Path Replacement works with SBS calls. Multiple SBS delays apply.
- Non-Avaya QSIG MSI are tandemed to and from any non-SBS QSIG portion of an SBS call (at the SBS interworking node) and on the SBS signaling call (at an SBS tandem node) per existing QSIG transit operation.
- QSIG MWI works with SBS calls.

- QSIG Temporary Signaling Connections (TSCs), known as Call Independent Signaling Connections (CISCs) in QSIG literature, are supported. Non Call Associated Temporary Signaling Connections (NCA TSCs) are signaling-only connections that transport feature information. While NCA TSCs can be initiated as a result of some activity on a bearer call, NCA TSCs are independent of bearer calls. NCA TSCs are set up as nonbearer calls, and use a call reference value (CRV) that is different than any CRV that is in use on any other existing bearer or signaling call on that interface.

  Communication Manager supports two different NCA TSC protocols. Use the signaling group **TSC Supplementary Service Protocol** field on the Signaling Group screen to administer these protocols. The **TSC Supplementary Service Protocol** field is set to **a** for AT&T NCA TSCs, and to **b** for QSIG NCA TSCs (CISCs).

  For full QSIG functionality, you must set the **Supplementary Service Protocol** field on both the Trunk Group screen and the Signaling Group screen to **b** (QSIG). You must set this field to **b**, because some QSIG features, such as QSIG Call Completion and QSIG Message Waiting Indication, use QSIG feature signaling on both the bearer call and on an NCA TSC to work properly.
- QSIG Centralized Attendant Service with MSI works with SBS calls.
- QSIG transit capabilities are supported with SBS calls through tandeming of QSIG signaling to and from any non-SBS QSIG portion of an SBS call (at the SBS interworking node), and on the SBS signaling call (at an SBS tandem node), per existing QSIG transit operation.
- QSIG VALU signaling works with SBS calls. You might need to increase the timer that is used to return QSIG VALU Call Coverage calls back when the calls are unanswered, so that SBS delays do not cause such calls to be returned prematurely. Use the **Local Cvg Subsequent Redirection/CFWD No An Interval (rings)** field on the System Parameters Call Coverage/Call Forwarding screen to administer the timer.
- QSIG Called/Busy Name ID is supported in the SBS signaling call.
- QSIG Calling/Connected Name/Number ID is supported in the SBS signaling call.
- QSIG Call Offer is supported in the same way as over normal QSIG trunks.
- Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or both AAR and ARS can be used to route the SBS signaling call. SBS bearer calls are routed by ARS only, but also can be directed to AAR from ARS.
- SBS calls to an analog station endpoint display the SBS signaling information if the endpoint is served by a TN793 or TN2793 port.
- The Russian Transit/Power Industry Tie Trunk is expected to work as an associated bearer trunk.
- The X-Station Mobility feature works for incoming or outgoing calls that are routed with SBS.
- Leave Word Calling (LWC) for Unanswered External Calls with Automatic Number Identification (ANI) is supported with the information in the SBS signaling call that is stored for the called party.

- ISDN Feature Plus calls are supported, as the SBS bearer call, with the SBS signaling call information that is used for endpoint displays.
- ISDN Calling Party Number Presentation options are supported by SBS in the SBS signaling call.
- QSIG/DCS Partial Reroute works is the same way as it does currently, with the SBS signaling call as the QSIG part of the call.
- DS1 With Echo Cancellation is supported for the SBS bearer call.

Network interface interactions

- DTMF ANI signaling on an incoming SBS bearer call could interfere with the SBS invoked DTMF signaling set to identify the correct bearer call. This service should not be subscribed to on trunk groups that may be used to deliver SBS bearer calls.
- If you use in-band call transfer capability from a network Service Provider (like Take back and Transfer) and subscribe to a *notify* option, the incoming DTMF signals on an SBS bearer call will cause the SBS bearer call to fail. *This service should not be subscribed to on trunk groups that may be used to deliver SBS bearer calls.*
- If you subscribe to Alternate Destination Routing, they must take care to not include the SBS extension numbers in the DID/DDI blocks subject to reroute. If such alternate routing occurs, the incoming SBS bearer call cannot be associated with its SBS signaling call and will be dropped.
- Hong Kong DTMF Supplementary Services information *will not* be displayed to the endpoint user on an SBS call since the display contains information from the SBS signaling call.
- Macedonia E1 Support for PPM messages *will not* be displayed to the endpoint user when this type trunk is used as an SBS bearer because bearer trunk signaling does not impact user displays on SBS calls.
- Calling Party Number (CPN) information received on an SBS bearer call will be tandemed on the SBS bearer call but it will not be displayed to the endpoint user. It is available for Call Detail Recording (CDR) on the bearer call record.
- An analog station connected to a TN793/TN2793 port with Incoming Call ID will see the SBS signaling information when making or receiving an SBS call.
- US Analog Trunk & Line - TN797 - Supports SBS.
- Country specific functionality that does not require end user activation, acknowledgement, or display will be supported on SBS bearer calls. For example, China Disconnect on No-Answer will disconnect the bearer call and the SBS signaling call will also disconnect.
- Disconnect supervision for an SBS bearer call is provided/processed as usual for that type of bearer trunk. If no disconnect supervision is available on a trunk used for an SBS bearer call, then disconnect supervision will be provided by the SBS signaling call. *Dropping either the SBS bearer call or the SBS signaling call will drop the associated SBS signaling/ bearer call respectively.*

- For ISDN trunks, the Incoming Call Handling Table may be used to delete leading digits of the SBS bearer call's called number to direct the call to the indicated SBS Extension. *Digit manipulation must not modify the extension portion of the number, or the SBS bearer call will not terminate to the indicated SBS Extension and thus cannot be associated with its SBS signaling call.*
- For non-ISDN trunks or ISDN bearer trunks using overlap receiving, insertion/deletion may also be used to direct the SBS bearer call to the indicated SBS Extension. *Again, digit manipulation must not modify the extension portion of the number, or the SBS bearer call will not terminate to the indicated SBS Extension and thus cannot be associated with its SBS signaling call.*
- Where ANI is received on an incoming non-SBS call, and the call is tandemed to another Communication Manager using SBS, the received ANI information will be tandemed in the SBS signaling call to the far end per current QSIG interworking procedures. The network interfaces that may receive ANI and then tandem to a SBS call include:
  - Analog CO Trunk (TN429)
  - R2-MFC trunks
  - India MFC trunks
  - Integrated R2-MFC Signaling - DID/CO
  - MFE
  - MFC and Russia MF Multiple ANI
  - Spain MFE
- For the No Disconnect Supervision Trunk Operation, the SBS signaling call will control disconnect supervision for the associated bearer call.

Service Observing

Use the Service Observing feature to allow designated users to listen to another user call.

Detailed description of Service Observing

This section provides a detailed description of the Service Observing feature.

This section describes service observing in environments without Automatic Call Distribution (ACD) or call vectoring. To use service observing in ACD or call vectoring environments, see the *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

With Service Observing, designated users, who are usually supervisors, can listen to other user calls. The user that observes the calls of another user is called an *observer*. Use the Service Observing feature to train agents, or to monitor the quality of service in call centers and other environments where employees serve customers over the telephone.

WARNING:
Listening to the call of another user can be subject to federal, state, or local laws, rules, or regulations. You might need to obtain the consent of one or both of the parties on the call. Ensure that you know, and comply with, all applicable laws, rules, and regulations when you use this feature.

An observer can monitor calls to any of the following entities:

- An extension
- A vector directory number (VDN), on systems with call vectoring
- A logical agent ID, on systems with Expert Agent Selection (EAS)

Observers can monitor calls in listen-only mode or listen-and-talk mode. In listen-and-talk mode, an observer can hear and speak with all parties on a call. The user that is monitored does not know that an observer listens to the call, unless you administer Communication Manager to provide a monitoring tone.

When an observer is off site, the observers can use remote access to monitor calls. In systems with call vectoring, a vector can control access to Service Observing.

If an observer uses a telephone that has a service observe button, the button:

- Blinks while the observer waits for an eligible call
- Lights steadily while the observer observes a call

The system does not reserve a call appearance while the observer is in the wait state, if:

- The observer uses a Feature Access Code (FAC) to activate Service Observing
- No service observe button is administered for the telephone

An idle call appearance must be available for an observer to go to the observing state when an eligible call arrives.

Listen and talk modes

When an observer uses the feature button for Service Observing, the observer can toggle between listen-and-talk mode and listen-only mode. However, when an observer activates Service Observing with an FAC, the observer must choose the listen-only mode or the listen-and-talk mode at the start of the session. If the user wants to change modes after the session starts, the observer must end the session, and then choose the other mode when the observer starts a new session. The FACs for Service Observing are the

- Service Observing Listen Only Access Code
- Service Observing Listen/Talk Access Code

Note that the system also requires a FAC for remote Service Observing.

An observer can observe an agent who is not active on a call. The observer is in wait state until the agent receives a call, and then the observer is bridged onto the call.

Service Observing with Multiple Observers

Service Observing with Multiple Observers means that:

- Up to two observers can monitor the same agent Login ID or station extension using the Service Observing station button or using any of the following Feature Access Codes (FACs):
  - Service Observing Listen-Only
  - Service Observing Listen/Talk
  - Service Observing No-Talk
- Two separate calls, each with an associated service observer, can be conferenced together with both service observers included in the merged conferenced call except when both observers are VDN observers. In this case one VDN observer will be dropped.
- If you use call recording product, such as the Avaya Witness Call Recording or NICE can connect a voice-storage server to a station or Login ID extension in order to record agent-to-customer transactions acting as an observer. Call recording observing can be given priority using the “Service Observing by Recording Device?” COR added for that purpose.

- If you use call recording products, you can allow an observer to monitor a station or Login ID extension and record the transaction at the same time. Note: This feature does not allow multiple observers on the same call for the Service Observing by VDN feature.

For more information on Service Observing with Multiple Observers, see *Avaya Aura™ Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568.

Telephone displays

The system displays the same information for both the user and the local observer. The service observer's display shows "<origination> to <destination> so <origination> is the Observed Party's information, and <destination> can either be the called-party or a trunk.

Trunk calls

When a user places a trunk call, Service Observing starts when the user finishes dialing the call. For calls on central office (CO) trunks, the system considers dialing to be complete when the answer supervision is returned, or when the answer supervision timeout occurs.

The system denies any attempt to use Service Observing over trunks that do not have disconnect supervision.

Warning and conference tones

You can administer a tone that notifies the parties on a call that the call is observed. You can administer the tone as a warning tone or a conference tone.

If you administer the tone as a:

- Warning tone, the system generates a unique 2-second, 440-Hz tone before an observer connects to the call. While the call is observed, the system repeats a shorter version of this tone every 12 seconds.
- Conference tone, the system generates the conference tone before an observer connects to the call. The system does not repeat the conference tone during the call.

Administering Service Observing

This section describes the screens that you use to administer the Service Observing feature

Screens for administering Service Observing

Screen name	Purpose	Fields
Class of Restriction	Set up the Class of Restriction (COR) to support Service Observing.	• **Can Be Service Observed** • **Can Be Service Observer** • **Service Observing COR Table**
Feature Access Code (FAC)	Specify the FACs for Service Observing.	• **Service Observing Listen Only Access Code** • **Service Observing Listen/Talk Access Code**
Feature-Related System Parameters	Enable Expert Agent Selection (EAS) for the system.	**Expert Agent Selection (EAS) Enabled?**
	Enable a conference tone for observed users.	**Service Observing Conference Tone?**
	Enable a warning tone for observed users.	**Service Observing Warning Tone**
Station (multiappearance)	Assign the **serv-obsrv** button for Service Observing.	Any available button field in the **Button Assignment** area
Optional Features	Enable Service Observing for: • Basic or logical agent ID observing • Remote access • Vector Directory Numbers (VDNs) • Vector-initiated observing	• **Service Observing (Basic)** • **Service Observing (Basic) and Service Observing (Remote/By FAC)** • **Service Observing (Basic) and the Service Observing (VDNs)** • **Vectoring (Prompting)**

End-user procedures for Service Observing

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Service Observing:

- Activating Service Observing
- Deactivating Service Observing

To activate Service Observing:

1. Press the **serv-obsrv** button or dial a Feature Access Code (FAC).
2. Dial the extension that you want to observe.

   When you use the **serv-obsrv** button to activate Service Observing, you start in listen-only mode. Press the **serv-obsrv** button to toggle between listen-only mode and listen/talk mode.

To deactivate Service Observing:

- Hang up, select another call appearance, or press the disconnect or release button.

Reports for Service Observing

The following reports provide information about the Service Observing feature:

- None

Considerations for Service Observing

This section provides information about how the Service Observing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Service Observing under all conditions. The following considerations apply to Service Observing:

- None

Interactions for Service Observing

This section provides information about how the Service Observing feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Service Observing in any feature configuration.

- Attendants

  An attendant can be observed, but cannot be an observer.

- Bridged Appearances

  You observe calls on a primary extension and all bridged appearances of that extension. You cannot observe bridged appearances on the extensions phone. For example, if you are observing extension 3082 and this telephone also has a bridged appearance for extension 3282, you cannot observe calls on the bridged call appearance for 3282. But if you observe extension 3282, you can observe activity on the primary and all of the bridged call appearances of 3282.

  The primary telephone user or bridging user can bridge onto a service observed call of the primary at any time. A bridging user cannot activate Service Observing using a bridged call appearance.

  If the primary is service observing on an active call, a bridged call appearance cannot bridge onto the primary line that is doing the service observing.

- Busy-Verification

  You cannot observe an extension that is being busy-verified. You cannot busy-verify an extension that is being observed.

- Call Coverage and Call Pickup

  An observer cannot observe a call that is answered by a covering agent or a member of a pickup group, unless the called agent bridges onto the call.

- Call Park

  An observer cannot park the observed call.

- Call Waiting

  Incoming calls do not wait on a single-line telephone that is being observed.

- Conference

  An observer cannot initiate a conference call while the observer is also observing a call.

  If an observed user starts a conference, or enters a conference call that has fewer than six parties, the system places the observer in the wait state until the system connects the call. Then the observer can observe the conference. The system counts the observer as one of the conference call participants. The observer can observer all of the conference participants, regardless of the Class of Restriction (COR). In addition, the system bridges the observer onto any calls that a conference participant places or receives while the conference is active. When the user leaves the conference, the observer also leaves and returns to observing the original call.

- Data Privacy

  An observer cannot observe an extension:

  - On which Data Privacy is active
  - While the extension is on a conference call with another extension for which Data Privacy is active

- Data Restriction

  An observer cannot observe an extension

  - On which Data Restriction is active.
  - While the extension is on a conference call with another extension for which Data Restriction is active

- Integrated Directory

  Observers do not hear a user dial an integrated directory number.

- Distributed Communications System (DCS)

  To observe user extensions that are on another node, such as a DCS station extension, the observer must set up remote-access service observing.

  The system does not transmit service observing displays across DCS networks.

- Hold

  An observer cannot place a call on hold while the observer is also observing a call.

  If a user who is being observed places a call on hold, the observer enters the wait state.

- IP Solutions

  If an observer observers an IP to IP direct call, the users on the call might hear a break-in conversation of about 200 milliseconds.

- Leave Word Calling (LWC)

  Parties on an observed call cannot use LWC.

- Music-on-Hold

  If an observer is in listen-talk mode, neither the caller nor the observer hears music-on-hold. If an observer is in listen-only mode, the caller hears music-on-hold, but the observer does not.

- Privacy - Manual Exclusion

  Observing towards a station with Exclusion active is denied, or if Exclusion is activated by a station while being observed, all bridged parties including the observer are dropped. If the **Service Observing with Exclusion** field on the Feature-Related System Parameters screen is **y**, then Service Observing of a station with Exclusion active, either by Class Of Service or by manual activation of Exclusion, is allowed.

- Transfer

  An observer cannot initiate a transfer while the observer is also observing a call.

  If a user transfers a call, the observer is placed in the wait state. The observer is bridged onto the call when the transfer is complete.

Station Hunting

Use the Station Hunting feature to find an extension that is available to answer a call when the called extension is busy. The system checks for an idle extension in the station-hunting chain of the called extension before the system routes the call to the coverage path of the called extension.

The Station Hunting feature supports the following capabilities:

- Station Hunting Before Coverage

  If the system finds an idle extension in the station-hunting chain of the called extension, the system leaves the call at the idle extension.

- Station Hunting After Coverage

  If the system does not find an idle extension in the station-hunting chain of the called extension, the system routes the call to the coverage path of the last extension in the station-hunting chain.

Detailed description of Station Hunting

This section provides a detailed description of the Station Hunting feature.

To use Station Hunting, you create a station-hunting chain. This chain governs the order in which the system routes the calls when the system encounters a busy station. Each station in the chain links to only one subsequent station in the station-hunting chain. However, a station can be the receiving link from any number of station-hunting chains.

When the system starts to check the station-hunting chain, the system updates the display of the calling party with an **h**. The system also updates the display of the called party with an **h**.

You can administer an unlimited number of extensions in a station-hunting chain.

Table 86: Routing calls through a Station Hunting chain on page 1500 shows how the system routes a call through the station-hunting chain.

Table 86: Routing calls through a Station Hunting chain

Condition	Response
The extension is idle.	• The caller hears ringing. • The system does not continue to route the call through the station-hunting chain.
The extension is busy.	The system routes the call to the next extension in the station-hunting chain.
The **hunt-to-station** field on the Station screen of the extension is blank.	• The caller hears busy tone. • The system does not continue to route the call through the station-hunting chain.
The system encounters a station in the station-hunting chain for the second time.	• The caller hears busy tone. • The system does not continue to route the call through the station-hunting chain.
The system checks 30 extensions in the station-hunting chain, and does not find an idle extension.	• The caller hears busy tone. • The system does not continue to route the call through the station-hunting chain.

Station Hunting and Call Coverage

You can administer the system to perform station hunting before the system sends calls to coverage, or after the system sends calls to coverage.

If you administer the system to use Station Hunting before the system uses Call Coverage, the system checks for a hunt-to station at the called extension. If the system finds a hunt-to station at the called extension, the system routes the call down the station-hunting chain. If the system does not find an idle extension in the station-hunting chain, the system routes the call to coverage.

Removing a station from a Station Hunting chain

When you remove a station from a station-hunting chain, the system attempts to maintain the chain. Consider the following examples:

- Station 1 links to station 2, and station 2 links to station 3. If you remove station 2, the system links station 1 to station 3.
- Station 1 links to station 2. Station 2 does not link to another extension. If you remove station 2, station 1 no longer links to another extension.

Duplicating a station in a Station Hunt chain

When you duplicate a station, the system does not copy the extension that is in the **hunt-to station** field on the Station screen to the station that you duplicate.

Administering Station Hunting

The following steps are part of the administration process for the Station Hunting feature:

- Assigning station hunting after coverage
- Assigning a hunt-to station to an extension
- Administering Station Hunting before Coverage

This section describes:

- Any prerequisites for administering the Station Hunting feature
- The screens that you use to administer the Station Hunting feature
- Complete administration procedures for the Station Hunting feature

Prerequisites for administering Station Hunting

You must complete the following actions before you can administer the Station Hunting feature:

- None

Screens for administering Station Hunting

Screen name	Purpose	Fields
Coverage Path	Activate the Hunt after Coverage capability for a coverage path.	**Hunt After Coverage**
Station	Assign a hunt-to station to an extension.	**Hunt-to Station**
System-Parameters Call Coverage/Call Forwarding	Enable the Station Hunting before Coverage capability for your system.	**Station Hunt Before Coverage**

Assigning station hunting after coverage

To assign the Station Hunting after Coverage capability to a coverage path:

1. Type **`change coverage-path n`**, where ***n*** is the number of the coverage path to which you want to assign the Station Hunting after Coverage capability. Press **Enter.**

   The system displays the Call Coverage screen (Figure 386: Coverage Path screen on page 1503).

Figure 386: Coverage Path screen

```
 change coverage path 2                                          Page 1 of 1
                                COVERAGE PATH

            Coverage Path Number: 2
                                          Hunt After Coverage: y
                Next Path Number: ___     Linkage: ___  ___

COVERAGE CRITERIA

  Station/Group Status   Inside Call   Outside Call
            Active?            n             n
              Busy?            y             y
     Don't Answer?             y             y Number of Rings:2
               All?            n             n
DND/SAC/Goto Cover?            y             y

COVERAGE POINTS

   Terminate to Coverage Pts. with Bridged Appearance? n

     Point1: _________ Point2: _________ Point3: _________
     Point4: _________ Point5: _________ Point6: _________
```

2. In the **Hunt After Coverage** field, perform one of the following actions:
   - If you want the system to check the station-hunting chain of the last extension in the coverage path, if the system does not find an idle station in the coverage path, type **y**.
   - If you want the system to leave the call at the last available point in the coverage path, type **n**.
3. Press **Enter** to save your changes.

Assigning a hunt-to station to an extension

To assign a hunt-to station to an extension:

1. Type **`change station n`**, where ***n*** is the number of the extension to which you want to assign a hunt-to station. Press **Enter.**

   The system displays the Station screen (Figure 387: Station screen on page 1504).

Figure 387: Station screen

```
change station 1014                                          Page 1 of 4
                              STATION

Extension: 1014               Lock Messages? n                    BCC: 0
     Type:                    Security Code:                       TN: 1
     Port:                  Coverage Path 1:                      COR: 1
     Name:                  Coverage Path 2:                      COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                           Message Lamp Ext: 1014
           Speakerphone: 2-way                    Mute button enabled? y
       Display Language? English                     Expansion Module?
                   Model:
                                                    Media Complex Ext:
                                                         IP Softphone? y
                                                  Remote Office Phone? y
```

2. In the **Hunt-to Station** field, perform one of the following actions:
   - Type the extension that you want the system to check for an idle status, if the extension is busy.
   - If you do not want the system to check further for an idle extension, if the extension that you specified in Step 1 is busy, leave the field blank.
3. Press **Enter** to save your changes.

Administering Station Hunting before Coverage

To administer the Station Hunting before Coverage capability for your system:

1. Type **`change system-parameters coverage-forwarding`**. Press **Enter.**

   The system displays the System-Parameters Coverage-Forwarding screen (Figure 388: System Parameters-Call Coverage/Call Forwarding screen on page 1505).

Figure 388: System Parameters-Call Coverage/Call Forwarding screen

```
 change system-parameters coverage-forwarding                      page 1

               SYSTEM PARAMETERS -- CALL COVERAGE / CALL FORWARDING

CALL COVERAGE/FORWARDING PARAMETERS
           Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): _
         Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): _
                          Coverage - Caller Response Interval (seconds): _
     Threshold for Blocking Off-Net Redirection of Incoming Trunks Calls: 1

COVERAGE
                                        Keep Held SBA at Coverage Point? _
        External Coverage Treatment for Transferred Incoming Trunk Calls? _
         Immediate Redirection on Receipt of PROGRESS Inband Information? _
                                                Maintain SBA At Principal? _
              QSIG VALU Coverage Overrides QSIG Diversion with Rerouting? _
                                           Station Hunt Before Coverage? n

FORWARDING
                                                    Call Forward Override? _
                                                  Coverage After Forwarding? _
```

2. In the **Station Hunt Before Coverage?** field, perform one of the following actions:
   - To enable the Station Hunting Before Coverage capability for your system, type **y**.
   - To disable the Station Hunting Before Coverage capability for your system, type **n**.
3. Press **Enter** to save your changes.

Reports for Station Hunting

The following reports provide information about the Station Hunting feature:

- The List Usage report shows all the extensions that use an extension as the hunt-to-station.

For detailed information on these reports and the associated commands, see *Avaya Aura™ Communication Manager Reports*, 555-233-505.

Interactions for Station Hunting

This section provides information about how the Station Hunting feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Station Hunting in any feature configuration.

Remember that the system checks the station-hunting chain only for idle and available extensions.

- Adjunct Switch Applications Interface (ASAI)

  The system checks the station-hunting chain when ASAI routes a call to an extension with a
  hunt-to station.

- Automatic Call Distribution (ACD)

  An agent extension can be part of a station-hunting chain. The system checks the station-hunting chain of the agent only when the caller places the call directly to the agent extension. The system does not check a station-hunting chain for calls that the system routes through hunt groups to an ACD agent.

  The system does not check a station-hunting chain for calls that are made to an extension for a logical agent.

- Automatic Callback

  The system does not check the station-hunting chain of the called extension when the call is a callback-return call.

- Bridged Appearance

  The system checks the station-hunting chain of an extension if the principal station does not have a call appearance at which the call can terminate. The system checks the chain, even though the extension has available bridged appearances on other stations.

- Busy Verification

  The system does not check a station-hunting chain for busy-verify calls.

- Call Coverage

  Call Coverage has precedence over Station Hunting.

  The system uses Station Hunting for the last coverage point of the last station in the station-hunting chain under the following conditions:

  - The **Hunt After Coverage** field, on the Call Coverage screen is set to **y**.
  - The last coverage point is unavailable because the coverage point is busy, or no one answers the call.
  - The last coverage point is a station that has an assigned hunt-to station.

– No one in the coverage path answers the call.

Coverage Don't Answer covers the call after the system checks the station-hunting chain, if the call can terminate at the coverage point, but no one answers the call.

If Station Hunting before Coverage is enabled on your system, the system checks the station-hunting chain of the called extension, before the system routes the call to the coverage path of the called extension.

The system routes the call to the coverage path of the called extension unless the called extension is associated with an XDID telephone. If the called extension is associated with an XDID telephone, the system routes the call to the coverage path of the non-XDID extension in the hunt-to field of the XDID station.

- Call Detail Recording (CDR)

  CDR records the called extension, and not the extension of the user who answers the call.

- Call Forwarding

  Call Forwarding has precedence over Station Hunting.

  If an idle station has Call Forwarding active, the system forwards the call. If a busy station has Call Forwarding active, the system forwards the call. If the forwarded-to station is busy, the call follows the station-hunting chain of the forwarded-to extension.

- Call Park

  The system does not check a station-hunting chain for callpark-return calls.

- Call Pickup

  Station Hunting does not change the operation or the characteristics of Call Pickup.

- Call Vectoring

  You cannot type a vector directory number (VDN) as a hunt-to station.

  If the system encounters **with cov y** in a **`route-to`** command, the system routes a call to a busy station to the station-hunting chain of the station. The system does not route the call to the coverage path of the station.For more information, see the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.

- Call Waiting and Attendant Call Waiting

  Station Hunting has precedence over Call Waiting.

  If a called extension has Call Waiting active, and the extension is already busy on a call, the system checks the station-hunting chain. If the system cannot terminate the call to a station in the station-hunting chain, the call waits at the called extension.

- Class of Restriction (COR)

  The system checks the COR of the called extension. The system does not check the COR of the stations in a station-hunting chain.

- Distributed Communications System (DCS)

  Station Hunting is not a DCS feature. All stations in a station-hunting chain must be on the same server that runs Communication Manager.

- Do Not Disturb

  If Do Not Disturb is active at a station, the system does not check a station-hunting chain for a call to the station.

- Extension Number Portability (ENP)

  You cannot assign a remote ENP extension as a hunt-to station.

- Hunting and Hunting Group

  You cannot assign a direct departmental calling (DDC) or uniform call distribution (UCD) extension as a hunt-to station.

- Intercom Call

  The system denies Station Hunting for intercom calls to a busy extension.

- Leave Word Calling (LWC)

  If a caller starts LWC, the LWC message is left at the called extension even if the system uses Station Hunting in an attempt to complete the call.

- Multimedia

  Calls to multimedia endpoints must convert to voice before the system checks a station-hunting chain for the call.

- Night Service

  The system denies Station Hunting when a night service call is made to a busy night-console extension.

- Outgoing Trunk Queueing (OTQ)

  The system does not attempt Station Hunting for an OTQ callback-return call.

- Personal Central Office Line (PCOL)

  The system does not attempt Station Hunting for a PCOL call.

- Personal Station Access (PSA)

  The system considers a station with PSA dissociated as busy and bypasses the station in the station-hunting chain.

- Priority Call

  The system denies Station Hunting for priority calls.

- Restriction

  The system applies proper intercept treatment to a restricted, called extension. Note that *the system does not check restrictions on hunt-to stations.*

- Send All Calls

  Send All Calls coverage takes precedence over Station Hunting.

- Tenant Partitioning

  The system applies normal tenant restrictions to a call to the called extension. Note, however, that *the system does not check tenant restrictions on hunt-to stations.*

- Terminal Translation Initialization (TTI)

  The system considers a station with TTI separation as busy and bypasses the station in the station-hunting chain.

- Terminating Extension Group (TEG)

  You cannot assign a TEG as a hunt-to station.

- Uniform Dial Plan (UDP)

  You cannot assign a remote UDP extension as a hunt-to station.

- X-ported extension

  You can assign a hunt-to station to a station that is administered with **x** in the **Port** field of the Station screen. The system bypasses a hunt-to station that is administered with an **x** in the **Port** field of the Station screen.

Station Lock

Use the Station Lock feature to lock a telephone to prevent others from placing outgoing calls from the telephone.

Detailed description of Station Lock

This section provides a detailed description of the Station Lock feature.

With the Station Lock feature, users can lock the telephone to prevent others from placing outgoing calls from the telephone.

A user with an analog telephone uses a Feature Access Code (FAC) to lock the telephone. A user with a digital telephone can use a FAC or a feature button to lock the telephone. Station Lock:

- Blocks unauthorized outgoing calls
- Allows outgoing emergency calls
- Allows incoming calls

The feature button lights when the user presses the button to activate Station Lock. Then, when a user attempts to place an outgoing call, the system generates a special dial tone to indicate that the Station Lock feature is active.

H.323 or DCP phones support the station lock functionality of Communication Manager. SIP phones do not support the functionality. If a digital or IP station has a Station Lock button but activates the feature with the FAC, the LED for the button lights and special dial tone is provided. Also, if a digital or IP station has a feature button for Station Lock and uses this button to activate the feature, the LED lights. In this case also, the system generates the special tone. If a digital telephone does not have a feature button for Station Lock, and uses a FAC to activate the feature, the system generates the special tone.

Avaya recommends that a user of a digital telephone use a Station Lock button, instead of a FAC, to activate Station Lock.

Any user who knows the system-wide FAC for Station Lock, and the Station Security Code (SSC) of a specific telephone, can lock or unlock the telephone.

A user can also lock or unlock a telephone from a remote location.

The attendant console can lock or unlock other telephones. The attendant console cannot be locked.

Station Lock by time of day

Beginning with Communication Manager 4.0 or later, you can you can also lock stations using a Time of Day (TOD) schedule.

To engage the TOD station lock/unlock you do not have to dial the station lock/unlock FAC, or use **stn-lock** button push.

When the TOD feature activates the automatic station lock, the station uses the Class of Restriction (COR) assigned to the station lock feature for call processing. The COR used is the same as it is for manual station locks.

The TOD lock/unlock feature does not update displays automatically, because the system would have to scan through all stations to find the ones to update.

The TOD Station Lock feature works as follows:

- If the station is equipped with a display, the display will show “Time of Day Station Locked”, if the station invokes a transaction which is denied by the Station Lock COR. Whenever the station is within a TOD Lock interval, the user will hear a special dial tone instead of the normal dial tone, if the special dial tone is administered.
- For analog stations or without a display, the user hears a special dial tone. The special dial tone has to be administered and the user hears it when the station is off hook.

After a station is locked by TOD, it can be unlocked from any other station if the Feature Access Code (FAC) or button is used. You have to also know the Station Security Code, and that the **Manual-unlock allowed?** field on the T**ime of Day Station Lock Table** screen is set to **y**.

Once a station has been unlocked during a TOD lock interval, the station remains unlocked until next station lock interval becomes effective.

If the station was locked by TOD and by Manual Lock, an unlock procedure will unlock the Manual Lock as well as the TOD Lock (“Manual-unlock allowed?” field on the **Time of Day Station Lock Table** screen is set to **y**).

The TOD feature does not unlock a manually locked station.

Note:
The attendant console cannot be locked by TOD or manual station lock.

For more information, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Screens for administering Station Lock

Screen name	Purpose	Fields
COR	Administer a Class of Service (COR) that allows the user to activate Station Lock with a Feature Access Code (FAC).	**Station Lock COR**
Feature Access Code (FAC)	Assign a FAC for Station Lock.	**Station Lock Activation**
Station	Assign the user a COR that allows the user to activate Station Lock with an FAC.	**COR** **Time of Day Lock Table**
	Assign a **sta-lock** feature button for a user.	Any available button field in the **Button Assignments** area
	Assign a Station Security Code (SSC) for a user.	**Security Code**
Time of Day Station Lock Table	Administer station lock by time of day.	**Table Active?** **Manual Unlock Allowed?** **Time Intervals**

End-user procedures for Station Lock

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Station Lock:

- Activating or deactivating Station Lock from a remote telephone

Activating or deactivating Station Lock from a remote telephone

To activate or deactivate Station Lock from a remote telephone:

1. Dial a valid barrier code.

   The system generates a dial tone.
2. Dial the Feature Access Code (FAC) for Station Lock.
3. Dial the extension number.
4. Dial the Station Security Code (SSC).

Interactions for Station Lock

This section provides information about how the Station Lock feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Station Lock in any feature configuration.

- Attendant Console

  You cannot lock an attendant console, but you can lock a digital station that has console permissions.

  You can dial the Feature Access Code (FAC) for Station Lock from the attendant console to remotely activate or deactivate Station Lock for another telephone.
- Personal Station Access (PSA)

  You can use Station Lock to lock a PSA telephone, if the telephone has an extension. When a telephone is dissociated, you cannot activate Station Lock from the telephone.

Hot Desking Enhancement

Hot Desking is a generic term for features that enable you to lock and unlock your telephones or to move a fully customized station profile to another compatible telephone. Hot Desking enhances the existing features:

- IP Login/Logoff
- PSA Association/Dissociation
- Station Lock and Time of Day Station Lock

Hot Desking Enhancement (HDE) is limited to the 96xx-series H.323 IP telephones. It does not require any special license to be operational. Parts of the enhancement require firmware changes for the telephones. Only the 96xx-series H.323 IP telephones with the appropriate firmware change support the full range of HDE. The **Hot Desking Enhancement Station Lock** field is available on page 3 of the Feature-Related System Parameters screen, as shown in Figure 389:

Figure 389: Feature-Related System Parameters Screen

```
change system-parameters features                              page 3 of x

                          FEATURE-RELATED SYSTEM PARAMETERS
TTI/PSA PARAMETERS

   WARNING! SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE

         Terminal Translation Initialization (TTI) Enabled? y_
              TTI State: ________         TTI Security Code:
         Enhanced PSA Location/Display Information Enabled?
                           Default COR for Dissociated Sets:
                              CPN, ANI for Dissociated Sets:
           Unnamed Registrations and PSA for IP Telephones?
               Customer Telephone Activation (CTA) Enabled?
  Don't Answer Criteria for Logged off IP/PSA/TTI Stations? n
                      Hot Desking Enhancement Station Lock? n

EMU PARAMETERS
          EMU Inactivity Interval for Deactivation (hours): 1

CALL PROCESSING OVERLOAD MITIGATION
           Restrict Calls: stations-first
```

Station Lock

Communication Manager Release 5.2 makes more restrictions available on the Station Lock feature. When the Hot Desking Enhancement feature is activated, the following are restricted:

- Access to telephone capabilities (applies to 96xx H.323 IP telephones with firmware changes)
- Call log
- Avaya menu
- Contact list
- USB access
- Redial button

- Bridging on Extension to Cellular calls
- Access to bridged appearances

Additionally, enabling the HDE feature by using the **Hot Desking Enhancement Station Lock** field in the Feature-Related System Parameters screen locks further capabilities. The capabilities are distributed among the telephone and Communication Manager.

Telephones

Parts of the Hot Desking Enhancement (HDE) feature apply only to telephones with firmware changes, while other parts apply to all telephones. The table here provides an overview. For information on firmware vintage number, contact your Avaya representative.

HDE Feature	96xx H.323 with FW changes	96xx H.323 without FW changes	Other sets with display	Other sets without display
PSA Logoff Display Login Information	X	X	X	–
Station Lock No access to telephone capabilities (Note 1)	X	X	–	–
Station Lock Extension to Cellular blocked (no make, answer and bridge)	X	X	X	X (Note 2)
Station Lock Bridged appearances blocked	X	X	X	X (Note 3)
Station Lock Limited Access to Feature Access Codes and Feature Buttons	X	X	X	X

Note 1: Telephone capabilities are call log, Avaya menu, contact list, USB access and redial button.

Note 2: If the set offers Extension to Cellular.

Note 3: If the set offers bridged appearances.

Station Security Code

Use the Station Security Code (SSC) to deny other users access to the functions that are associated with the station. Each station user can change their own SSC if they know the station's current settings.

Detailed description of Station Security Code

This section provides a detailed description of the Station Security Code (SCC) feature.

Use the Station Security Code (SSC) to deny other users access to the functions that are associated with the station. Each station user can change their own SSC if they know the station's current settings.

SCC enhances system security. To use SCC, you must provide each user with an individual SSC. You must also create a system-wide Feature Access Code (FAC) that users use to change the individual SSC. A user cannot change a blank SSC.

Administering Station Security Code

The following steps are part of the administration process for the Station Security Code feature:

- Creating a Station Security Code

This section describes:

- The screens that you use to administer the Station Security Code feature
- Complete administration procedures for the Station Security Code feature

Screens for administering Station Security Code

Screen name	Purpose	Fields
Feature Access Code (FAC)	Set the access code for the feature.	**Station Security Code Change Access Code**
Security-Related System Parameters	Set the minimum length of the code.	**Minimum Station Security Code Length**
Station	Set the code for the station extension.	**Security Code**

Creating a Station Security Code

To create a Station Security Code:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen.

2. Type **#5** in the **Station Security Code Change Access Code** field.

   This action sets the access codes for this feature. The system displays the Command prompt.

3. Press **Enter** to save your changes.

4. Type **`change system-parameters security`**. Press **Enter**.

   The system displays the Security-Related System Parameters screen.

5. In the **Minimum Station Security Code Length** field**,** type **7**.

   This action determines the minimum required length of the Station Security Codes that you enter on the Station screen. Longer codes are more secure. If you use station security codes for external access to telecommuting features, Avaya recommends that you use a minimum length of 7 digits.

6. Press **Enter** to save your changes.

7. Type **`change station`** ***`n`***, where ***`n`*** is the extension that you configured for telecommuting. Press **Enter**.

   The system displays the Station screen (Figure 390: Station screen on page 1519).

Figure 390: Station screen

```
change station 1014                                          Page 1 of 4
                                  STATION

Extension: 1014                Lock Messages? n                      BCC: 0
     Type:                     Security Code: 7654321                 TN: 1
     Port:                   Coverage Path 1:                        COR: 1
     Name:                   Coverage Path 2:                        COS: 1
                             Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                           Message Lamp Ext: 1014
           Speakerphone: 2-way                    Mute button enabled? y
       Display Language? English                     Expansion Module?
                   Model:
                                                    Media Complex Ext:
                                                         IP Softphone? y
                                                  Remote Office Phone? y
```

8. Type a number in the **Security Code** field that is equal in length to the number of digits that you entered in the Security-Related System Parameters screen in Step 5.

   In this example, the security code is **7654321** in the **Security Code** field. This number is equal to the minimum number of digits that you entered in the Security-Related System Parameters screen.

9. Press **Enter** to save your changes.

Interactions for Station Security Code

This section provides information about how the Station Security Code feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Station Security Code in any feature configuration.

Users may need a Station Security Code to use the following system features and capabilities:

- Demand printing
- Extended User Administration of Redirected Calls
- Leave Word Calling (LWC)
- Personal Station Access (PSA)
- Voice Message Retrieval
- Station Lock

- Terminal Self-Administration
- User Change Coverage

Station Security Code (Display Guidance)

You can change the Security Code after the system administrator enables the feature on the Feature Access Code (FAC) screen. Use the following change security code procedure for changing the station security code:

End-user administration

Activation

1. After dialing the Feature Access Code (FAC), you can hear a dial tone, and the following text appears:



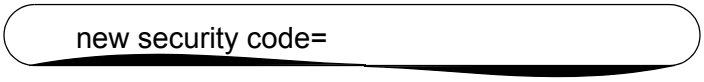
This text appears together with the dialed digits until the number is complete.

2. After this, you receive no dial tone but the display prompts:



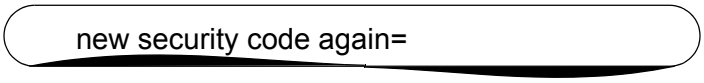
The typed-in security code appears as asterisks (*).

3. Then you receive dial tone and the display prompts:



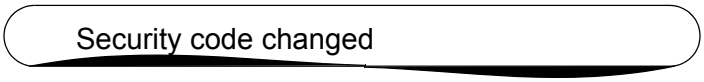
The typed-in security code appears as asterisks (*).

4. Then you receive dial tone and the display prompts:



The typed-in security code appears as asterisks (*).

5. You receive acknowledgement from the confirmation tone (3-beep) and additionally the text appears as follows:



When the call appearance turns to idle (for example, you place the handset on hook, or after timeout) this text is deleted.

Exception Handling

The system notifies you with a rejection tone where it detects an incorrect input and the following message displays:



When the call appearance turns to idle (for example, you place the handset on hook, or after timeout) this text is deleted.

Supporting TTY Callers

Use the Supporting TTY Callers feature to enable callers to use a teletypewriter device (TTY) to listen to announcements that play TTY recordings. You can also use this feature to set up hunt groups for TTY callers, and to create vectors that process both TTY callers and voice callers.

TTY is also known as TDD (Telecommunications Device for the Deaf).

Detailed description of Supporting TTY Callers

This section provides a detailed description of the Supporting TTY Callers feature.

Reliable transmission of TTY information complies with the requirements and guidelines that are outlined in United States accessibility-related laws. Those laws include:

- Titles II, III, and IV of the Americans with Disabilities Act (ADA) of 1990.
- Sections 251 and 255 of the Telecommunications Act of 1996.
- Section 508 of the Workforce Investment Act of 1998.

Communication Manager TTY support is currently restricted to TTY devices that use either the:

- US English standard TTY protocol, specified by ANSI/TIA/EIA 825 as: "A 45.45 Baud FSK modem."
- UK English standard TTY protocol, Baudot 50.

Important characteristics of the standards are:

- TTYs are silent when not transmitting. Unlike fax machines and computer modems, TTYs have no "handshake" procedure at the start of a call, nor do they have a carrier tone during the call. This approach has the advantage of permitting TTY tones, DTMF, and voice to be intermixed on the same call.
- The ability to intermix voice and typed TTY data on the same call. The most common usage is by people who are hard of hearing, but who can speak clearly. These people often prefer to receive text on a TTY device, and then speak in response. This process is referred to as Voice Carry Over (VCO).
- Operation is "half duplex." TTY users must take turns transmitting and typically cannot interrupt each other. If two people try to type at the same time, two TTY devices might show no text at all or show text that is unrecognizable. Also, no automatic mechanism exists to let TTY users know when a character that the user correctly typed was received incorrectly.

- Each TTY character consists of a sequence of seven individual tones.The first tone is always a "start tone" at 1800 Hz. This tone is followed by a series of five tones, at either 1400 or 1800 Hz, which specify the character. The final tone in the sequence is always a "stop tone" at 1400 Hz. The stop tone is a border that separates this character from the next.

The following types of systems support TTY communication:

- Analog telephones and trunks
- Digital telephones and trunks
- VoIP gateways
- Messaging systems
- Automated attendant systems
- Interactive Voice Response (IVR) systems
- Wireless systems in which a TTY-compatible coder is used

Setting up announcements for TTY callers

TTY devices typically resemble a laptop computer. TTY devices have a one line-or a two-line alphanumeric display, instead of the computer screen.

You record announcements for TTY callers in the same way as you record voice announcements. However, instead of recording from the handset of your telephone, you record from a TTY device. The device is attached to your telephone. You use an n acoustic coupler into which you place the telephone handset or by plugging the TTY device directly into the back, if it is a digital phone. After calling the announcement extension, and pressing 1 to record. To use the device, you type the announcement using the TTY device.

If you use an acoustic coupler to connect your telephone for recording, you can record TTY and voice into a single announcement. In this case, when you press **1** to record, you can type the TTY message, then immediately pick up the handset to record the voice message. For this type of recording, digital phones also offer the option to press **#** to complete the recording, which eliminates any extraneous noise at the end of the recording. Unfortunately, using this method for combined TTY and voice recordings is likely to create extraneous noise in the middle of your announcements.

As a alternative to recording with your telephone, you can create .WAV files on other recording applications and you can then copy and save the .WAV files to your announcement board.

Setting up hunt groups for TTY callers

In a call center, TTY callers can be accommodated by a hunt group that includes TTY-equipped agents. Although many TTYs can connect directly with the telephone network by way of analog RJ-11 jacks, Avaya recommends that agents be equipped with TTYs that include an acoustic coupler that can accommodate a standard telephone handset. One reason for this recommendation is that a large proportion of TTY users are hearing impaired, but can speak clearly. These individuals often prefer to receive calls on a TTY and then speak in response. This requires the call center agent to alternate between listening on the telephone and then typing on the TTY. An acoustically coupled configuration makes this process considerably easier.

Although TTY-emulation software packages are available for personal computers, most of these packages do not have the ability to intermix voice and TTY on the same call.

For a TTY hunt group, you can record TTY announcements and use them for the hunt group queue. To record announcements for TTY, follow the same steps as with voice recordings from your telephone. However, instead of speaking into your phone to record, you type the announcement with the TTY device.

For an alternative to creating a TTY hunt group, you can use vectors to process TTY calls. With vectors, you can allow TTY callers and voice callers to use the same phone number. In this case, you can also record a single announcement that contains both TTY signaling and a voice recording.

Handling TTY calls with vectors

Unlike fax machines and computer modems, a Tele-typewriter device (TTY) has no handshake tone and no carrier tone. A TTY is silent when not transmitting. This is why systems cannot identify TTY callers automatically. However, the absence of these special tones also means that voice and TTY tones can be intermixed in prerecorded announcements. The ability to provide a hybrid voice-and-TTY announcement, when combined with the automated attendant vectoring capability, can permit a single phone number to accommodate both voice and TTY callers.

The following sample shows a vector that allows TTY callers to access a TTY agent. It begins with a step that plays a TTY announcement combined with a voice announcement. The announcement tells the TTY caller to dial a digit that will direct them to a TTY support person. The vector then processes the digit entered to connect the TTY caller to the TTY split (or hunt group).

In the following example, split 47 (hunt group 47) has already been established and consists of TTY-enabled agents.

If a TTY caller calls the number that connects to vector 33, the following actions occur:

1. After a short burst of ringing, a quick burst of TTY tones is sent to the caller to tell the caller to hold, HD. Then a voice announcement is played for callers using a normal telephone connection. The announcement tells them to stay on the line. Finally, another burst of TTY tones is sent to the TTY caller which displays on the caller's TTY device as, "Dial 1."

   The TTY caller does not hear the voice announcement, but because the step collects digits, the steps allows the caller to dial a 1 from a touchtone telephone.

   Note:
   For voice callers, the burst of TTY tones lasts about one second and sounds like a bird chirping.

2. In vector step 3, since the TTY caller entered 1 in vector step 2, the TTY caller is sent to vector step 8. At this point, the caller is put in queue for a TTY-enabled agent in split 47.

   Note:
   The voice caller is sent to vector step 3 also, but a voice caller does not go to vector step 8 because the caller did not enter 1 at vector step 2. Instead, voice callers continue on to vector step 4, where they connect to split 48.

3. While the TTY caller waits in queue, the caller hears silence from vector step 9, and then the announcement in vector step 10, and is then looped back to wait with silence by vector step 11.

Administering Supporting TTY Callers

This section describes the screens that you use to administer the Supporting TTY Callers feature.

Screens for administering Supporting TTY Callers

- None

Reports for Supporting TTY Callers

The following reports provide information about the Supporting TTY Callers feature:

- None

Team Button

Use the Team Button feature to monitor members of a team of stations. The Team Button feature is a standard feature starting with Communication Manager Release 4.0.

Detailed description of Team Button

A team is a virtual set of stations. Members of a team can be any station type with multiple call appearance displays and administrable feature buttons. Attendant consoles, remote stations, BRI-stations and SIP-Phones are excluded as valid stations, either as monitoring station or as monitored station.

In Communication Manager Release 5.2, the following station types are allowed as valid monitored stations, but not as monitoring stations:

- Analog stations
- BRI-stations
- SIP-telephones
- X-ports
- X-mobiles

The assignment of a team button on a station brings it automatically into the virtual team, allocating the data relation in the user records of the monitored station and the monitoring station. Deleting takes it out of the virtual team, and cancels the data relation.

The Team Button has two functions:

- Display function

  Allows any member of a team (monitoring station) to observe the station state of other team members (monitored station). The indicators depend on the type of station and could be either a green and red button LED, or as an icon on the display. In addition, the ringing of a call on a monitored station might be indicated with audible ringing on the monitoring station.

  Also, active call forwarding from the monitored station to the monitoring station and active send all calls path at the monitored station with the monitoring station as first destination in the coverage path are displayed.

  Hunt group calls can be displayed on the monitoring station if the monitored station is a member of the hunt group. Active, idle, and ringing states are displayed. Hunt group calls can also be picked up from the monitored station.

  When there is an incoming call on the monitored station, the audible ringing alert on the monitoring station with at least one active call appearance can be suppressed. See Administering audible ringing on page 1533.

  Calls from the monitoring station to monitored station, irrespective of whether they are established by pressing the team button or by dialing, are not displayed on the monitoring station.

- Execution function

  Allows the Team Button to be used as a Speed Dial Button or Pick-Up Button. Depending on the state of the monitored station, when the Team Button on the monitoring station is pushed, a call to the monitored station is established directly or a ringing call is picked from the monitored station.

  Speed dialing

  - When the monitored station is accessed from the monitoring station through speed dialing, the type of ringing on the monitored station can be configured as priority ringing or intercom ringing. See Administering Priority Ring for speed dialing on page 1534.
  - Speed dialing is treated as *enbloc* dialing (equivalent to pressing # after dialing the digits) to avoid time-outs in case of multi-location and mixed-length dial plans.
  - When the monitoring station is active on a call, pressing the team button puts the call on hold and establishes a connection to the monitored station. The call can be transferred by pressing the transfer button. On such call transfers, any active Send All Calls (SAC), Call Forwarding (CFWD), and Enhanced Call Forwarding (ECF) settings on the monitored station are overridden. However, coverage criteria are followed as set.

  Call Pickup

- If the overall call state of the monitoring station is idle, call pickup can be handled by pressing the team button on the monitoring station once and then going off hook.

  The first press of the team button displays details of the call on the monitored station. If more than one call is ringing on the monitored station, details of other calls can be viewed by clicking **Next**. When two monitoring stations press the team button of the same monitored station, call details are displayed on both the monitoring stations, but the station that first goes offhook or presses the **SPEAKER** button gets to answer the call and the display on the other monitoring station is erased.

Note:
If the overall call status of the monitoring station is any state other than idle, you need to press the team button a second time to get the call redirected and pick up the call.

- When the monitoring station is active on a call and the monitored station is ringing, pressing the team button twice will first display the extension number of the calling station and then pick the call, putting the active connection on hold, if the **Auto Hold?** system parameter feature is set to **y**.

In Communication Manager Release 5.2, the number of team buttons per station is increased to 31. However, the number of monitored stations that can be monitored by other stations is limited to a maximum of 15. In effect, the maximum number of team buttons in a system is 15, that is, each station is able to supervise and work on a maximum of 15 other stations.

The Team Button is a station oriented feature, not a call appearance oriented feature. You must consider all call appearances on a station as one call appearance of that station. The option to use the name of the monitored station name instead of its extension is available.

Audible Ringing and Call States for Team Button

A monitored station can have two call states and two ringing states. The call states and ringing states are displayed separately on the monitoring station:

The call states are:

- IDLE – All primary call appearances are in an idle state.
- BUSY – One or more call appearance have a state which is different to idle.

Note: A ringing station is considered as a station with the idle overall call state.

The busy states are as follows:

- Off-hook
- Dialing
- Calling
- Active
- Hold

- Soft hold (used for conference and transfer steps)

The overall ringing states are as follows:

- IDLE – No incoming call appearance is ringing
- RINGING – One incoming call appearance is ringing, silent ringing or audible ringing
- DOUBLE RINGING – More than one incoming call appearance is ringing, silent ringing or audible ringing.

Administering Team Button

The following steps are part of the administration process for the Team Button feature:

- Configuring the Team Button
- Viewing the status of Team Button usage
- Viewing system capacity for Team Button

Configuring the Team Button

To configure the Team Button feature for your system:

1. Type **change station *xxxx***, where ***xxxx*** is the extension of the station you want to administer.
   The system displays the Station screen.

Figure 391: .Station screen

```
change station 4002                                Page   4 of   x
                                    STATION
 SITE DATA
       Room:                                  Headset? n
       Jack:                                  Speaker? n
      Cable:                                  Mounting: d
      Floor:                                  Cord Length: 0
   Building:                                  Set Color:




ABBREVIATED DIALING
     List1:            List2:                     List3:

BUTTON ASSIGNMENTS
 1: call-appr          5: team        Ext: 4007          Rg:a
 2: call-appr          6: team        Ext: 4003          Rg:r
 3: call-appr          7: team        Ext: 4012          Rg:n
 4:                    8: team        Ext: 4011          Rg:d
```

2. Page down till you see the Button Assignments area. Enter team and required extension numbers in the extension fields.
3. In the **Rg** field, enter the audible ringing type that you want to set for each extension. (Audible Ringing types are discussed in the Audible Ringing and Call States for Team Button on page 1529.) You can use the help index.

Viewing the status of Team Button usage

To view the status of team button usage:

1. Type **`list usage extension xxxx`**, where ***xxxx*** is the extension.

   The system displays the List Usage Report screen.

Figure 392: List Usage Report screen

```
list usage extension 4003

                              LIST USAGE REPORT

Used By
Hunt Group            Group Number         1                Member 1
Team Button Assigned in Station            4002             Button 4
Team Button Assigned in Station            4007             Button 6
Team Button Assigned in Station            4013             Button 258
Terminating Ext Grp   Group Number         1                Member 1
Station               Station Extension    4003            Emrgncy Loc Ext
```

2. Page down till you see the fields for **Team Button Assigned in Station**. You can view the extension numbers and button assignments for each extension on this page.

Viewing system capacity for Team Button

To view system capacity for the Team Button feature:

1. Type **display capacity**.

   The system displays the System Capacity screen.

Figure 393: System Capacity screen

```
display capacity                                          Page   8 of  x
                                SYSTEM CAPACITY

                                                                   System
                  VOICE TERMINALS                  Used Available  Limit
                                                   ----------------------
                     Station Button Memory (units):    0 %   100 %  23256000
                  Team button / Monitored stations:      9    5991      6000
                          Customized Button Labels:    0 %   100 %    100000
                                   Station Records:     24   35976    36000
           Station Records Used By TTI(Not Shared):     41
               Station Records Used By TTI(Shared):      0
                  Stations (includes BRI stations):     24     -        -
                                Stations With Port:     24
                             Stations Without Port:      0
                                    Other Stations:      0     -        -
                                         TTI Ports:     53     -        -
                                Auto Moves Stations:      0    5000     5000
                          Administered IP SoftPhones:     0     -        -
                         Video Capable H.323 Stations:    0       0        0
                          Video Capable IP Softphones:    0       0        0
                    ISDN BRI Endpoint And Trunk Ports:    20    6980     7000
```

2. Page down till you see the **Team button/Monitored Stations** field. You can view the used, available and system limit for Team Buttons for your system.

Administering audible ringing

1. Type **change cor**. Press **Enter**.

   The system displays the **Class of Restriction** screen. See Figure 394.

2. Click **Next** till you see the **Team Btn** fields.

Figure 394: Class of Restriction screen

```
change cor 1                                                  Page   3 of  23
                              CLASS OF RESTRICTION

               SAC/CF Override by   Team Btn? n  Priority Call? n  Dialing? n
   SAC/CF Override Protection for   Team Btn? n  Priority Call? n  Dialing? n



                           one-X Server Access? y
Team Btn  Silent if Active? n  Priority Ring? n
Team Btn  Display Name? n      Pick Up by Going Off Hook? n
```

3. To disable audible ringing on the monitoring station, set **Team Btn Silent if Active?** to **y**.
4. Press **Enter** to save your changes.

Note:
Use **`display cor`** SAT command to view the settings.

Administering Priority Ring for speed dialing

1. Type **`change cor`**. Press **`Enter`**.

   The system displays the **Class of Restriction** screen. See Figure 394.
2. Click **Next** till you see the **Team Btn** fields.
3. To enable priority ringing, set **Priority Ring?** to **y**.
4. Press **Enter** to save your changes.

Administering display of station name

1. Type **`change cor`**. Press **`Enter`**.

   The system displays the **Class of Restriction** screen. See Figure 394.
2. Click **Next** till you see the **Team Btn** fields.
3. To enable display of monitored station name instead of the number, set **Team Btn Display Name?** to **y**.

4. Press **Enter** to save your changes.

Administering Call Pickup by going off hook

1. Type **change cor**. Press **Enter**.

   The system displays the **Class of Restriction** screen. See Figure 394.
2. Click **Next** till you see the **Team Btn** fields.
3. To enable pick up of a call by going off-hook, set the **Pick Up by Going Off Hook?** to **y**.
4. Press **Enter** to save your changes.

Team Button Override Send All Calls/Call Forward

In Communication Manager Release 5.1, the Team Button feature allows you to use its speed dial function, to override a rerouting caused by active Send All Calls (SAC), Call Forwarding (CFWD) all, or Enhanced Call Forward (ECF) unconditional.

When the team button is pressed on the monitoring station and the monitored station has a direct rerouting active (SAC, CFWD all, ECF unconditional), the call may do any of the following, depending upon administration:

- Be rerouted
- Ring the monitored station
- Display a message asking the caller which of (1) or (2) to do

Dialing the number of the team member is handled by pressing a team button.

The monitored station with active rerouting is able to disallow overriding in general.

The monitoring station must be a member in a class in which overriding of SAC/CFWD is allowed.

The functionality is controlled by:

- COR settings (Figure 395: COR Settings)
  - monitoring station: **SAC/CR Override by Team Btn**
  - monitored station: **SAC/CF Override Protection for Team Btn**
- Setting on monitoring station form (Figure 396: Station Form)
  - **SAC/CF override** [a(sk), n(o), y(es)]

Figure 395: COR Settings

```
change cor 1                                                          Page 3 of x

                            CLASS OF RESTRICTION

               SAC/CF Override by    Team Btn? n
   SAC/CF Override Protection for    Team Btn? n
   Display Names on Bridged Appearance Labels? n
            Remove Caller Id from Set display? n
```

Figure 396: Station Form

```
change station 27001                                          Page   3 of   x
                                    STATION

          Conf/Trans on Primary Appearance? n
Bridged Appearance Origination Restriction? n


       Call Appearance Display Format: disp-param-default
IP Phone Group ID:

                              ENHANCED CALL FORWARDING
                                    Forwarded Destination         Active
 Unconditional For Internal Calls To:                                n
                   External Calls To:                                n
          Busy For Internal Calls To:                                n
                   External Calls To:                                n
      No Reply For Internal Calls To:                                n
                   External Calls To:                                n

            SAC/CF Override: n
```

The settings on the station form of the monitoring station are:

- **n(o)** – cannot override rerouting. The station does not have the ability to override rerouting.
- **y(es)** – can override rerouting. The station has the ability to override the rerouting the monitored station has set, as long as one incoming call appearance is free. If no free call appearance is available, the call fails and the user of the monitoring station hears busy tone.

- **a(sk)** – ask whether the user wants to follow the rerouting or override it. When the user of the station can decide whether rerouting should take place or not, a message is sent to the station which displays the active rerouting and the number of the forwarded station. The user of the monitoring station can now follow the rerouting by dialing "1" or "#", or by letting the timer which supervises the team button pushes expire, or overriding the active rerouting by dialing "0" or "*".

No Overriding of SAC/CFWD

COR of monitoring station: SAC/CF Override by Team Btn	COR of monitored station: SAC/CF Override Protection for Team Btn	Monitoring station form: SAC/CF override
no	no / yes	ask / no / yes
yes	yes	ask / no / yes
yes	no	no

Using speed dialing by pressing the team button on the monitoring station doesn't establish a call to the monitored station (with active SAV, CFWD all, or ECF unconditional), but follows the assigned active rerouting.

Unconditional Overriding of SAC/CFWD

COR of monitoring station: SAC/CF Override by Team Btn	COR of monitored station: SAC/CF Override Protection for Team Btn	Monitoring station form: SAC/CF Override
yes	no	yes

Using speed dialing by pressing the team button on the monitoring station establishes a call to the monitored station (with active SAC, CFWD all, or ECF unconditional) instead of following the active rerouting.

If the monitored station does not answer the call within 30 seconds, the call is rerouted to the assigned rerouting destination.

Overriding of SAC/CFWD by Asking

COR of monitoring station: SAC/CF Override by Team Btn	COR of monitored station: SAC/CF Override Protection for Team Btn	Monitoring station form: SAC/CF Override
yes	no	ask

Using speed dialing by pressing the team button on the monitoring station neither establishes a call to the monitored station (with active SAC, CFWD all, or ECF unconditional) nor reroutes the call to the assigned rerouting destination.

Instead, a message is displayed on the station which shows the rerouting destination and asks the user of the station if the user wants to follow the rerouting or override it.

Dialing digits or pressing any other button by the user of the station leads to a result as follows:

- Dialing 1 or #: rerouting
- Dialing 0 or *: overriding of rerouting
- No action within 9 seconds: rerouting
- Exit button: rerouting
- Drop button: end of call establishment
- Almost any other digit or button press: no reaction and timer (9 seconds) is restarted

If rerouting is overridden and the monitored station does not answer the call within 30 seconds, the call is rerouted to the assigned rerouting destination.

Telephone Display

Use the Telephone Display feature to provide users of multiappearance telephone with current call and message information. The information that appears depends on the type of display that the user selects with the buttons on the telephone.

Users can use the features of the telephone to retrieve stored information, such as messages and directory information. You can select English, French, Italian, Spanish, user-defined, or Unicode languages to display the messages or the information.

Detailed description of Telephone Display

This section provides a detailed description of the Telephone Display feature.

Users can use the features of the telephone to retrieve stored information, such as messages and directory information. You can select English, French, Italian, Spanish, user-defined, or Unicode languages to display the messages or the information.

With Enhanced telephone display, you can choose the types of characters that appear on the telephone display of the user. You can administer the software to display Roman (European) characters, or Cyrillic (Russian), Katakana (Japanese), or Ukrainian characters. The type of telephones that your company uses determine the character sets that you can display.

Telephone Display supports the following capabilities:

- Button display modes
- Call-related information display
- Message retrieval
- Feature information displays
- Unicode "Native Name" support
- Enhanced telephone display

Button display modes

You can assign several display modes to telephone buttons. To access these modes, users press the assigned button on the telephone. All the buttons are administrable.

Button mode	Function
Normal	Displays call-related information for the active call appearance. This information includes call appearance, and the name and the number of the calling party or the called party, depending on the type of call. Can also displays elapsed time when the display is in normal mode. The system shows the elapsed time in hours, minutes, and seconds. Timing starts and stops when the button is pressed.
Inspect	Displays call-related information for an incoming call when the user is active on a different call appearance. Users must reset the mode manually for each call.
Stored Number	Displays one of the following numbers: ● The last number that the user dialed (Last Number Dialed) ● The number that is stored in an Abbreviated Dialing button that is administered to the telephone ● A number that is stored in an Abbreviated Dialing list ● A number that is assigned to a button that is administered by Facility Busy Indication
Date and Time	The current date and time of day.
Integrated Directory	Turns off the touchtone signals and allows the user to use the touchtone buttons to enter the name of a system user. After the user enters a name, the display shows the name and the extension. Integrated Directory can use one additional related button: ● Call-Disp automatically returns the call that is requested by the currently displayed message or the currently displayed name and extension. Note, if the name was entered with tildes as the first two characters the name will be hidden (when Display Character Set = roman) and is not sent to a telephone with any integrated directory search.

Button mode	Function
Message Retrieval	Retrieves messages for telephone users. If no messages are stored, the display shows `NO MESSAGES`. Users can retrieve messages even if the retriever is active on a call. Message Retrieval can use 3 additional related buttons: • Next Message retrieves the next message, or displays **End of File, Push Next To Repeat** when in Retrieval mode. • Call-Disp automatically returns the call that is requested by the currently displayed message or the currently displayed name and extension. • Delete deletes the currently displayed message.
Coverage Message Retrieval Mode	Retrieves messages for users of the telephone users who do not have a display module. You must administer retrieval permission for a user to retrieve messages of other users. The user does not need to lift the handset to retrieve messages. The user can retrieve messages even if the retriever is active on a call. Coverage Message Retrieval can use three additional related buttons: • Next Message retrieves the next message, or displays **End of File, Push Next To Repeat** when in Retrieval mode. • Call-Disp automatically returns the call that is requested by the currently displayed message or the currently displayed name and extension. • Delete deletes the currently displayed message.

Enhancements for Communication Manager 4.0

Communication Manager 4.0 enhanced the Integrated Directory feature. Another enhancement is the ability to search on names using Cyrillic characters (Display Character Set = Cyrillic or Ukrainian).

Integrated Directory:

The Integrated Directory feature allows users to retrieve a party's extension number by keying in the name of the desired party on the touch-tone pad. Once the desired party is found, a call can be placed to that party by simply pressing the CALL button. The Integrated Directory is a Personal-Service Display Mode, adding to the list of Message-Retrieval, Coverage-Message-Retrieval, Stored-Number, and Date/Time modes. This Integrated Directory feature now provides the ability to look up names with international characters (Latin letter with a diacritic) when Display Character Set = Roman.

Integrated Directory Data Base:

Station users' names are entered from the System Administration Terminal. If you want the station user name to be hidden from the Integrated Directory feature, the name should be entered with '~~' as the first two characters of the name. Names entered in this way are not added to the Integrated Directory Database. The Integrated Directory feature only retrieves names that are in the Integrated Directory Database.

INTEGRATED DIRECTORY Mode Button:

An INTEGRATED DIRECTORY mode button is provided to activate the Integrated Directory service.

The Integrated Directory feature allows you to do the following changes:

- The ability to hide names (Display Character Set = Roman) can only be accomplished if the name begins with two tildes. Before Communication Manager 4.0, other symbols might have been used to hide names. This is no longer supported. If your site was using a symbol other then the tilde to hide names, the recommended upgrade procedure is to export such names to a CSV file. You must do a global change on the symbol you used replacing such symbol with two tildes. After making the change, import the data back to your Communication Manager server.
- Before Communication Manager 4.0, the asterisk was used as a wild card to skip the comma in Integrated Directory names such as "Doe, John." The comma is now supported on button 1 and so the one key should be pressed rather then the asterisk key when you want to move past the comma in any Integrated Directory name.

When the **Display Character Set** field on the System-Parameters Country-Options screen is set to Cyrillic or Ukrainian:

- Names are stored in a Roman or a Cyrillic integrated directory.
  If a name includes a tilde (~) the name is stored only in the Cyrillic integrated directory. If not, the name is stored in the Roman integrated directory.
- The integrated directory searched is determined by the value (Roman or Cyrillic) in the **Directory Search Sort Order** of the System-Parameters Country-Options screen.
- While in the integrated directory feature, Communication Manager interprets # key as an instruction to switch the Directory Search Sort Order to the non-administered value when the # key is pressed before any other dialpad keys: 1,2,3,4,5,6,7,8,9,*,0. The # key is ignored if it is not the first dialpad key pressed.
  This switch to the non-administered value only stays in effect during the current integrated directory feature session. So the next invocation of the integrated directory feature uses the administered value.

Table 87 shows the characters assigned to Dial Pad Keys when Display Character Set = Roman.

Table 87: Dial Pad International Character Assignment

Key	Characters Assigned
0	0 *space*
1	, . @ 1
2	a A á Á à À ă Ă â Â å Å ä Ä ã Ã ą Ą æ Æ b B c C ć Ć č Č ç Ç 2
3	d D Ď ð Đ e E é É è È ě Ě ê Ê ë Ë ė Ė ę Ę f F 3
4	g G ğ Ğ h H i I í Í ì Ì î Î ï Ï 4
5	j J k K l L ł Ł 5
6	m M n N ń Ń ň Ň ñ Ñ o O ó Ó ò Ò ô Ô ö Ö ő Ő õ Õ ø Ø 6
7	p P q Q r R ř Ř s S ś Ś š Š ş Ş ß 7
8	t T Ť Ţ u U ú Ú ù Ù û Û ů Ů ü Ü ű Ű v V 8
9	w W x X y Y ý Ý ÿ Ÿ z Z ź Ź ž Ž ż Ż Þ þ 9
*	´ ‘ - ! “ # $ % & ( ) * + / : ; < = > ? [\ ] ^ _ ` { | }

Table 88 shows the Dial Pad keys when Display Character Set = Cyrillic or Ukrainian.

Table 88: Dial Pad Cyrillic Character Assignment

Key	Character
0	0 *space*
1	, . @ 1
2	a A Б b B Г 2
3	Ä e E ¨ ª Æ Ç 3
4	È i I ¯ É k K Ë 4
5	m M h H o O П 5
6	p P c C t T y Y 6
7	Ô x X Ö × 7
8	Ø Ù Ú Û 8

Table 88: Dial Pad Cyrillic Character Assignment

Key	Character
9	Ü Ý Þ ß 9
*	‘ - ! “ # $ % & ( ) * + / : ; < = > ? [\ ] ^ _ ` { | }

For more information on character mapping for the 9600 IP telephones, see *Character Mapping and Text Entry on 9600 IP Telephones*, Issue 1, 16-601991.

Call-related information display

The software provides the following call-related information:

- Call appearance identification

  A lowercase letter is used to designate call appearance buttons on the display. The display shows **a=** for an incoming call on the first button, **b=** for an incoming call on the second button, and so on.

  The system might omit the call-appearance information so that the Call Log find capability in the **PC**/**PBX** Connection software works properly.

Note:

The displays of IP phones and call logs show whether calls were answered through call pickup from another station, and if the Temporary Bridged Appearance feature is in use. This does not apply to pickup through the Team button.

- Calling party identification

  When a call is from inside the system, the display shows the name of the caller or a unique identification that is administered for the telephone being used, and the extension of the calling party. When the call is from outside the system, the display shows the trunk group name (such as **CHICAGO**) and the Trunk Access Code (TAC) that is assigned to the trunk group used for the call. If a user is active on a call and receives another call, the display automatically shows the identification of the second caller for a few seconds. The system then automatically restores the display to show the information that is associated with the active call appearance.

  For example:

  outgoing trunk call

  ```
  b=87843541
  ```

  8 is the TAC, and 784-3541 is the number that was dialed

  then

  ```
  b=OUTSIDE CALL                  8
  ```

  or

  ```
  b=WATS               101
  ```

Note:
Because of space limitations, some name displays are shortened to 15 characters. These displays include displays for transferred or covered calls, non-DCS, ISDN-PRI calls, VDN service observing displays, LWC messages, or the queue status of an agent.

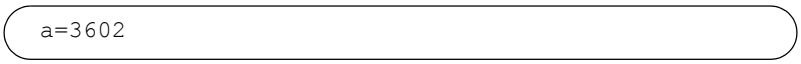
- Called party identification

  On calls to a system user, the digits appear on the display as the digits are dialed. After dialing is complete, the name and the extension of the called party appears. If no name is accessed, the dialed digits remain on the display.

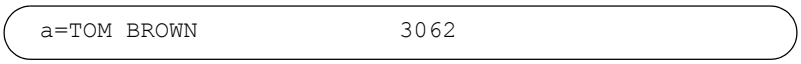
  On outgoing calls, the digits appear on the display as the digits are dialed. After dialing is complete, the display shows the name and the TAC that is assigned to the trunk group being called. Optionally on a trunk-group basis, the display can show only the dialed digits, not the trunk group name and the TAC.

  For example:

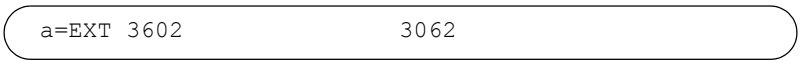
  Dialed digits

  then:

  or, if no name is available:

- Call purpose

  Call purpose identifies the reason for an incoming call or a redirected call. The system does not identify a call purpose for a normal incoming call. The following identifiers sometimes appear on the display:

Display	Meaning
b - (Busy)	The called user is active on a call, and has a temporary bridged appearance of the call.
c - (Cover All)	The called user has Cover All assigned.
callback	The call is an Automatic Callback call from the system.
d - (Coverage on Don’t Answer)	The call was redirected because the called telephone unanswered. This message also indicates that the called user has a temporary bridged appearance of the call.
f - (Call Forwarding)	Another user has forwarded calls to this telephone.
h - (Station hunt)	The called user is active on a call, and station hunt was used to route the call.
ICOM	The call is an Intercom call.

Display	Meaning
p - (Pickup)	The user answered the call of a Call Pickup group member.
park	The user parked a call.
priority	The call has priority status.
s - (Send All Calls)	The called user is temporarily sending all calls to coverage and the call was redirected to this telephone.

Message retrieval

You can designate certain telephones and attendant groups for system-wide message retrieval. Users of these telephones or consoles can retrieve Leave Word Calling (LWC) and call coverage messages for other telephone users. These other users can include Direct Department Calling (DDC) groups, Uniform Call Distribution (UCD) groups, and Terminating Extension Groups (TEGs). Users of these telephones or consoles can also retrieve external call logs. You can assign system-wide retrieving telephones or consoles. Use the Feature-Related System Parameters screen to make these assignments.

Messages for a telephone user can be retrieved at selected telephones, or any attendant console. However, the retriever must be on the call coverage path of the user, and permission to retrieve messages must be assigned for the telephone of the user.

Feature information displays

Telephone displays provide information about the activity on individual telephones and consoles, including confirmation that a certain feature is being used. You administer the language to use for messages on the Station screen for each telephone.

Note:

As of July 1, 2005, new messages are no longer added to the Language Translations screens, so these screens may not show all available Communication Manager messages. As a preferred method for entering translations for user-defined phone messages, Avaya recommends using the Avaya Message Editing Tool (AMET). This tool is available for download from http://www.avaya.com.

Unicode "Native Name" support

Communication Manager supports Unicode for the "Name" associated with Vector Directory Numbers (VDNs), trunk groups, hunt groups, and stations. The **Unicode Name** (also referred to as *Native Name* and *Name 2)* fields are hidden fields that are associated with the name fields you administer on the respective screens for each. These fields can only be administered using Avaya Site Administration (ASA) or MultiSite Administrator (MSA).

- The Unicode VDN Name is associated with the name administered in the **Name** field on the Vector Directory screen. You must use MSA.
- The Unicode Trunk Group Name is associated with the name administered in the **Group Name** field on the Trunk Group screen. You must use MSA.
- The Unicode Hunt Group Name is associated with the name administered in the **Group Name** field on the Hunt Group screen. You must use MSA.
- The Unicode Station Name is associated with the name administered in the **Name** field on the Station screen. You must use ASA or MSA.

Note:

Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.). To display time in 24-hour format and display messages in English, set the **Display Language** field to "unicode." When you enter "unicode," the station displays time in 24-hour format, and if no Unicode file is installed, displays messages in English by default. For more information on Unicode, see Administering Unicode display in *Administering Avaya Aura™ Communication Manager*, 03-300509.

Enhanced telephone display

With enhanced telephone display, you can choose the types of characters that appear on your telephone displays. You can choose standard Roman characters, or Cyrillic, Katakana, or Ukrainian characters. Your Avaya representative sets the character type on the System Parameters Country-Options screen. The character set that you can display also depends on the telephones that your company uses.

You can choose one of the following character sets for messages on your display telephones:

- Cyrillic contains the characters that are required to display the Russian language. All Russian characters appear in uppercase letters.
- Katakana contains the characters that are required to display the Japanese language, and as some European characters and other symbols. All Japanese characters appear in uppercase letters.
- Roman contains two character sets:

  - US English contains the Roman alphabet, and the numerals and the special characters that are standard on the US English keyboard. US English characters appear in uppercase and lowercase letters.
  - European contains characters for many European languages. All European characters appear in uppercase letters.
- Ukrainian contains the characters that are required to display the Ukrainian language. All Ukrainian characters appear in uppercase letters.

The type of telephones that your company uses must support the characters that you want to display. Each character set requires specific firmware in the telephone. Ensure that you use telephones with the same firmware type across your entire system. If you do not use telephones with the same firmware type across your entire system, the displays do not appear as expected. Your Avaya representative can ensure that you have the correct telephone types for the characters that you want to display.

This section shows the English, the French, Italian, and Spanish message for each feature. When time is displayed, the English language uses the abbreviations AM and PM. All other languages use 24-hour time.

Table 89: Telephone features

English	French	Italian	Spanish
AUTO WAKEUP - Ext: xxxxx Time: --:-- xM	REVEIL AUTO. - POSTE: xxxxx HEURE: --:--	SERVIZIO SVEGLIA - Tel: xxxxx Ora: --:--	DESPERT AUTOMA - EXT: xxxxx HORA: --:--
INVALID EXTENSION - TRY AGAIN	NUMERO DE POSTE EST ERRONE - REESSAYER	NUMERO ERRATO - RIPETERE	EXTENSION NO VALIDO - INTENTE DE NUEVO
WAKEUP ENTRY DENIED - INTERVAL FULL	DEM. REVEIL REFUSEE - INTERVALLE PLEIN	SVEGLIA NON ATTIVATA - ORARIO OCCUP	ENTRADA DENEGADA - INTERVALO COMPLETO
WAKEUP ENTRY DENIED - NO PERMISSION	DEM. REVEIL REFUSEE - SANS AUTORISATION	SVEGLIA NON ATTIVATA - NON PERMESSO	ENTRADA DENEGADA - SIN PERMISO
WAKEUP ENTRY DENIED - SYSTEM FULL	DEM. REVEIL REFUSEE - ENCOMBREMENT	SVEGLIA NON ATTIVATA - CONGESTIONE	ENTRADA DENEGADA - SISTEMA COMPLETO
WAKEUP ENTRY DENIED - TOO SOON	DEM. REVEIL REFUSEE - TROP TOT	SVEGLIA NON ATTIVATA - TROPPO PRESTO	ENTRADA DENEGADA - MUY PRONTO
WAKEUP REQUEST CANCELED	DEMANDE DE REVEIL EST ANNULEE	RICHIESTA SVEGLIA CANENTRYATA	SOLICITUD DE DESPERTADOR CANCELADA

1 of 2

Table 89: Telephone features (continued)

English	French	Italian	Spanish
WAKEUP REQUEST CONFIRMED	DEMANDE DE REVEIL EST CONFIRMEE	RICHIESTA SVEGLIA CONFERMATA	SOLICITUD DE DESPERTADOR CONFIRMADA
WAKEUP CALL	APPEL DE REVEIL	SERV. SVEGLIA	DESPIERTE
			2 of 2

Table 90: ASAI displays

English	French	Italian	Spanish
YOU HAVE ADJUNCT MESSAGES	MESSAGES SUPPLEMENTAIRES	MESSAGGI AGGIUNTIVI	TIENE MENSAJES ADICIONALES

Table 91: Busy verification of terminals and trunks

English	French	Italian	Spanish
ALL MADE BUSY	TOUS OCC.	TUTTI OCCUPATI	TODAS OCUPADAS
BRIDGED	EN DERIVATION	OCCUPATO	PUENTEADA
DENIED	INTERDIT	NON PERMESSO	DENEGADO
INVALID	ERRONE	NON VALIDO	NO VALIDO
NO MEMBER	AUCUN MEMBRE	NESSUN ELEMENTO	NINGUN MIEMBRO
OUT OF SERVICE	HORS SERVICE	FUORI SERVIZIO	FUERA SERVICIO
RESTRICTED	RESTREINT	RISTRETTO	RESTRINGIDO
TERMINATED	TERMINE	TERMINATO	TERMINADO
TRUNK SEIZED	CIRCUIT SAISI	GIUNZIONE IMP.	ENLACE OCUPADO
VERIFIED	VERIFIE	VERIFICATO	VERIFICADO

Call Appearance

For each language, the active call appearance appears as:

"a =" (English)

Call-appearance buttons are shown on the display by a lower-case letter (a through z for the first 26 call appearances), followed by "=." Lowercase letters A through Z, followed by "=" are used for additional call appearances.

Table 92: Call Detail Recording

English	French	Italian	Spanish
CDR OVERLOAD	SURCHARGE EDA	SVRACCARICO DAC	SOBRECARGA DAT

Table 93: Call progress feedback displays

English	French	Italian	Spanish
busy (Extension Busy, Intrusion Not Allowed, Call Waiting Not Allowed)	OCCUPE (Occupe)	occ (Occupato)	OCUPADA (Ocupada)
busy(I) (Extension Busy, Intrusion Allowed, Call Waiting Not Allowed)	OCC.(E) (Entree ligne occupe)	occ(I) (Occupato- Intrusione)	OCUP(I) (Ocupada- intrusion)
ringing (Extension Ringing)	SONNE (Libre)	libero (Libero)	LIBRE (Libero)
wait (Extension Busy, Intrusion Not Allowed, Call Waiting Allowed)	ATTENTE (Attente)	auat (Autoattesa)	ESPERA (Espera)
(I) wait (Extension Busy, Intrusion Allowed, Call Waiting Allowed)	(E) ATTENTE (Entree ligne attente)	(I) auat (Intrusione- Autoattesa)	(I) ESPERA (Intrusion, en espera)

Table 94: Class of Restriction (COR) displays

Restriction	English	French	Italian	Spanish
Toll	TOLL	INT.	TASS	TARF
Full	FULL	COM.	DISB	LLEN
No Restrictions	NONE	AUC.	ABIL	NING
Origination	ORIG	DEP.	ORIG	ORIG
Outward	OTWD	SOR.	USCN	SALI

Use the following screens to translate time messages, if appropriate.

Figure 397: Date/Time Mode and Formats - English

```
<DATE/TIME>     <TIME><b><b><DATE>
   <TIME>          <HR>:<MIN><b><M>
   <HR>            1-12 (hour of day, no leading zeroes)
   <MIN>           00-59 (minute of hour)
   <M>             "am" or "pm"
   <DATE>          <DOW><b><MONTH><b><DOM>,<b><YEAR>
   <DOW>           Day of week, upper case, unabbreviated
   <MONTH>         Month of year, upper case, unabbreviated
   <DOM>           1-31 (day of month, no leading zeroes)
   <YEAR>          Year in 4 digits
   <b>             Blank
```

Figure 398: Date/Time Mode and formats - French, Italian, Spanish, and User-Defined

```
<DATE/TIME>     <TIME><b><b><DATE>
   <TIME>          <HR>:<MIN>
   <HR>            0-23 (hour of day, no leading zeroes)
   <MIN>           00-59 (minute of hour)
   <DATE>          <DOW><b><DOM><b><MONTH>,<b><YEAR>
   <DOW>           Day of week, upper case, unabbreviated
   <DOM>           1-31 (day of month, no leading zeroes)
   <MONTH>         Month of year, upper case, unabbreviated
   <YEAR>          Year in 4 digits
   <b>             Blank
```

Table 95: Days of the week format

English	French	Italian	Spanish
SUNDAY	DIMANCHE	DOMENICA	DOMINGO
MONDAY	LUNDI	LUNEDI	LUNES
TUESDAY	MARDI	MARTEDI	MARTES
WEDNESDAY	MERCREDI	MERCOLEDI	MIERCOLES
THURSDAY	JEUDI	GIOVEDI	JUEVES
FRIDAY	VENDREDI	VENERDI	VIERNES
SATURDAY	SAMEDI	SABATO	SABADO

Table 96: Date and Time mode - time not available

English	French	Italian	Spanish
SORRY, TIME UNAVAILABLE NOW	HEURE ET DATE INDISPONIBLES	ORA E DATA TEMPON DISPONIBILI	HORA Y FECHA NO DISPONIBLES AHORA

Table 97: Months of the year format

English	French	Italian	Spanish
JANUARY	JANVIER	GENNAIO	ENERO
FEBRUARY	FEVRIER	FEBBRAIO	FEBRERO
MARCH	MARS	MARZO	MARZO
APRIL	AVRIL	APRILE	ABRIL
MAY	MAI	MAGGIO	MAYO
JUNE	JUIN	GIUGNO	JUNIO
JULY	JUILLET	LUGLIO	JULIO
AUGUST	AOUT	AGOSTO	AGOSTO
SEPTEMBER	SEPTEMBRE	SETTEMBRE	SEPTIEMBRE
OCTOBER	OCTOBRE	OTTOBRE	OCTUBRE
NOVEMBER	NOVEMBRE	NOVEMBRE	NOVIEMBRE
DECEMBER	DECEMBRE	DICEMBRE	DICIEMBRE

Table 98: Do Not Disturb (Hotel/Motel feature)

English	French	Italian	Spanish
DO NOT DIST - Group: xx Time: --:-- xM	NE PAS DERANGER GROUPE: xx HEURE: --:--	NON DISTURBARE - Grp: xx Ora: --:--	NO MOLESTAR - GRUPO: xx HORA: --:--
DO NOT DIST - Ext: xxxxx Time: --:-- xM	NE PAS DERANGER POSTE:xxxxx HEURE: --:--	NON DISTURBARE - Tel: xxxxx Ora: --:--	NO MOLESTAR - EXT: xxxxx HORA: --:--
DO NOT DIST ENTRY DENIED - INTERVAL FULL	DEMANDE EST REFUSEE - INTERVALLE PLEIN	SERVIZIO NON ATTIVATO - ORARIO OCCUP	ENTRADA DENEGADA - INTERVALO COMPLETO
DO NOT DIST ENTRY DENIED - NO PERMISSION	DEMANDE EST REFUSEE - SANS AUTORISATION	SERVIZIO NON ATTIVATO - NON PERMESSO	ENTRADA DENEGADA - SIN PERMISO

1 of 2

Table 98: Do Not Disturb (Hotel/Motel feature) (continued)

English	French	Italian	Spanish
DO NOT DIST ENTRY DENIED - SYSTEM FULL	DEMANDE EST REFUSEE - ENCOMBREMENT	SERVIZIO NON ATTIVATO - CONGESTIONE	ENTRADA DENEGADA - SISTEMA COMPLETO
DO NOT DIST ENTRY DENIED - TOO SOON	DEMANDE EST REFUSEE - TROP TOT	SERVIZIO NON ATTIVATO - TROPPO PRESTO	ENTRADA DENEGADA - MUY PRONTO
INVALID GROUP - TRY AGAIN	GROUPE ERRONE - REESSAYER	GRUPPO NON VALIDO - RIPETERE	GRUPO NO VALIDO - INTENTE DE NUEVO
THANK YOU - DO NOT DIST ENTRY CONFIRMED	MERCI - DEMANDE EST CONFIRMEE	NON DISTURBARE - RICHIESTA CONFERMATA	NO MOLESTAR - ENTRADA CONFIRMADA
THANK YOU - DO NOT DIST REQUEST CANCELED	MERCI - DEMANDE EST ANNULEE	NON DISTURBARE - RICHIESTA CANENTRYATA	MUCHAS GRACIAS - SOLICITUD CANCELADA

2 of 2

Enhanced Abbreviated Dialing - user defined

Figure 399: Language Translations screen

```
display display-messages ad-programming                          Page 1 of 1
                          Language Translations

     English

 1. Press button to program.          1. ************************************
 2. Change number?                    2. ********************
 3. Yes=1 No=2                        3. **************
 4. Enter number:                     4. ************************************
 5. Press # to save.                  5. **************
 6. Number saved.                     6. ************************************
 7. Change label?                     7. ********************
 8. Enter label:                      8. ************************************
 9. Press  * to advance; # to save.   9. ****************************
10. Press  * to reenter; # to save.  10. ****************************
11. Label saved.                     11. ************************************
```

Table 99: Field separator

English	French	Italian	Spanish
<calling party> "to" <called party>	<calling party> "a" <called party>	<calling party> "a" <called party>	<calling party> "a" <called party>

English	French	Italian	Spanish
DIRECTORY - PLEASE ENTER NAME	ANNUAIRE - ENTRER LE NOM	ELENCO UTENTI - INTRODURRE NOME	GUIA TELEFONICA - INTRODUZCA NOMBRE
DIRECTORY UNAVAILABLE - TRY LATER	ANNUAIRE INDISPONIBLE - REESSAYER	ELENCO UTENTI TEMP. NON DISPONIBILE	GUIA TEL INDISPONIBLE - INTENTE DESPUES
NO MATCH - TRY AGAIN	INTROUVABLE - REESSAYER	NESSUNA CORRISPONDENZA - RIPETERE	NO CORRESPONDE - INTENTE DE NUEVO

Table 100: ISDN

English	French	Italian	Spanish
ANSWERED BY	REPONDU PAR	RISPOSTA DA	RESPONDIDO POR

Table 100: ISDN

English	French	Italian	Spanish
CALL FROM	APPEL DE	CHIAMATA DA	LLAMADA DE
INTL	INTL	INTL	INTL

Leave Word Calling

Figure 400: Leave Word Calling Formats - English

```
<CALLER_ID><b><DATE><b><TIME><M><b><C><b>CALL<EXT_NO>

   <CALLER_ID>     The calling identifier, up to 15 characters
   <DATE>          <MONTH>/<DOM>
   <MONTH>         1-12 (month of year, no leading zeroes)
   <DOM>           1-31 (day of month, no leading zeroes)
   <TIME>          <HR>:<MIN>
   <HR>            1-12 (hour of day, no leading zeroes)
   <MIN>           00-59 (minute of hour)
   <M>             "a" or "p"
   <C>             Number of calls received, 1 digit *
   <EXT_NO>        Calling extension number, up to 7 digits
   <b>             blank
```

Figure 401: Leave Word Calling Formats - French, Italian, Spanish, and User-Defined

```
<CALLER_ID><b><DATE><b><TIME><b><C><b>APPL<b><EXT_NO>

   <CALLER_ID>     The calling identifier, up to 15 characters
  <DATE>          <DOM>/<MONTH>
   <DOM>           1-31 (day of month, no leading zeroes)
   <MONTH>         1-12 (month of year, no leading zeroes)
   <TIME>          <HR>:<MIN>
   <HR>            0-23 (hour of day, no leading zeroes)
   <MIN>           00-59 (minute of hour)
   <C>             Number of calls received, 1 digit *
   <EXT_NO>        Calling extension number, up to 5 digits
```

Table 101: Leave Word Calling messages

English	French	Italian	Spanish
CANNOT BE DELETED - CALL MESSAGE CENTER	NE PEUT ETRE SUPP./ APPELER RECEP. MESS.	NON CANENTRYATO. CHIAMARE CENTRO MESSAGGI	NO ELIMINADO-LLAMA CENTRO DE MENSAJES
DELETED	SUPPRIME	MESSAGGIO CANENTRYATO	ELIMINADO
END OF MESSAGES (NEXT TO REPEAT)	FIN DES MESSAGES (SUIVANT POUR REPETER)	FINE MESSAGGI. <successivo> PER RIPETERE	FIN DE MENSAJES (SIGUIENTE PARA REPITIR)
GET DIAL TONE, PUSH Cover Msg Retrieval	TONALITE D'ENVOI - <LECT. MESS. COUV.>	<rec mess copert> DOPO IL TONO DI CENTR	OBTENGA TONO OPRIMA <RECUP MNSJE COBERT>
IN PROGRESS	EN COURS	ATTENDERE...	EN CURSO
MESSAGE RETRIEVAL DENIED	LECTURE DE MESSAGES INTERDITE	LETTURA MESSAGGIO NON PERMESSA	RECUPERACION DE MENSAJES DENEGADA
MESSAGE RETRIEVAL LOCKED	LECTURE DE MESSAGES BLOQUEE	LETTURA MESSAGGIO BLOCCATA	RECUPERACION DE MENSAJES BLOQUEADA
MESSAGES FOR	MESSAGES POUR	MESSAGGI PER	MENSAJES PARA
MESSAGES UNAVAILABLE - TRY LATER	MESSAGES INDISPONIBLES - REESSAYER	MESSAGGI TEMPORANEAMENTE NON DISPONIBILI	MENSAJES NO DISPONIBLES, INTENTE DESPUES
Message Center (AUDIX) CALL	APPEL DE LA RECEPTION DE MESS. (AUDIX)	Chiamata dal Centro Messaggi (AUDIX)	LLAMADA DEL CENTRO DE MENSAJES (AUDIX)
NO MESSAGES	PAS DE MESSAGES	NESSUN MESSAGGIO	NINGUN MENSAJE
WHOSE MESSAGES? (DIAL EXTENSION NUMBER)	MESSAGES DE QUEL NO.? (ENTRER NO. POSTE)	LETTURA MESSAGGI. INTRODURRE NUMERO TEL.	MENSAJES DE QUIEN? (MARCAR EXTENSION)

Table 102: Malicious Call Trace

English	French	Italian	Spanish
MALICIOUS CALL TRACE REQUEST	DEPISTAGE D'APPELS MALVEILLANTS	RICHIESTA RINTRACCIO CHIAMATE MALEVOLE	RASTREO DE LLAMADA MALINTENCIONADA
MCT activated by: for:	DAM ACTIVE par: pour:	RCM attivato da: per:	RLM activada por: para:
original call redirected from:	redirection appel initial de: (EXTENSION)	chiamata iniziale rinviata da:	llamada orig. transferida de:

Table 102: Malicious Call Trace

English	French	Italian	Spanish
party: (EXTENSION)	demandeur: (EXTENSION)	utente: (INTERNO)	usuario: (EXTENSION)
party: (ISDN SID/CNI)	demandeur: (NIP/INA ISDN)	utente: (NIC/INC ISDN)	usuario: (ISDN NIE/ INU)
party: (PORT ID)	demandeur: (REF. PORT ISDN)	utente: (ID DELLA PORTA ISDN)	usuario: (ID DEL PUERTO ISDN)
party: (ISDN PORT ID)	demandeur: (REF. PORT)	utente: (ID DELLA PORTA)	usuario: (ID DEL PUERTO)
END OF TRACE INFORMATION	FIN DES INFO DE DEPISTAGE	INFORMAZIONI FINALI SUL RINTRACCIO	FIN DE INFORMACION DE RASTREO
voice recorder port:	port enregistreur vocal:	porta del registratore:	puerto de grabado de voz:

Table 103: Caller information

English	French	Italian	Spanish
Info:	INFO.:	Info:	INFORM:

Table 104: Emergency access to attendant

English	French	Italian	Spanish
a=xxxxxxxxxxxxxxx Ext xxxxx xx in EMRG Q	a=xxxxxxxxxxxxxxx POSTE xxxxx xx FIL URG	a=xxxxxxxxxxxxxxx Der xxxxx xx in C EMRG	a=xxxxxxxxxxxxxxx EXT xxxxx xx EN C EMRG

Table 105: Queue status

English	French	Italian	Spanish
HUNT GROUP <x> NOT ADMINISTERED	GROUPE DE DIST. <x> NON ADMINISTRE	GRUPPO <x> NON AMMINISTRATO	GRUPO BUSQUEDA <x> NO ADMINISTRADO

Table 106: Queue status indication

English	French	Italian	Spanish
<15 chrs> Q-time xx:xx calls xx	<15 chrs> TEMPS-F xx:xx APPELS xx	<15 chrs> T-coda xx:xx chiam xx	<15 chrs> HORA-C xx:xx LLAMADAS xx

Table 107: Miscellaneous call identifier

English	French	Italian	Spanish
sa (ACD Supervisor Assistance)	AS (Assistance surveillant)	as (Assistenza Supervisoree)	AS (Ayuda de supervisor)
ac (Attd Assistance Call)	AA (Appel assistance)	ao (Assistenza Operatore)	AO (Ayuda de operadora)
tc (Attd Control Of A Trunk Group)	CF (Commande faisceau)	fc (Fascio Controllato)	CE (Control enlaces)
an (Attd No Answer)	TR (Telephoniste sans reponse)	on (Operatore Non Risponde)	ON (Operadora no responde)
pc (Attd Personal Call)	AP (Appel personnel)	cp (Chiamata Personale)	LP (Llamada personal)

1 of 4

Table 107: Miscellaneous call identifier (continued)

English	French	Italian	Spanish
rc (Attd Recall Call)	RA (Rappel)	rc (Richiamata)	RL (Rellamada)
rt (Attd Return Call)	RE (Retour)	rt (Ritornata)	RT (Retorno)
sc (Attd Serial Call)	AS (Appel en serie)	ic (Inoltro a Catena)	LS (Llamada en serie)
co (Controlled Outward Restriction)	RD (Restriction de depart)	cu (Controllata Uscente)	RS (Restriccion saliente)
cs (Controlled Station to Station Restriction)	RP (Restriction vers postes)	cd (Controllata Derivati)	CS (Control estacion)
ct (Controlled Termination Restriction)	AR (Restriction d'arrivee)	ct (Controllata Terminante)	RE (Restriccion entrante)
db (DID Find Busy Station With CO Tones)	OP (Occupation du poste)	po (Passante Occupata)	EO (Estacion occupada)
da (DID Recall Go To Attd)	RT (Rappel telephoniste)	pr (Richiamata su Passante)	RD (Rellamada directa)
qf (Emerg. Queue Full Redirection)	FP (File d'urgence pleine deviation)	de (Deviata Emergenza)	DE (Desvio de emergencia)
hc (Held Call Timed Reminder)	AG (Indicatif d'appel en garde)	at (Avviso Chiamata in tenuta)	LR (Recordatorio de llamada retenida)
ic (Intercept)	IN (Interception)	in (Intercettata)	IN (Intercepcion)
ip (Interposition Call)	AI (Appel interposition)	ip (Interposizione)	EP (Entre posiciones)
ld (LDN Calls on DID Trunks)	SD (Selection directe)	pd (Diretta Passante)	LD (Larga distancia)
so (Service Observing)	ES (ecoute du service)	is (Inclusione Supervisore)	SS (Supervision del servicio)
na (Unanswered or Incomplete DID Call)	SR (Sans reponse)	pn (Passante Non Risposta)	SR (Sin respuesta)
ACB (Automatic Callback)	R. AUTO. (Rappel automatique)	PRN (Prenotazione Automatica)	RA (Rellamada automatica)
callback (Callback Call)	RAPPEL (Rappel)	prenotaz (Prenotazione)	RELLAM (Rellamada)

2 of 4

Table 107: Miscellaneous call identifier (continued)

English	French	Italian	Spanish
park (Call Park)	G. I. (garde par) indicatif	parch. (Parcheggiata)	ESTAC (Estacionamiento de llamada)
control (Control)	CONTROLE (Controle)	cntr.op. (Controllo Operatore)	CONTROL (Control)
ICOM (Intercom Call)	INTERCOM (Intercommunication)	ICOM (Intercom)	INTERF (Llamda interfono)
OTQ (Outgoing Trunk Queuing)	FFD (File faisceaux de depart)	RFO (Richiamata su Fascio Occupato)	EES (Espera de enlace de salida)
priority (Priority Call)	PRIORITE (Appel prioritaire)	priorita (Priorita')	PRIORIT (Llamada prioritaria)
recall (Recall Call)	APP.RAP. (Appel rappel)	richiam (Richiamata)	REPET (Rellamada)
return (Return Call)	RETOUR (Retour)	ritorno (Chiamata Ritornata)	RETORNO (Llamada de retorno)
ARS (Automatic Route Selection)	SAA (Selection de l'acheminement automatiqe)	SAI (Selez. Autom. Instradam.)	SAR (Seleccion automatica de rutas)
forward (Call Forwarding)	RENVOI (Renvoi)	deviata (Deviata)	REENVIO (Reenvio de llamada)
cover (Cover)	SUPPL. (Suppleance)	copert. (Copertura)	COBER (Cobertura)
DND (Do Not Disturb)	NPD (Ne pas deranger)	nd (Non Disturbare)	NM (No molestar)
p (Call Pickup)	P (Prise)	a (Assente)	C (Captura de llamada)
c (Cover All Calls)	s (Suppleance)	c (Copertura)	c (Cobertura de toda llamada
n (Night Sta. Serv., Incoming No Answer)	N (Service nuit, entrant pas reponse)	n (Serv. Notte, Esterna Non Risposta)	N (Servicion noct. ext. no responde)
B (All Calls Busy)	O (Tous occupes)	O (Tutte Occupate)	O (Todas ocupadas)
f (Call Forwarding)	R (Renvoi)	d (Deviata)	R (Reenvio de llamada)
b (Cover Busy)	o (Suppleance occupee)	o (Copertura per Occupato)	o (Cobertura ocupada)

3 of 4

Table 107: Miscellaneous call identifier (continued)

English	French	Italian	Spanish
d (Cover Don't Answer)	n (Suppleance pas de reponse)	n (Copertura per Non Risposta)	n (Cobertura sin respuesta)
s (Send All Calls)	E (Envoi tous appels)	r (Rinvio)	E (Envio de toda llamada)

4 of 4

Table 108: User identifiers

English	French	Italian	Spanish	Identifier
OPERATOR	TELEPHONISTE	OPERATORE	OPERADORA	Attendant
CONFERENCE	CONFERENCE	CONFERENZA	CONFERENCIA	Conference Call
EXT	POSTE	DER	EXTENSION	Extension
PAGING	PAGING	PAGING	PAGING	Paging (cannot be transplated)
OUTSIDE CALL	APPEL EXT.	ESTERNA	LLAMADA EXT.	Trunk Group
UNKNOWN NAME	INTROUVABLE	NOME SCONOSC.	DESCONOCIDO	Unknown

Table 109: Property Management System interface

English	French	Italian	Spanish
CHECK IN - Ext:	ENREGISTREMENT - POSTE:	CHECK IN - Tel:	REGISTRARSE - EXTENSION:
CHECK IN: ROOM ALREADY OCCUPIED	ENREGISTREMENT: CHAMBRE OCCUPEE	CHECK IN: CAMERA OCCUPATA	REGISTRARSE: HABITACION OCUPADA
CHECK IN COMPLETE	ENREGISTREMENT EFFECTUE	CHECK IN COMPLETATO	REGISTRO TERMINADO
CHECK IN FAILED	ECHEC D'ENREGISTREMENT	CHECK IN ERRATO	REGISTRARSE: FALLIDO
CHECK OUT - Ext:	DEPART - POSTE:	CHECK OUT - Tel:	PAGAR LA CUENTA - EXTENSION:
CHECK OUT COMPLETE: MESSAGE LAMP OFF	DEPART: PAS DE MESSAGES	CHECK OUT COMPLETATO: NESSUN MESSAGGIO	PAGO TERMINADO: NINGUN MENSAJE
CHECK OUT COMPLETE: MESSAGE LAMP ON	DEPART: MESSAGES	CHECK OUT COMPLETATO: MESSAGGI IN ATTESA	PAGO DE CUENTA TERMINADO: MENSAJES
CHECK OUT FAILED	ECHEC PROCEDURE DE DEPART	CHECK OUT ERRATO	PAGAR LA CUENTA: FALLIDO
CHECK OUT: ROOM ALREADY VACANT	DEPART - CHAMBRE INOCCUPEE	CHECK OUT: CAMERA NON OCCUPATA	PAGAR LA CUENTA: HABITACION VACANTE
MESSAGE LAMP OFF	PAS DE MESSAGES	NESSUN MESSAGGIO IN ATTESA	LUZ DE MENSAJE APAGADA
MESSAGE LAMP ON	MESSAGES	MESSAGGI IN ATTESA	LUZ DE MENSAJE ENCENDIDA
MESSAGE NOTIFICATION FAILED	ECHEC D'AVIS MESSAGES	NOTIFICA MESSAGGI ERRATA	AVISO DE MENSAJE FALLIDO
MESSAGE NOTIFICATION OFF - Ext: xxxxx	AVIS DE MESSAGES DESACTIVE - POSTE:xxxxx	NOTIFICA MESSAGGI DISABIL. - Tel: xxxxx	AVISO DE MENSAJE APAGADO - EXT: xxxxx
MESSAGE NOTIFICATION ON - Ext: xxxxx	AVIS DE MESSAGES ACTIVE - POSTE:xxxxx	NOTIFICA MESSAGGI ABILITATA - Tel: xxxxx	AVISO DE MENSAJE ENCENDIDO - EXT: xxxxx

Table 110: Security Violation Notification *1 of 2*

English	French	Italian	Spanish
Barrier Code Violation	VIOLATION DU CODE D'ENTREE	VIOLAZIONE DI CODICI DE TAGLIO	VIOLACIAON CONDIGO LIMITE
Login Violation	VIOLATION DE L'ACCES A L'ADMINISTRATION	IOLAZIONE DI INIZIO DI REGISTRAZIONE	VIOLACION CLAVE ACCESO

Table 110: Security Violation Notification *2 of 2*

English	French	Italian	Spanish
Station Security Code Violation	VIOLATION DE CODE D'ACCESS DE SECURITE	VIOLAZIONE DI CODICE DE SICUREZZA UTENTE	VIOLACION DE SEGURIDAD DE LA ESTACION
Authorization Code Violation	VIOLATION DEU CODE ACCES	VIOLAZION DEL CODICE D'AUTHORIZZAZIONE	VIOLACION DE CODIGO DE AUTORIZACION

Table 111: Stored number

English	French	Italian	Spanish
NO NUMBER STORED	AUCUN NUMERO EN MEMOIRE	NESSUN NUMERO IN MEMORIA	NINGUN NUMERO ALMACENADO

Table 112: Special codes

English	French	Italian	Spanish
m (Mark)	M (Marquer)	m (Marcato)	M (Marca)
p (Pause)	P (Pause)	p (Pausa)	P (Pausa)
s (Suppress)	S (Supprimer)	s (Soppresso)	S (Suprimir)
w (Wait)	A (Attendre)	a (Attesa)	E (Espera)
W (Indefinite Wait)	a (Attendre)	A (Attesa)	e (Espera)

Station Hunting

Table 113: Calling party display

English	French	Italian	Spanish
HUNT	Routage	Ricerca	Busqueda

Table 114: Hunt-to station display

English	French	Italian	Spanish
h	r	r	b

In the following displays, x and y denote the Route Plan Number (RPN 1-8), yyy is a 3-letter abbreviation for the day of the week, and zz:zz is the activation time (24-hour time). Also below is the table that lists the 3-letter abbreviations for the day of the week.

Table 115: Time-of-Day routing messages

English	French	Italian	Spanish
ENTER ACTIVATION ROUTE PLAN, DAY & TIME	ENTRER PLAN D'ACTIVATION, JOUR ET HEURE	INTRODURRE PIANO DA ATTIV., GIORNO E ORA	INTRODUZCA PLAN ACT DE RUTAS, DIA Y HORA
ENTER DEACTIVATION DAY AND TIME	ENTRER JOUR ET HEURE DE DESACTIVATION	INTRODURRE GIORNO E ORA DI DISATTIVAZ	INTRODUZCA DIA Y HORA DE DESACTIVACION
OLD ROUTE PLAN: x ENTER NEW PLAN:	ACHEMINEMENT ANT.: x ENTRER NOUVEAU:	INSTRADAMENTO PREC: x INTROD IL NUOVO:	PLAN RUTAS ANT: x INTRODUZCA EL NUEVO:
OLD ROUTE PLAN: x NEW PLAN: y	ACHEMINEMENT ANT.: x NOUVEAU PLAN: y	INSTRADAMENTO PREC: x NUOVO PIANO: y	PLAN RUTAS ANT: x NUEVO PLAN: y
ROUTE PLAN: x FOR yyy ACT-TIME: zz:zz	ACHEM.: x POUR yyy ACT-HEURE: zz:zz	INSTRADAMENTO: x PER yyy ATTIV ORE:zz:zz	PLAN RUTAS: x PARA yyy HORA-ACT: zz:zz
ROUTE PLAN: x FOR yyy DEACT-TIME: zz:zz	ACHEM.: x POUR yyy DESACT-HEURE: zz:zz	INSTRADAM.: x PER yyy DISATTIV ORE:zz:zz	PLAN RUTAS: x PARA yyy HORA-DESACT:zz:zz

To enter the day of the week, the user dials 1 for Sunday, 2 for Monday, and so on.

Table 116: Time-of-Day routing days of the week

English	French	Italian	Spanish
MON	LUN	LUN	LUN
TUE	MAR	MAR	MAR
WED	MER	MER	MIE
THU	JEU	GIO	JUE
FRI	VEN	VEN	VIE
SAT	SAM	SAB	SAB
SUN	DIM	DOM	DOM

English	French	Italian	Spanish
TRANSFER COMPLETED	TRANSFERT EFFECTU	TRASFERIMENTO COMPLETATO	TRANSFERENCIA REALIZADA

Mapping enhanced display characters

Use the following tables to map US English characters to Russian, Japanese, European, or Ukrainian characters. Characters appear on the display terminal in the order in which you enter them. If you want the display to read right to left, enter the characters in reverse order on the screen.

US English to Russian characters

US English to Russian characters

Russian	US English	Russian	US English
space	space	Й	Q
Ф	A	К	R
И	B	Ы	S
С	C	Е	T
В	D	Г	U
У	E	М	V
А	F	Ц	W
П	G	Ч	X
Р	H	Н	Y
Ш	I	Я	Z
О	J	Х	[
Л	K	Ъ	]
Д	L	Ж	;
Ь	M	э	\
Т	N	Ъ	,
Щ	O	Ю	.
З	P		

US English to Japanese characters

Japanese	US English	Japanese	US English
space	space	ｺ	:
｡	!	ｻ	;
｢	“	ｼ	<
｣	#	ｽ	=
､	$	ｾ	>
･	%	ｿ	?
ｦ	&	ﾀ	@
ｧ	‘	ﾁ	A
ｨ	(	ﾂ	B
ｩ	)	ﾃ	C
ｪ	*	ﾄ	D
ｫ	+	ﾅ	E
ｬ	,	ﾆ	F
ｭ	-	ﾇ	G
ｮ	.	ﾈ	H
ｯ	/	ﾉ	I
ｰ	0	ﾊ	J
ｱ	1	ﾋ	K
ｲ	2	ﾌ	L
ｳ	3	ﾍ	M
ｴ	4	ﾎ	N
ｵ	5	ﾏ	O
ｶ	6	ﾐ	P
ｷ	7	ﾑ	Q

Japanese	US English	Japanese	US English
ｹ	8	ｿ	R
ｺ	9	ﾀ	S
ｻ	[	ﾁ	T
ｼ	\	ﾂ	U
ｽ	]	ﾃ	V
	^	ﾄ	W
ｾ	_	ﾅ	X
		ﾆ	Y
		ﾇ	Z

For Japanese, the letter z and the left brace { and the pipe (|) characters map to Kanji characters as follows:

- The letter z. Symbol for 1,000
- The left brace {. Symbol for 10,000
- The pipe (|). Symbol for Yen

US English to European characters

Some of the characters in the following map appear in only uppercase or lowercase, such as, €, Ê, ø, and others.

European	US English	European	US English
í	space	ø	=
ï	!	æ	>
ã	“	Ó	?
á	#	î	@
à	$ ‘	å	A
ú	%	ą	B
ù	&	â	C
é	‘	ű	D
è	(	ů	E
ć	)	è	F
ł	*	ė	G
Ď	+	ę	H
ý	,	Ç	I
ž	-	ř	J
õ	.	Đ	K
ò	/	ÿ	L
Í	0	ń	M
Ï	1	Æ	N
Ã	2	ő	O
Á	3	Î	P
À	4	Å	Q
Ú	5	Ă	R

European	US English	European	US English
Ù	6	Â	S
É	7	Ü	T
È	8	Ů	U
č	9	Ê	V
Ł	:	ė	W
đ	;	Ę	X
Ý	<	ṡ	Y
ř	Z	â	r
´	[	Ă	s
Ÿ	\	ū	t
Ń	]	Ū	u
Ñ	^	Ě	v
ō	_	Ë	w
ì	`	ğ	x
ä	a	Ş	y
β	b	Ť	z
ů	d	þ	{
Ü	e	Ż	|
ě	f	Ň	}
ë	g		
ğ	h		
Š	i		
Ţ	j		
¿	k		
ź	l		
ň	m		
ñ	n		
ö	o		
İ	p		
Ā	q		

US English to Ukrainian characters

Ukrainian	US English	Ukrainian	US English
space	space	й	Q
Ф	A	К	R
И	B	;	S
С	C	Е	T
В	D	г	U
У	E	М	V
А	F	Ц	W
П	G	ч	X
Р	H	Н	Y
Ш	I	Я	Z
О	J	Х	[
Л	K	І	]
д	L	Ж	;
Ь	M	Є	\
Т	N	Б	,
Щ	O	ю	.
З	P		

Administering Telephone Display

This section describes the screens that you use to administer the Telephone Display feature.

Screens for administering Telephone Display

Screen name	Purpose	Fields
Date/Time Mode and Formats - English	Set up the appearance of the date and time displays.	All
Date/Time Mode and Formats - French, Italian, Spanish, User-Defined, and Unicode	Set up the appearance of the date and time displays.	All
Language Translations	Enter translations in a user-defined language.	All
Leave Word Calling Format - English	Set up the appearance of the Leave Word Calling displays.	All
Leave Word Calling Format - French, Italian, Spanish, User-Defined, and Unicode	Set up the appearance of the Leave Word Calling displays.	All

Reports for Telephone Display

The following reports provide information about the Telephone Display feature:

- None

Considerations for Telephone Display

This section provides information about how the Telephone Display feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Telephone Display under all conditions. The following considerations apply to Telephone Display:

- None

Interactions for Telephone Display

This section provides information about how the Telephone Display feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Telephone Display in any feature configuration.

The following interactions apply to all capabilities:

- Distributed Communications System (DCS)

  Trunk group and attendant information that is associated with a DCS call can be translated. If the displays are not associated with a DCS call, the name that appears is the name of the trunk group that is administered on the Trunk Group screen.

- Single-Digit Dialing and Mixed-Station Numbering

  If the system dial plan uses prefixed extensions, the prefix is not displayed when the extension is displayed. Users can use the Return Call button to dial prefixed extensions, because the system dials the prefix, even though the prefix is not displayed.

The following interactions pertain to the Enhanced Telephone Display capability:

- Adjunct Switch Application Interface (ASAI) and related adjuncts

  Information that Communication Manager sends to any adjunct is the literal value of the field, not the enhanced characters. The display appears as a string of random characters. For example, "2<@^."

- INTUITY AUDIX Voice Power and Audix Voice Power Lodging

  Not supported.

- Data Call Setup

  Not supported.

- Distributed Communications Systems (DCS)

  All switch nodes in a DCS network must have must have the same software load installed on each server or media server, must have the enhanced characters enabled, and must have telephones with the same firmware type.

- ECMA and QSIG Networking

  Information must be sent between the servers that run Communication Manager.

- Leave Word Calling - Adjunct

  Not supported.

- Message Retrieval - Print Messages (Demand Print)

  Not supported.

- Monitor 1 and OneVision

  Monitor 1 and OneVision receive ASCII characters.

- OSSI

  OSSI displays the literal value of the display field, and not the enhanced characters.

- Passageway Direct Connect

  Not supported.

- VUStats

  You must use telephones that support enhanced characters. If telephones do not use enhanced characters, the software might clear the display, or show the information on the display incorrectly.

Temporary Bridged Appearance

Use the Temporary Bridged Appearance feature to allow multiappearance telephone users in a Terminating Extension Group (TEG) or a Personal Central Office Line (PCOL) group to bridge onto an existing group call. If the Call Pickup feature is used to answer the call, the originally called party can bridge onto the call. This feature also allows a called party to bridge onto a call that redirects to coverage before the called party can answer the call.

Detailed description of Temporary Bridged Appearance

This section provides a detailed description of the Temporary Bridged Appearance feature.

An incoming call to a Terminating Extension Group (TEG) or Private Central Office Line (PCOL) group is not a call to an individual. However, one particular member of the group can be the most qualified person to handle the given call. If this individual does not answer the call originally, this individual can bridge onto the call. The answering party does not have to transfer the call.

A call to an individual can be answered by a member of a call pickup group. While the call is still connected, the called party can bridge onto the call, and the answering party hangs up.

Call Coverage provides redirection of calls to alternate answering positions or covering users. A temporary bridged appearance is maintained at the called telephone.

The called party can answer the call at any time, even if the call is already answered by a covering user. If the called party does not bridge onto the call, the covering user can use the Consult function of Call Coverage to determine if the called party wants to accept the call. The Consult function uses the temporary bridged appearance that is maintained on the call. When the consult call is finished, the temporary bridged appearance is removed.

Stations that usually have a temporary bridged appearance with their coverage point do not have a temporary bridged appearance if the coverage point is CM Messaging.

Administering Temporary Bridged Appearance

This section describes the screens that you use to administer the Temporary Bridged Appearance feature.

Screens for administering Temporary Bridged Appearance

Screen name	Purpose	Fields
Feature-Related System Parameters	Enable the Temporary Bridged Appearance feature for Call Pickup.	**Temporary Bridged Appearance on Call Pickup**
system-parameters coverage-forwarding	Govern how a covering user who has placed an answered coverage call on hold is treated if the original principal bridges onto the call.	**Keep Held SBA at Coverage Point**
	Allow a user to maintain a simulated bridged appearance when a call redirects to coverage.	**Maintain SBA At Principal?**
	Either direct the system to maintain a simulated bridged appearance on the principal when redirecting to a final off-net coverage point or allow the system to drop the SBA on the principal's telephone when the call redirects off-net at the last coverage point, eliminating the cut-through delay inherent in CCRON calls, but sacrificing the principal's ability to answer the call.	**Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point?**

Considerations for Temporary Bridged Appearance

This section provides information about how the Temporary Bridged Appearance feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Temporary Bridged Appearance under all conditions. The following considerations apply to Temporary Bridged Appearance:

- Temporary Bridged Appearance allows a party to bridge onto a call. The answering party does not have to transfer the call, which is convenient and saves time.

- Temporary Bridged Appearance does not provide the capability to originate calls, or the capability to answer the calls of another party. The Bridged Call Appearance feature provides these capabilities.
- If two parties are bridged together on an active call with a third party, and if the Conference Tone feature is enabled, conference tone is heard.
- The Bridged Call Appearance feature enhances Temporary Bridged Appearance by allowing:
  - More than one call to an extension to be bridged.
  - Calls to be originated from bridged appearances.

Interactions for Temporary Bridged Appearance

This section provides information about how the Temporary Bridged Appearance feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Temporary Bridged Appearance in any feature configuration.

- Call Coverage

  Calls that are redirected to Call Coverage maintain a temporary bridged appearance on the called telephone if a call appearance is available to handle the call. The called party can bridge onto the call at any time. The system can be administered to allow a temporary bridged appearance of the call to either remain at, or be removed from, the covering telephone after the principal bridges onto the call. If two parties are bridged together on an active call with a third party, all three parties hear the bridging tone.

- Consult

  Consult calls use the temporary bridged appearance that is maintained on the call. At the conclusion of a consult call, the bridged appearance is no longer maintained. If the principal chooses not to talk with the calling party, the principal cannot bridge onto the call later.

- Conference and Transfer

  If a call has, or had a temporary bridged appearance and the call is then conferenced or transferred, and is redirected to coverage again, a temporary bridged appearance is not maintained at the conferenced-to or the transferred-to extension.

- Privacy - Manual Exclusion

  When Privacy - Manual Exclusion is activated, other users are prevented from bridging onto a call. A user who attempts to bridge onto a call when this feature is active is dropped.

Note:

The displays of IP phones and call logs show whether calls were answered through call pickup from another station, and if the Temporary Bridged Appearance feature is in use. This does not apply to pickup through the Team button.

Tenant Partitioning

Use the Tenant Partitioning feature to provide telecommunications services to multiple independent groups of users through a single server that runs Communication Manager. The Tenant Partitioning feature usually provides these services from a single provider to multiple tenants of an office complex. Each tenant appears to have a dedicated Communication Manager, even though the tenants share the same Communication Manager. You can also use this feature to provide group services, such as departmental attendants, on a single-customer server that runs Communication Manager.

Detailed description of Tenant Partitioning

This section provides a detailed description of the Tenant Partitioning feature.

The Tenant Partitioning feature is not available with Offer B.

The Tenant Partitioning feature provides the following services to tenants:

- Telephone equipment
- Building wiring
- Public network access and private network access
- Attendant services

You can also use the Tenant Partitioning feature to assign a separate music source to each tenant partition that plays when a user or an attendant places a caller on hold.

Note:
If you use equipment that rebroadcasts music or other copyrighted materials, you might be required to obtain a copyright license from, or pay fees to, a third party. A Magic-on-Hold system does not require such a license. You can purchase a Magic-on-Hold system from Avaya, or from an Avaya business partner.

Proper administration can protect tenant resources, including trunking facilities, and all other Communication Manager endpoints from unauthorized access by other tenants.

For the Tenant Partitioning feature to function properly in your system, you must ensure that:

- All tenants can call and be called by tenant 1. This is the system default. If you change this default, some call types fail. For example, dial 0 fails, as do security violation calls and automatic circuit assurance calls.
- All stations in a call-pickup group are under control of the same tenant.
- All stations with bridged appearances are under control of the same tenant.

- Stations in different departments, for the purposes of attendant services, can call each other.

You must assign a tenant partition number to each entity, such as an endpoint or a virtual endpoint, to which you assign a Class of Restriction (COR). You do not assign a tenant partition number to an authorization code or to fixed-assignment virtual endpoints.

You must specify an attendant group for each tenant that you define, even if the attendant group does not have an assigned console. You must also assign an attendant console to a tenant partition, and you must assign a group number to the attendant console.

Partitioning tenants

The system has a default of one universal tenant for the system. This tenant is in partition 1, and is usually the service provider. Another system default that the tenant in partition 1 has access to all facilities in the system, and that all other tenants can access the tenant in partition 1. The tenant in partition one is usually referred to as tenant 1.

The service provider creates additional partitions that are based on tenant requirements. When you create tenant partitions, remember that:

- You can assign each Communication Manager endpoint to only one tenant partition. And, you must pass each endpoint to a partition. For example, you must assign each telephone, attendant console, trunk, and virtual endpoint. Virtual endpoints include listed directory numbers and virtual directory number (VDN) to a tenant partition.
- Most tenant partitions are separate units. By default, the system does not allow tenants, except tenant 1, to access telephones or trunk facilities that belong to other tenants. However, you can change this system default. You can give explicit permission for a tenant to access another tenant. For example, you can allow tenant 6 to call only tenant 9 and tenant 16.

  Note:
  If a tenant has permission to call another tenant, the tenant has access to all the endpoints that belong to the other tenant. For example, if tenant 6 has permission to call tenant 9, tenant 6 can also use any trunk facilities in tenant partition 9.
- The system can use tenant partitioning restrictions to block calls between two users in the system. However, either user can use the Direct Inward Dialing (DID) extension of the other user to call over the public network.
- If tenants want to share some, but not all, facilities, you must group the shared facilities into a separate partition. For example, if two tenants share a trunk, but do not have direct system access to call each other, put the trunk in its own partition. Both tenants can then access the trunk.

You must also consider the constraints and the requirements of access control, attendant services, music sources on hold, and network route selection when you establish or assign partitions.

Access control

Tenant-to-tenant access restrictions limit some features, such as Call Coverage. For example, the coverage of tenant 2 includes a telephone from tenant 3 in its coverage path. If tenant 4 has permission to call tenant 2, but does not have permission to call tenant 3, a call from tenant 4 to tenant 2 skips the tenant 3 coverage point.

You might also want to set up tenants with special access privileges. For example, you might give a restaurant in an office complex permission to receive calls from any other tenant. You might also want tenants to have permission to call, or be called by, building security, or those who administer and troubleshoot Communication Manager.

You can also assign all central office (CO) trunks to one tenant partition. All other tenants can then access the CO trunks.

Attendant services

With Tenant Partitioning, you can administer personalized attendant services for each tenant.

The system provides one principal attendant, and either one night attendant or one day and night attendant, for each attendant group. You assign each tenant an attendant group for service. Each attendant group has a separate queue. Queue warning lamps remain dark when Tenant Partitioning is active. However, when someone presses a queue-status button, the system displays the status of the attendant-group queue. The total number of calls queued for all tenants cannot exceed the system limit.

Attendant groups can serve more than one tenant, if the two tenants have permission to access each others facilities. For example, can use the facilities of one tenant to extend a call to another tenant, if the tenant has permission to access the facilities of the other tenant.

Each tenant can have a designated night-service station. When a night attendant is unavailable, the system directs calls to an attendant group that is in night service, to the night-service station of the appropriate tenant. When someone places an attendant group into night service, all trunk groups and hunt groups that belong to tenants that the attendant group serves, go into night service. In this case, the system routes incoming calls to the night-service destination of the appropriate tenant. Each tenant can have exclusive access to the following entities:

- Listed directory number (LDN) night destination
- Trunk answer on any station (TAAS) port
- Night attendant

An attendant can specify that access to a trunk group is under attendant control, if the trunk group is assigned to a tenant served by that attendant group. The system directs any valid user attempt to access the trunk group to the attendant group that serves the tenant.

Network route selection

You can place trunk groups that belong to different tenants in the same route pattern. Calls that the system routes to that pattern select the first trunk group in the pattern that has caller access permission.

Tenant Partitioning examples

The following example describes how you might administer Tenant Partitioning in an office complex.

You assign tenant partition 1, the universal tenant, as the service provider. All other tenants can call, and be called by, the service provider.

You assign tenant partitions 2 through 15 to individual businesses in the complex. You maintain the system-default restrictions for these tenants. These restrictions specify that tenants cannot access the telephones, the trunk facilities, or the other Communication Manager endpoints that belong to other tenants.

You assign tenant partition 16 to the restaurant in the building complex. You give all tenants permission to call the restaurant. However, to prevent access to trunks and other facilities that belong to other tenants, you do not allow the restaurant to call the other tenants.

You assign tenant partition 17 to all the CO trunk groups. You give all tenants permission to call tenant 17.

You assign tenant partition 18 to a trunk group that tenants 3 and 7 want to share. You give tenants 3 and 7 access to this partition, and you deny all other tenants access to partition 18. To prevent toll fraud, you do not allow tenant 18 to place calls to tenant 18.

All tenants can use the same Automatic Route Selection (ARS) route pattern. In this example, the trunk for tenant partition 18, the private trunk that tenants 3 and 7 share, is first in the route pattern. Tenant partition 17 is second in the route pattern. The system routes calls that tenants 3 and 7 make to partition 18 and then, as a second option, to partition 17. The system routes all other tenants directly to partition 17, because you deny all other tenants access to partition 18.

Assign the facilities that the tenants do not share to the tenant partition that the facilities serve. These facilities can include trunk groups, VDNs, telephones, attendant consoles, and other endpoints.

Table 117: Calling permissions for the partitions on page 1583 summarizes the calling permissions for the different tenant partitions. *Yes* indicates that the partitions have permission to call, and be called by, each other. *No* indicates that partitions cannot call, or be called by, each other.

Table 117: Calling permissions for the partitions

Calling tenant partition number	Called tenant partition number					
	1	**2, 4 through 6, and 8 through 15**	**3, 7**	**16**	**17**	**18**
1	Yes	Yes	Yes	Yes	Yes	Yes
2, 4-6, 8-15	Yes	Each partition can call itself, but cannot call the other partitions.	No	Yes	Yes	No
3, 7	Yes	No	Each partition can call itself, but cannot call the other partitions.	Yes	Yes	Yes
16	Yes	No	No	Yes	Yes	No
17	Yes	Yes	Yes	Yes	Yes	No
18	Yes	No	Yes	No	No	No

Multiple Music-on-Hold

Tenant Partitioning allows you to assign a separate music source to each tenant partition. A caller hears the music when a user places a call on hold. The tenant number that you assign to the called extension usually determines the music source that the user hears. This capability allows you to customize the music, or the messages, for the business needs of each tenant partition.

If the COR of the user extension that places the call on hold allows music-on-hold, a caller on hold hears the music source that is assigned to the partition at which the call initially terminates. For example, if the system first routes a call to an CM Messaging automated attendant, and then routes the call to the appropriate tenant partition, the caller who is on hold hears the music source of the CM Messaging automated attendant. The caller who is on hold does not hear the music source of the tenant partition to which the system routes the call. Likewise, if a caller in tenant partition 2 makes an out-going call that uses the trunk groups of tenant 3, the caller hears the music source that is assigned to tenant 3. If the COR of the called extension does not allow music on hold, the caller hears nothing.

The maximum number of allowed music sources is the same as the maximum number of allowed tenant partitions. More than one tenant partition can use each music source.

Table 118: Types of music-on-hold on page 1584 shows which music-on-hold types that you can assign to each tenant partition.

Table 118: Types of music-on-hold

Type	System response for a call who is on hold
none	Silence
tone	System-wide administered tone
music	This is the type of music that is associated with the administered port. The number of allowed music sources equals the number of allowed tenant partitions. Each partition can have its own music source.

Administering Tenant Partitioning

The following steps are part of the administration process for the Tenant Partitioning feature:

- Defining a tenant partition
- Assigning a tenant partition number to an access telephone
- Assigning a tenant partition number to an agent login ID
- Assigning a tenant partition number to an announcement
- Assigning a tenant partition number to an attendant
- Assigning a tenant partition number to a data module
- Assigning a tenant partition number to a hunt group
- Assigning a tenant partition number to a loudspeaker paging zone
- Assigning a tenant partition number to the remote access extension
- Assigning a tenant partition number to a user extension
- Assigning a tenant partition number to a terminating extension group
- Assigning a tenant partition number to a trunk group
- Assigning a tenant partition number to a vector directory number
- Assigning the sources of music for the tenant partitions

This section describes:

- Any prerequisites for administering the Tenant Partitioning feature
- The screens that you use to administer the Tenant Partitioning feature
- Complete administration procedures for the Tenant Partitioning feature

Prerequisites for administering Tenant Partitioning

You must complete the following actions before you can administer the Tenant Partitioning feature:

- Ensure that the **Tenant Partitioning?** field on the Optional Features screen is set to **y**. If the **Tenant Partitioning?** field is set to **n**, your system is not enabled for the Tenant Partitioning feature. Contact your Avaya representative for assistance before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Screens for administering Tenant Partitioning

Screen name	Purpose	Fields
Access Endpoint	Assign a tenant partition number to an access endpoint.	**TN**
Agent LoginID	Assign a tenant partition number to an agent login ID.	**TN**
Announcements/Audio Sources	Assign a tenant partition number to an announcement that is assigned to an extension.	**TN**
Attendant Console	Assign the group number and the tenant partition number to an attendant.	• **Group** • **TN**
Data Module	Assign a tenant partition number to a data module.	**TN**
Feature-Related System Parameters	Enable the Tenant Partitioning feature for your system.	**Tenant Partitioning?**
Hunt Group	Assign a tenant partition number to a hunt group.	**TN**
Loudspeaker Paging	Assign a tenant partition number to each loudspeaker paging zone.	**TN**
Music Sources	Assign the sources of the music for the system.	All
Remote Access	Assign a tenant partition number to the remote access extension.	**TN**

Screen name	Purpose	Fields
Station	Assign a tenant partition number to a user extension.	**TN**
Tenant	Define a tenant to the system.	All
Terminating Extension Group	Assign a tenant partition number to a Terminating Extension Group (TEG).	**TN**
Trunk Groups	Assign a tenant partition number to a trunk group.	**TN**
Vector Directory Number	Assign a tenant partition number to a vector directory number (VDN).	**TN**

Defining a tenant partition

To assign a music source to a tenant partition:

1. Type **change tenant *n***, where ***n*** is the tenant that you want to change. Press **Enter**.

   The system displays the Tenant screens (Figure 402: Tenant screen on page 1586).

Figure 402: Tenant screen

```
change tenant 18
                                  Tenant 18


               Tenant Description: ____________________________________________

                  Attendant Group: 1

            Ext Alert Port (TAAS): _______ Ext Alert (TAAS) Extension: ____*

                Night Destination: _____

                     Music Source: 1
```

   The **Tenant** field is a display-only field. This field contains the tenant number that you typed on the command line.

2. In the **Tenant Description** field, type a description of the tenant. You can type 40 characters. You can leave the field blank, but a description helps you identify the tenant when you change other information about the tenant.

3. In the **Attendant Group** field, type the number of the attendant group for the tenant partition. The system assigns the number 1 as the default for the **Attendant Group** field.

   The default for the system is that all attendant groups exist. However, the attendant group is empty if you do not assign consoles to the attendant group.

4. **In the Ext Alert Port (TAAS)** field, perform one of the following actions:

   - If trunk answer from any station (TASS) alert port information does not exist, type an **x**.
   - If TASS alert port information exists, enter the 7-character port number.

     The circuit pack must be installed and defined to the system before you can refer to the circuit pack in the **Ext Alert Port (TAAS)** field. The port type and the object type must be consistent. You can assign the port to only one tenant. Use the information in Port information for the Ext Alert Port (TAAS) field on page 1587 to construct the 7 character port number.

Table 119: Port information for the Ext Alert Port (TAAS) field

Characters	Meaning	Value
1-2	Cabinet Number	01 through 03
3	Carrier	A through E
4-5	Slot Number	00 through 20
6-7	Circuit Number	01 through 31

5. In the **Night Destination** field, type the night service station extension, if you want night service for the tenant. Type an extension that already exists in the system.
6. In the **Ext Alert (TAAS) Extension** field, type an extension that already exists in the system.

   Note that, the system displays the **Ext Alert (TAAS) Extension** field if you type an **x** in the **Ext Alert Port (TAAS)** field.

7. In the **Music** field, type the source of the music or the tone for the tenant partition.
8. Press **Enter** to save your changes.
9. Click **Next** until you see the **Calling Permission** area (Figure 403: Tenant screen on page 1588).

   Note that the **Tenant** field is a display only field. This field contains the tenant number that you entered on the command line.

Figure 403: Tenant screen

```
                                  Tenant 18


CALLING PERMISSION (Enter y to grant permission to call specified Tenant)


 1? y   11? n   21? n   31? n   41? n   51? n   61? n   71? n   81? n   91? n
 2? n   12? n   22? n   32? n   42? n   52? n   62? n   72? n   82? n   92? n
 3? n   13? n   23? n   33? n   43? n   53? n   63? n   73? n   83? n   93? n
 4? n   14? n   24? n   34? n   44? n   54? n   64? n   74? n   84? n   94? n
 5? n   15? n   25? n   35? n   45? n   55? n   65? n   75? n   85? n   95? n
 6? n   16? n   26? n   36? n   46? n   56? n   66? n   76? n   86? n   96? n
 7? n   17? n   27? n   37? n   47? n   57? n   67? n   77? n   87? n   97? n
 8? n   18? y   28? n   38? n   48? n   58? n   68? n   78? n   88? n   98? n
 9? n   19? n   29? n   39? n   49? n   59? n   69? n   79? n   89? n   99? n
10? n   20? n   30? n   40? n   50? n   60? n   70? n   80? n   90? n  100? n
```

10. In the numbered fields, perform one of the following actions:
    - To enable calling permission between the tenant that you entered in the command line and any other tenant in the system, type **y**.
    - To disable calling permission between the tenant that you entered in the command line and any other tenant in the system, type **n**.

    The system default for the calling permissions are to:
    - Allow the tenant to call itself
    - Allow the tenant to call tenant 1
    - Turn off all other calling permissions between tenants

Assigning a tenant partition number to an access telephone

To assign a tenant partition number to an access telephone:

1. Type **change access-endpoint *n***, where ***n*** is the extension of the access telephone. Press **Enter**.

   The system displays the Access Endpoint screen (Figure 404: Access Endpoint screen on page 1589).

Figure 404: Access Endpoint screen

```
change access-endpoint 30001                                    Page 1 of 1
                              ACCESS ENDPOINT

           Extension: 30001      (Starting) Port:_______
   Communication Type: voice-grade-data      Name:_____________

                 COR: 1                       COS: 1
                  TN: 1                       ITC: restricted
```

2. In the **TN** field, type the tenant partition number for the access endpoint. The valid entries for this field are **1** to **100**.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to an agent login ID

To assign a tenant partition number to an announcement:

1. Type **change agent loginid *n***, where ***n*** is the number of the agent login ID that you want to change. Press **Enter**.

   The system displays the Agent LoginID screen (Figure 405: Agent LoginID screen on page 1590).

Figure 405: Agent LoginID screen

```
change agent-loginID 100                                    Page 1 of 2
                                AGENT LOGINID

                Login ID: 100                                   AAS? n
                    Name:                                     AUDIX? n
                      TN: 1                             LWC Reception: spe
                     COR: 1                       LWC Log External Calls? n
           Coverage Path:                       AUDIX Name for Messaging:
           Security Code:
                                              LoginID for ISDN Display? n
                                                          Password:
                                            Password (enter again):
                                                       Auto Answer: station




     WARNING:  Agent must log in again before skill changes take effect
```

2. In the **TN** field, type the tenant partition number for the agent login ID. The system assigns the number 1 as the default for a tenant partition number.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to an announcement

To assign a tenant partition number to an announcement:

1. Type **change announcements**. Press **Enter**.

   The system displays the Announcements/Audio Sources screen (Figure 406: Announcements/Audio Sources screen on page 1591).

Figure 406: Announcements/Audio Sources screen

```
                                                              Page 1 of X
                          ANNOUNCEMENTS/AUDIO SOURCES
    Ext.    Type       COR  TN  Name                      Q  QLen Pro  Rate Port
 1: 1701_   analog____ 1_   1_  busy                      y  1000 N/A  N/A  1B0404
 2: 1702_   analog____ 1_   1_  out of service              N/A  N/A  N/A  1B1701
 3: 1703_   integrated 1_   1_  please dial                n  N/A  n    32   1B18
 4: 1704_   aux-trunk_ 1_   1_  call-back                  y  20   N/A  N/A  2C0902
 5: _____   _________  1_   1_  _________________________ n
 6: _____   _________  1_   1_  _________________________ n
 7: _____   _________  1_   1_  _________________________ n
 8: _____   _________  1_   1_  _________________________ n
 9: _____   _________  1_   1_  _________________________ n
10: _____   _________  1_   1_  _________________________ n
11: _____   _________  1_   1_  _________________________ n
12: _____   _________  1_   1_  _________________________ n
13: _____   _________  1_   1_  _________________________ n
14: _____   _________  1_   1_  _________________________ n
15: _____   _________  1_   1_  _________________________ n
16: _____   _________  1_   1_  _________________________ n
```

2. In the **TN** field, type the tenant partition number for the extension. The system assigns the number 1 as the default for a tenant partition number.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to an attendant

To assign the tenant partition number to an attendant:

1. Type **`change attendant`** ***`n`***, where ***`n`*** is the number of the attendant that you want to change.

   The system displays the Attendant Console screen, Figure 407: Attendant Console screen on page 1592.

Figure 407: Attendant Console screen

```
change attendant 1                                          Page 1 of 4
                            ATTENDANT CONSOLE 1

         Type: console          Name: Gertrude Attendant 64B0824
    Extension: 70199           Group: 1                Auto Answer: none
 Console Type: principal          TN: 1                Data Module? n
         Port: 64B0824           COR: 1          Disp Client Redir? n
                                 COS: 1           Display Language: english
                                                  H.320 Conversion? n

DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS (Trunk Access Codes)
    Local Remote           Local Remote             Local Remote
 1:                     5:                       9:
 2:                     6:                      10:
 3:                     7:                      11:
 4:                     8:                      12:

HUNDREDS SELECT BUTTON ASSIGNMENTS
 1:           5:           9:           13:          17:
 2:           6:          10:           14:          18:
 3:           7:          11:           15:          19:
 4:           8:          12:           16:          20:
```

2. In the **Group** field, type the group number for the Attendant. The valid entries for this field are **1** to **28**.
3. In the **TN** field, type the tenant partition number for the Attendant. The valid entries for this field are **1** to **100**.
4. Press **Enter** to save your changes.

Assigning a tenant partition number to a data module

To assign a tenant partition number to a data module:

1. Type **change data-module *n***, where ***n*** is the extension of the data module. Press **Enter**.

   The system displays the Data Module screen (Figure 408: Data Module screen on page 1593).

Figure 408: Data Module screen

```
change data-module 30                                          Page 1 of 2
                                DATA MODULE

  Data Extension: 30            Name: 27                          BCC:
            Type: data-line___   COS: 1
            Port: _______        COR: 1
             ITC: restricted__    TN: 1                 Connected to: dte


ABBREVIATED DIALING
  List1:

SPECIAL DIALING OPTION:



ASSIGNED MEMBER (Station with a data extension button for this data module)

          Ext     Name
      1: 1002    27 character   station name
```

2. In the **TN** field, type the tenant partition number for the data module. The valid entries for this field are **1** to **100**.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to a hunt group

To assign a tenant partition number to a hunt group:

1. Type **change hunt-group *n***, where ***n*** is the hunt group number to which you want to assign a partition number. Press **Enter**.

   The system displays the Hunt Group screen (Figure 409: Hunt Group screen on page 1594).

Figure 409: Hunt Group screen

```
change hunt-group 4                                          Page 1 of X
                                    HUNT GROUP

           Group Number: 4__                                    ACD?
             Group Name: _____________________________        Queue? y
        Group Extension: ________                            Vector?
             Group Type:                                Coverage Path: ____
                     TN:                        Night Service Destination: ____
                    COR:                                MM Early Answer?
          Security Code: ____
       ISDN Caller Disp: ________

           Queue Length: ___
Calls Warning Threshold: ___   Port: x      Extension: ____
 Time Warning Threshold: ___   Port: x      Extension: ____
```

2. In the **TN** field, type the tenant partition number for the hunt group.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to a loudspeaker paging zone

To assign a tenant partition number to a loudspeaker paging zone:

1. Type **`change paging loudspeaker`**. Press **Enter**.

   The system displays the Loudspeaker Paging screen (Figure 410: Loudspeaker Paging screen on page 1595).

Figure 410: Loudspeaker Paging screen

```
  change paging loudspeaker                                        Page 1 of 1
                              LOUDSPEAKER PAGING

                                    CDR? y
            Voice Paging Timeout (sec):
           Code Calling Playing Cycles:

PAGING PORT ASSIGNMENTS
                  Voice Paging     Code Calling
 Zone  Port       TAC  COR  TN     TAC  COR  TN     Location:
   1:                        1                1     27 character LOUDSPK PAGING
   2:                        1                1     PAGING
   3:                        1                1     PAGING
   4:                        1                1     PAGING
   5:                        1                1     PAGING
   6:                        1                1     PAGING
   7:                        1                1     PAGING
   8:                        1                1     PAGING
   9:                        1                1     PAGING
 ALL:                        1                1
```

2. In the **TN** field, type the tenant partition number for the loudspeaker paging zone.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to the remote access extension

To assign a tenant partition number to the remote access extension:

1. Type **`change remote-access`**. Press **Enter**.

   The system displays the Remote Access screen (Figure 411: Remote Access screen on page 1596).

Figure 411: Remote Access screen

```
change remote-access
                                  REMOTE ACCESS
   Remote Access Extension_________          Barrier Code Length____
Authorization Code Required? y                  Remote Access Dial Tone: n
Barrier Code    COR  TN  COS    Expiration Date   No. of Calls    Calls Used
1:_________     1__  1_  1__     __/__/__          ______          ______
2:_________     1__  1_  1__     __/__/__          ______          ______
3:_________     1__  1_  1__     __/__/__          ______          ______
4:_________     1__  1_  1__     __/__/__          ______          ______
5:_________     1__  1_  1__     __/__/__          ______          ______
6:_________     1__  1_  1__     __/__/__          ______          ______
7:_________     1__  1_  1__     __/__/__          ______          ______
8:_________     1__  1_  1__     __/__/__          ______          ______
9:_________     1__  1_  1__     __/__/__          ______          ______
10:________     1__  1_  1__     __/__/__          ______          ______
Permanently Disable? __ Disable Following A Security Violation? y
(NOTE:  You must logoff to effect permanent disabling of Remote Access)
```

2. In the **TN** field, type the tenant partition number for the remote access extension. The system assigns the number 1 as the default tenant partition number.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to a user extension

To assign a tenant partition number to a user extension:

1. Type **change station *n***, where ***n*** is the extension to which you want to assign a tenant partition number. Press **Enter**.

   The system displays the Station screen (Figure 412: Station screen on page 1597).

Figure 412: Station screen

```
change station 30019                  STATION

Extension: 30019                        Lock Messages? n          BCC: 0
     Type: 4612                         Security Code: *           TN: 1
     Port: S04007                    Coverage Path 1:             COR: 1
     Name: station 30019             Coverage Path 2:             COS: 1
                                     Hunt-to Station:

STATION OPTIONS
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 30019
           Speakerphone: 2-way                Mute Button Enabled? y
       Display Language: english

                                                   Media Complex Ext:
                                                        IP SoftPhone? n
```

2. In the **TN** field, type the tenant partition number for the user extension.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to a terminating extension group

To assign a tenant partition number to a Terminating Extension Group (TEG):

1. Type **change term-ext-group *n***, where ***n*** is the terminating extension group number to which you want to assign a tenant partition number. Press **Enter**.

   The system displays the Terminating Extension Group screen (Figure 413: Terminating Extension Group screen on page 1598).

Figure 413: Terminating Extension Group screen

```
change term-ext-group                                        Page 1 of 1
                        TERMINATING EXTENSION GROUP

    Group Number: 1                              Group Extension:
      Group Name: 27 character                     Coverage Path:
   Security Code:                                           COR: 1
                                                            TN: 1
ISDN Caller Disp:                                 LWC Reception: none
      AUDIX Name:                           Messaging Server Name:

GROUP MEMBER ASSIGNMENTS

    Ext     Name                                Ext    Name
 1: 51001   27 character name sta 51001  3:
 2:                                       4: 51002  27 character name sta 51002
```

2. In the **TN** field, type the tenant partition number for the TEG. The system assigns the number 1 as the default for a tenant partition number.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to a trunk group

To assign a tenant partition number to a trunk group:

1. Type **change trunk-group *n***, where ***n*** is the trunk group number to which you want to assign a tenant partition number. Press **Enter**.

   The system displays the Trunk Group screen.
2. In the **TN** field, type the tenant partition number for the trunk group.
3. Press **Enter** to save your changes.

Assigning a tenant partition number to a vector directory number

To assign a tenant partition number to a vector directory number (VDN):

1. Type **change vdn *n***, where ***n*** is the VDN to which you want to assign a tenant partition number. Press **Enter**.

   The system displays the Vector Directory Number screen (Figure 414: Vector Directory Number screen on page 1599).

Figure 414: Vector Directory Number screen

```
change vdn 5000                                                  Page  1 of 1
                        VECTOR DIRECTORY NUMBER

                                Extension: 5000
                                     Name:
                           Vector Number: 234
                     Attendant Vectoring: n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                    COR: 59
                                     TN: 1
                               Measured: none
          Acceptable Service Level (sec):
           VDN of Origin Annc. Extension: 301
                               1st Skill:
                               2nd Skill:
                               3rd Skill:
```

2. In the **TN** field, type the tenant partition number for the VDN.
3. Press **Enter** to save your changes.

Assigning the sources of music for the tenant partitions

To assign the sources of music for the tenant partitions:

1. Type **change music-sources**. Press **Enter**.

   The system displays the Music Sources screen (Figure 415: Music Sources screen on page 1600).

Figure 415: Music Sources screen

```
change music-sources                                          Page 1 of X
                              Music Sources
               Source    Type      Port       Description

                 1      music      01A1003    Easy listening
                 2      tone                  Tone-on-Hold
                 3      music      01A1004    Rock
                 4      none
                 5      none
                 6      none
                 7      music      12B1301    Oldies
                 8      none
                 9      none
                10      none
                11      music      04C2003    Classical
                12      none
                13      none
                14      none
                15      none
```

The **Source** field is a display-only field.

Note that if the **Tenant Partitioning?** field on the Optional Features screen is set to **y**:

- The **Music/Tone on Hold** field on the Feature-Related System Parameters screen disappears.
- The value in the **Music/Tone on Hold** field on the Feature-Related System Parameters screen appears in the first **Source** field on the Music Sources screen.
- If the value in the **Music/Tone on Hold** field on the Feature-Related System Parameters screen contained **music**, the port address also appears on the ***Music Sources*** screen.

Note that when you change the **Tenant Partitioning?** field on the Optional Features screen from **y** to **n**:

- The **Music/Tone on Hold** field reappears on the Feature-Related System Parameters screen.
- The system displays the value from the Music Sources screen, in the **Music/Tone on Hold** field on the Feature-Related System Parameters screen.

2. In the **Type** field, perform one of the following actions:
   - If you want the users to hear music, type **music**.
   - If you want the users to hear the tone-on-hold tone, type **tone**.

     You can specify **tone** for only one music source.
   - If you want the users to hear nothing, type **none**.

3. In the **Port** field, type the auxiliary trunk address or the analog port address of the music source. You cannot enter duplicate addresses in the **Port** field.

   The system displays the **Port** field only if you typed **music** in the **Type** field.

4. In the **Description** field, type a maximum of 20 characters that describe the source of the music.

   The system displays the **Description** field, only if you typed **music** or **tone** in the **Type** field.

5. Press **Enter** to save your changes.

Reports for Tenant Partitioning

The following reports provide information about the Tenant Partitioning feature:

- None

Considerations for Tenant Partitioning

This section provides information about how the Tenant Partitioning feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Tenant Partitioning under all conditions. The following considerations apply to Tenant Partitioning:

- None

Interactions for Tenant Partitioning

This section provides information about how the Tenant Partitioning feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Tenant Partitioning in any feature configuration.

Tenant-partition identification is not passed between servers. A network of servers that run Communication Manager does not enforce Tenant Partitioning restrictions without special administration. For example, Tenant Partitioning on a network of servers that run Communication Manager does not enforce tenant-specific tie trunks.

Administration of the following features requires special care to avoid unintended access between tenants.

- Bridging
- Call Pickup
- Call Vectoring
- Controlled Restriction
- Facility Busy Indication
- Facility Test Calls
- Integrated Directory
- Inter-PBX Attendant Calls
- Main/Satellite/Tributary
- Malicious Call Trace
- Personal central office (CO) line
- Private Networking - Automatic Alternate Routing (AAR)
- Service Observing
- Uniform Dial Plan

Specific information about how the Tenant Partitioning feature interacts with other features follows.

- Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS)

  The Tenant Partitioning feature is not the same as the Time-of-Day Plan Numbers or the Partition Groups in AAR and ARS.

  However, if you use the Tenant Partitioning feature, you can use the Time-of-Day Plan Numbers and the Partition Groups in AAR and ARS.

- Attendant and Attendant Group features

  The Tenant Partitioning feature creates multiple attendant groups. Attendant operations such as direct-station or direct trunk group select (DTGS) are subject to tenant-to-tenant restrictions, both at selection time and at split time.

  All the calls that an attendant within an attendant group places on hold hear the music source from the attendant group.

- Attendant Control of Trunk Group Access

  An attendant group controls access to the trunk groups of the tenants that the attendant group serves. An attendant does not control access to any other trunk groups.

- CM Messaging

  The system applies the same tenant-to-tenant restrictions to CM Messaging voice and data ports that the system applies to any other endpoints.

  CM Messaging can restrict one group of subscribers from sending voice mail to another tenant partition group.

  Those who control the tenant partitions can:

  - Create 10 different communities within each CM Messaging
  - Allow voice message access across the community boundaries
  - Deny voice message access across the community boundaries

- Authorization Codes

  Authorization codes are associated with class of restriction (COR). If you want to assign a unique set of authorization codes to a tenant, you create a unique set of CORs. You only assign the CORs to objects that are within the partition that the tenant uses.

- Automatic Wakeup

  Those who control a tenant partition assign a music source to the partition. The system uses this music source as the wakeup music for users in the partition.

- Bridged Call Appearance

  Assign all stations with bridged call appearances to the same tenant.

- Call Coverage

  The tenant-to-tenant access restrictions apply to coverage paths. The system does not allow a call to cover to a tenant if the tenant-to-tenant access restrictions do not allow the user to call the tenant.

  When you specify an attendant in a coverage path, the system accesses the attendant group of the called tenant. The system does not access the attendant group of the calling tenant.

  When the system uses the Call Coverage feature for a call, and a user answers the call and then places the call on hold, the system plays the music-on-hold music that is assigned to the original called party.

- Call Detail Recording (CDR)

  CDR does not report the tenant partition number of the extension or the trunk group that the system uses. You must infer the tenant partition number from the extension or the trunk-group number.

- Call Pickup

  Assign all stations in a call-pickup group to the same tenant. The system supports Call Pickup only if the caller and the called party can both call the pickup user. The caller and the called party do not need to be in the same pickup group.

- Call Vectoring and Vector Directory Number (VDN)

  When the system routes a call to a new destination as a result of a vector step, the caller hears the music that is assigned to the last active VDN.

  While a call is in vector processing, the system uses the tenant number that is assigned to the active VDN, as determined by VDN Override, to select the music source for callers on hold. Note the following exception. If you use a **wait-time *<time>* hearing *<extension>* then *<treatment 2>*** command where the ***<extension>*** is a music source, that music source plays instead of the music source that is associated with the active VDN.

  The COR that is assigned to the VDN must allow music-on-hold.

- Call Management System (CMS)

  You can administer CMS to provide CMS reports to each tenant. You can restrict each CMS login to control, on a permission basis, only those entities that are assigned to a particular tenant. Outputs to separate printers allow any tenant to print their own CMS reports. The
  tenant-partitioning provider must administer CMS to provide this separation of tenant permissions.

- Dial Access to Attendant

  When a tenant dials an attendant, the tenant accesses the attendant group to which the tenant is assigned.

- Emergency Access to the Attendant

  When a tenant dials the emergency access, the tenant accesses the attendant group to which the tenant is assigned.

- Expert Agent Selection (EAS)

  The COR that you assign to the logical agent ID in the EAS system determines whether callers that are on hold hear music.The COR that you assign to the physical extension does not control whether callers that are on hold hear music.

- Hunt groups

  The tenant number that you assign to the hunt group extension determines the music source that the callers to the hunt group hear while the callers are in queue or on hold.

- Intercept Treatment

  When access to the attendant is designated as intercept treatment, the caller accesses the attendant group to which the caller is assigned.

- Malicious Call Trace (MCT)

  The system assigns MCT extensions to tenant partition 1 as the default for the system. If MCT is enabled, any user who has permission to call tenant partition 1 can use MCT.

- Multiple Listed Directory Numbers (LDNs)

  Assign a tenant partition to each LDN.

- Multiple Audio and Music Sources for Vector Delay

  When you specify the audio source by a **wait-time *<time>* hearing *<treatment>*** vector step, the audio source that is assigned to the tenant number of the active VDN is the audio source that plays.

  If you use a **wait-time *<time>* hearing *<extension>* then *<treatment 2>*** command where the ***<extension>*** is an audio source, that audio source plays instead of the audio source that is associated with the active VDN. For information on administering multiple audio sources, see the *Avaya Aura™ Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780.

- Music-on-Hold Access

  You can assign a unique source for music to each tenant.

- Night Service

  Each tenant can have a listed directory number (LDN) night destination, a trunk answer on any any station (TAAS) port, or a night attendant that only the tenant uses.

- PC Interfaces

  You must assign each PC interface to a tenant partition.

- PC/PBX Connections

  You must assign each PC/PBX Connection to a tenant partition.

- PC/ISDN

  You must assign each PC/ISDN to a tenant partition.

- Remote Access

  You must assign each remote access barrier code to a tenant.

- Traffic Studies

  Traffic studies do not report the tenant partition number of the extension or the trunk group. You must infer the tenant partition number from the extension or trunk-group number.

- Uniform Dial Plan (UDP)

  If a UDP is in place between servers, the system does not pass tenant partition identification between the servers. The system does not enforce tenant-partition restrictions between the servers unless you provide special administration.

  Tenant Partitioning restrictions do not override COR restrictions. COR restrictions are independent of tenant partitions.

Terminal Translation Initialization

Use the Terminal Translation Initialization (TTI) feature to merge an X-ported extension to a valid port, or to separate an extension from a port.

Detailed description of Terminal Translation Initialization

This section provides a detailed description of the Terminal Translation Initialization (TTI) feature.

Use TTI to:

- Merge an X-ported extension to a valid port. To merge an X-ported extension to a valid port, enter the system-wide TTI security code, and then the extension from a telephone that is connected to the valid port.
- Separate an extension from the port to which the extension is assigned. To separate the extension from the port, enter the required numbers. When you enter the required numbers, the extension is administered as an X port.

When TTI is enabled for voice, all voice ports, except Basic Rate Interface (BRI) ports, become TTI ports, or ports from which a TTI merge sequence can occur.

You usually use TTI to move telephones. However, you can also use TTI to connect and move attendants and data modules.

Attendant consoles

You must assign an extension to the attendant console, if you want the attendant to use TTI.

TTI port translations are the same for both digital telephones and attendant consoles. To merge a digital TTI voice port and an attendant console, you must:

1. Administer the attendant console as an X port.
2. Plug a digital telephone into the jack that is assigned to the attendant console.
3. Enter the TTI merge digit sequence at the digital telephone.
4. Unplug the digital telephone.
5. Plug the attendant console into the jack.

You can separate an attendant console from its port only through administration. A TTI separate request from an attendant console gives the user intercept treatment.

Note:
If you want to use TTI, you must assign a call appearance (call-appr) to the first button position. TTI needs the button on the first call appearance to get dial tone.

Data modules

The system provides status information during the TTI merge, and the separate operations on a telephone that is connected to a data module. If the **TTI State** field on the Feature-Related System Parameters screen is set to **data**, the system displays the status information. If the **TTI State** field on the Feature-Related System Parameters field is set to **voice**, the system generates tones to indicate status.

For a standalone data module, you enter the TTI merge and separate digit sequence on one line at a DIAL prompt:

- DIAL: ***<TTI feature access code><TTI security code><extension>***

The system does not generate separate prompts for the TTI security code and the extension.

Voice and data telephones

The system process a telephone with a data terminal (DTDM) as a telephone in the TTI merge and separation sequence operations. The DTDM is merged with and separated from its hardware translation at the same time that the telephone is merged or separated. You can start the TTI merge and separate sequence only through the telephone. You cannot start the sequences for DTDMs through the data port.

ISDN-BRI telephones

You use the same TTI separation sequence for Automatic-TEI SPID-initializing BRI telephones that you use for other telephones. However, the merge sequence is different.

Separation sequence

1. Feature access code (FAC)
2. Security code
3. Extension

Merge sequence

1. Connect the telephone to any port to get power.
2. Program the service profile identifier (SPID) to the extension with which the telephone is to be merged.
3. Unplug the telephone.

   You must unplug the telephone, even if the telephone is connected to the intended port.
4. Connect the telephone to the intended port.

   The intended port must indicate Equipment Type: TTI Port.
5. Listen for the dial tone.
   - If you hear dial tone, the merge is complete.
   - If you do not hear dial tone, the SPID of the telephone is an unavailable extension.

You can dial the TTI merge sequence for BRI telephones only if a user separates a BRI extension from its telephone, and then wants to reassociate the telephone to the same extension. Note that you cannot use the system access terminal (SAT) to put an **x** in the **Port** field of a BRI Station record that is still connected to the server that runs Communication Manager. You must use the TTI separation sequence from the telephone.

Analog queue warning ports and external alert ports

You can administer the analog queue warning port that is used for hunt groups, and the external alert port, with an **x** in the **Port** field. You can use TTI to merge these extensions to an analog port. You must perform the merge at an analog set, and then unplug the analog set from the port. You cannot use TTI to separate these extensions from their port location. A TTI separate request from one of these ports gives you intercept treatment.

Security

SECURITY ALERT:
If you do not manage TTI carefully, unauthorized use of this feature can cause you security problems. For example, someone who knows the TTI security code can disrupt normal business functions by separating telephones or data terminals. You can help protect against unauthorized use of TTI by frequently changing the TTI security code. To further enhance system security, remove the Feature Access Code (FAC) from the system when the FAC is not needed. Consult the *Avaya Products Security Handbook* for additional information to secure your system, and to find out about regularly obtaining updated security information.

Erase user data from DCP telephones

Beginning with Communication Manager Release 4.0, administrators can delete local information that is stored in a DCP telephone (2410 and 2420 sets only) when the telephone is reset by a PSA logoff or similar event. Depending on Communication Manager administration, this feature might eliminate the telephone's local speed dial lists, call logs, language, button labels or customized option settings that were defined by the user and may be of a personal nature.

System administrators are able to re-assign terminals without the need to send a technician to user's desk to manually erase the data.

Any of the following events can erase the following local data items from the 2420 and R2 of the 2410 DCP sets

- PSA disassociate & TTI unmerge
- Use by a Enterprise Mobility User (EMU) visiting extension
- A new **`erase terminal`** SAT command

Note:
Communication Manager does not erase data from an IP terminal upon receiving an unregistration request from the terminal. Avaya IP terminals do not allow users access to local terminal information while the terminal is unregistered.

To administer this feature, use the following fields on the Class of Restriction screen:

- Use the **ERASE 24xx USER DATA UPON Dissociate or unmerge at this phone** field to administer what local terminal data items are erased when the 24xx is dissociated or unmerged.

- Use the **Use the EMU login or logoff at this phone field** to administer what local terminal data items are erased upon Enterprise Mobility User (EMU) login or logoff.

For more information on the values and defaults for these fields, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

For more information on the new **`erase terminal`** SAT command, see *Maintenance Commands for Avaya Aura™ Communication Manager Media Gateways and Servers*, 03-300431.

Administering Terminal Translation Initialization

This section describes the screens that you use to administer the Terminal Translation Initialization feature.

Screens for administering Terminal Translation Initialization

Screen name	Purpose	Fields
Attendant Console	Define an attendant console.	All
Data Module	Define a data module.	All
Feature Access Codes (FACs)	Create FACs for the TTI merge and separate operations.	• **Terminal Translation Initialization Merge Code** • **Terminal Translation Initialization Separation Code**
Feature-Related System Parameters	Enable TTI for the system.	• **TTI Enabled** • **TTI State** • **TTI Security Code**
Station	Define a station.	All

Interactions for Terminal Translation Initialization

This section provides information about how the Terminal Translation Initialization feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Terminal Translation Initialization in any feature configuration.

- Attendant

  You can separate an attendant if the attendant is in Position Available Mode. However, you cannot separate an attendant if any calls are in the queue, held, or active for the attendant.

- Attendant Night Service

  You cannot separate the night service station, when the station is in night service.

- Attendant Release Loop Operation

  If the attendant separates before the attendant-timed reminder-interval expires, the system reclassifies all calls that are held with the release loop operation by the attendant as attendant group calls.

- Automatic Callback

  If you use TTI to separate either telephone that is part of Automatic Callback, the system breaks the automatic callback sequence.

- Call Coverage

  Send All Calls and Go to Coverage remain active, while the telephone has no associated hardware.

  You can separate a telephone that is the receiver of Send All Calls or Go to Coverage. The system processes calls to the telephone as if the telephone is busy.

- Call Coverage Answer Group

  If an extension that was an X port rejoins a call coverage answer group as a result of a TTI merge, the system excludes the extension from all transactions that are already active in the call coverage answer group.

- Call Forwarding

  You can separate a telephone while Call Forwarding is active. If a destination extension for call forwarding separates, Call Forwarding to that extension remains active. The system processes calls to the telephone as if the telephone is busy.

- Call Pickup

  If a line appearance is available, a member of a call pickup group can separate at any time. If a call is attempting to terminate, and a member of a group associates, that member does not join the group for the call that is currently in progress. The member can participate in all subsequent calls to the call pickup group.

- Expert Agent Selection (EAS)

  Station user records cannot be shared between **TTI** ports and Expert Agent Selection (EAS) login ID extensions. For example, if you administer 2,000 **EAS** login IDs, the maximum number of **TTI** ports that the system can provide is reduced by 2,000.

- Hunt Group Uniform Call Distribution (UCD) and Direct Department Calling (DDC)

  The system excludes telephones that are previously X-ported as a result of a **TTI separation request** from all transactions that are already active in the hunt group when the telephone is merged.

- Site Data

  If TTI is enabled, the system displays a warning message after you administer the **Site Data** fields.

  If TTI is enabled, and you change the **Port** field on the Station screen from **x** to a port number, and change the **Room**, **Jack**, or **Cable** fields in the **Site Data** section of the Station screen, the system displays a warning message when you tab off the fields.

- Terminating Extension Group (TEG)

  If any member of a TEG that was previously an X port as a result of TTI is merged, the member is excluded from all transactions that are already active in the TEG when the member is merged. The member can join all subsequent calls to the group.

Terminating Extension Group

Use the Terminating Extension Group (TEG) feature to allow an incoming call to ring as many as four telephones at one time. Any user in the group can answer the call.

Detailed description of Terminating Extension Group

This section provides a detailed description of the Terminating Extension Group (TEG) feature.

You can administer any telephone as a TEG member. However, only a multiappearance telephone can be assigned a **TEG** button with a merged-status lamp. With the **TEG** button, the user can select a TEG call appearance to answer or bridge onto an existing call, but not to originate the call. The TEG members are assigned on an extension number basis. Call reception restrictions applicable to the group are specified by the class of restriction (COR) for the group. The group COR takes precedence over an individual member’s COR. When a Terminating Extension Group (TEG) receives an incoming call, the TEG's primary Class of Restrictions (COR) is considered for the calling and called restrictions. The members could all be termination-restricted but still receive calls if the group is not restricted.

When a TEG members answers an incoming call, a temporary bridged appearance is maintained at the multiappearance telephones in the group. However, this appearance is not visible. Any TEG member can press the TEG button to bridge onto the call.

Administering Terminating Extension Group

This section describes the screens that you use to administer the Terminating Extension Group (TEG) feature

Screens for administering Terminating Extension Group

Screen name	Purpose	Fields
Terminating Extension Group	Define the groups for the TEG feature.	• **Coverage Path** • **Group Name** • **Group Extension** • **COR** • **TN** • **ISDN Call Display** • **Ext**

Considerations for Terminating Extension Group

This section provides information about how the Terminating Extension Group (TEG) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Terminating Extension Group under all conditions. The following considerations apply to Terminating Extension Group:

- A telephone user can be a member of more than one TEG, but can have only one **TEG** button for each group.
- A TEG can handle only one TEG call at a time. Additional calls do not reach the TEG. If a coverage path is assigned to the TEG, the system routes the additional calls accordingly.

Interactions for Terminating Extension Group

This section provides information about how the Terminating Extension Group (TEG) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Terminating Extension Group in any feature configuration.

- Automatic Callback

  This feature cannot be active for a **T**EG.

- Bridged Call Appearance

  Calls to a TEG cannot be bridged, except by way of a Temporary Bridged Appearance.

- Call Coverage

  A TEG can have a Call Coverage path assigned, but cannot be a point in a Call Coverage path.

  A **Send Term** button for the TEG can be assigned to group members who have multiappearance telephones. When a user presses Send Term, the system redirects calls to the TEG redirect to coverage. The merged status lamp lights on all telephones with a Send Term button. Any member with a Send Term button can press the button to deactivate Send Term. Incoming calls are directed to the group.

- Call Park

  A TEG call cannot be parked on the group extension. However, group members who answer a call can park a TEG call on their own extensions.

- Direct Department Calling (DDC) and Uniform Call Distribution (UCD)

  A TEG cannot be a member of a DDC or a UCD group.

- Internal Automatic Answer

  TEG calls are not eligible for Internal Automatic Answer. However, calls that are placed to an individual extension are eligible.

- Leave Word Calling (LWC)

  Leave Word Calling messages can be stored for a TEG. Any member of the group, covering user of the group, or system-wide message retriever can retrieve the stored messages. Phone Display and proper authorization can be assigned to the message retriever. Also, a remote Automatic Message Waiting lamp can be assigned to a group member to provide a visual indication that a message has been stored for the group. One indicator is allowed per TEG.

- Privacy - Manual Exclusion

  Privacy - Manual Exclusion can be assigned to any of the telephones in a TEG to prohibit bridging by other group members. A TEG member who attempts to bridge onto a call with Privacy - Manual Exclusion active is dropped.

- Temporary Bridged Appearance

  At multiappearance telephones in the TEG, a temporary bridged appearance is maintained after a call is answered. Thus, other members of the group can bridge onto the call.

Transfer

Use the Transfer feature to allow telephone users to transfer trunk calls or internal calls to other telephones or trunks without attendant assistance.

Detailed description of Transfer

This section provides a detailed description of the Transfer feature.

Transfer supports the following capabilities:

- Pull Transfer
- Abort Transfer
- Transfer Recall
- Transfer Upon Hangup
- Trunk-to-Trunk Transfer
- Outgoing Trunk to Outgoing Trunk Transfer
- Emergency Transfer
- Name Display on Unsupervised Transfer

Pull Transfer

Use Pull Transfer to allow either the transferring party or the transferred-to party to press the Transfer button to complete the transfer operation.

When attendants control calls, called parties cannot use Pull Transfer. Attendants who are called parties cannot use Pull Transfer. When attendants have parties on hold, the parties are transferred with the standard transfer process.

To use Pull Transfer, calling parties and called parties must be on the same server, or called parties must be reached by way of Italian TGU/TGE tie trunks.

Called parties who use analog telephones flash the switch hook, or press the flash key or recall button to transfer calls. Called parties who use digital telephones press the transfer key to complete transfers.

Abort Transfer

Use Abort Transfer to stop the transfer operation whenever a user presses a non-idle call appearance button in the middle of the transfer operation, or when the user hangs up. If both the **Abort Transfer** and **Transfer Upon Hang-Up** fields are set to **y** and you press the **transfer** button, and then dial the complete transfer-to number, hanging up the telephone transfers the call. You must select another non-idle call appearance to abort the transfer. If the **Transfer Upon Hang-Up** field is **y**, hanging up completes the transfer. Requires DCP, Hybrid, IP, ISDN-BRI or wireless telephones

Transfer Recall

Use Transfer Recall to return the unanswered transfer call back to the person who transferred the call.Transfer Recall uses a priority alerting signal. The display on the telephone also shows "rt," which indicates a returned call from a failed transfer operation.

Transfer Upon Hangup

Use Transfer Upon Hangup to hang up to transfer the call without the need to press the Transfer button a second time. You press the Transfer button, dial the number to which the call is being transferred, and then hang up.Transfer Upon Hangup is an optional capability at the system level. You can still press the transfer button a second time to transfer the call.

Trunk-to-Trunk Transfer

With Trunk-to-Trunk Transfer, an attendant or a user can connect an incoming trunk call to an outgoing trunk.

SECURITY ALERT:
Trunk-to-Trunk Transfer poses a significant security risk. Use this capability with caution.

The system provides three levels of administration for this Trunk-to-Trunk Transfer:

- Systemwide
- COR to COR
- COS

To administer Trunk-to-Trunk Transfer systemwide, complete the Feature-Related System Parameters screen. To restrict Trunk-to-Trunk Transfer on a trunk-group basis, assign COR-to-COR calling-party restrictions on the Class of Restriction screen. To allow individual users to control Trunk-to-Trunk Transfers, assign capabilities on the Class of Service screen.

Outgoing Trunk to Outgoing Trunk Transfer

With Outgoing Trunk to Outgoing Trunk Transfer (OTTOTT), a controlling party such as a station user or an attendant, initiates two or more outgoing trunk calls, and then connects the trunks. This operation removes the controlling party from the connection and conferences the outgoing trunks. The controlling party can also establish a conference call with the outgoing trunks, drop out of the conference, and leave only the outgoing trunks on the conference.

Note:

This capability is an optional enhancement to Trunk-to-Trunk Transfer and requires careful administration and use. The Distributed Communications System (DCS) Trunk Turnaround may be an acceptable and safer alternative to this feature.

With OTTOTT, you can establish calls in which the only parties involved are external to Communication Manager and are on outgoing trunks. This type of call can result in locked-up trunks, such as trunks that cannot be disconnected except by busying-out and releasing the affected trunk circuit. To clear the lockup, a service technician must reset the trunk board, or busy-out and release the affected trunk.

Emergency Transfer

Emergency Transfer provides service to and from the central office (CO) to the local telephone company during a power failure, or when service is impaired. Emergency Transfer is also called Power Failure Transfer.

With Emergency Transfer, users of the 500 type or 2500-type analog telephones can access the local CO and answer incoming calls during a power failure. Each server cabinet supports Emergency Transfer panels by way of the AUX connectors on the rear panel. The transfer is initiated when:

- A transfer panel or the associated cabinet loses power
- Someone manually activates the Emergency Transfer switch on the associated maintenance circuit pack
- The software determines that service for that cabinet is severely impaired

You cannot activate any other system features during a complete system power failure.

Emergency Transfer panels are available in multiples of five telephones. These telephones can either be pulse-dialing or touchtone telephones. You must use pulse dialing if the CO accepts only dial pulses. Each telephone can be connected to a separate CO.

When the system is not in Emergency Transfer mode, you can use the transfer telephones as regular telephones.

Name Display on Unsupervised Transfer

Communication Manager Release 4.0 or later displays transferred-to names on calls redirected with Call Transfer, in order to interoperate with the Tenovis I55. This enables sending the transferred-to station name (not answered enquire call) using the primary Private Integrated Network Exchange (PINX) after call transfer. The transferred-to name will appear on the calling station display after receiving the name in the primary PINX.

Previously, when transferring to a not answered connection (primary connection was established through QSIG) the redirection name was not sent in the FACILITY message independent from the value of the **Send Name** field on the trunk group associated with the primary PINX QSIG trunk. Therefore the name of the transferred-to station (enquiry call) did not appear immediately after call transfer on the display of the station in the primary connection.

Now, When Station A calls B, and is transferred to C, Station B has established a connection through QSIG to station A and an enquire connection (internal or through QSIG) to station C. Station B transfers station C to station A. The name of Station C (not answered enquire call) is sent after call transfer to station A (through QSIG to primary PINX) when the **Send Name** field on the Trunk Group screen is set to **y** at the QSIG trunk side to the primary PINX. So the name of the transferred-to station C appears on the display of the station A in the primary connection immediately after the call transfer.

To administer this capability, you must set the **QSIG value-added** field to **y** on the Trunk Group screen. This allows a match of the name and number on the extension.
In addition, on the Trunk Group screen, there is a new function for the **Send Name** field. The existing values **y**(es), **r**(estrict), and **n**(o) values now also control the sending of the name at the QSIG trunk side.

:**y** = send redirection Name

r, **n** = do not send redirection Name

For more information on these fields, see *Avaya Aura™ Communication Manager Screen Reference*, 03-602878.

Administering Transfer

This section describes the screens that you use to administer the Transfer feature.

Screens for administering Transfer

Screen name	Purpose	Fields
Feature-Related System Parameters	Define Transfer options	

Considerations for Transfer

This section provides information about how the Transfer feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Transfer under all conditions. The following considerations apply to Transfer:

- You can administer transferred trunk calls to receive either music or silence if the first part of the transfer places the call on hold.
- Multiappearance telephones must have an idle appearance to transfer a call.
- Single-line telephone users momentarily flash the switch hook or press the Recall button, dial the desired extension, and hang up. Multiappearance telephone users press the Transfer button, dial the desired extension, and press the Transfer button again.
- If, on the Feature-Related System Parameters screen, the **Transfer Upon Hang-up** field is set to **y**, users can transfer a call by press the Transfer button, dial the desired extension, and then hang up. Users can hang up while the desired extension is ringing or after the party has picked up. The user also can still press the Transfer button a second time to complete the transfer process.
- If, on the Feature-Related System Parameters screen, the **Abort Transfer** field is set to **y**, users press the Transfer button, dial the desired extension, and then hang up or select any non-idle call appearance. The user must press the Transfer button again to complete the process (see Note). If the user selects an idle call appearance, the transfer is still active.

Note:

If both the **Abort Transfer and Transfer Upon Hang-Up** fields are **y** and you press the Transfer button and then dial the complete transfer-to number, hanging up the telephone transfers the call.

- Users of Digital Communications Protocol (DCP), hybrid, and wireless telephones can transfer a call that is on hold without removing the call from hold. If only one call is on hold, no active call appearances exist, and call appearance is available for the transfer, the user can transfer the call simply by pressing the Transfer button. Communication Manager assumes that the transfer is for the call on hold, and the transfer feature works as usual.

  If more than one call is on hold, the user must make a call active in order to transfer it. If the user presses the Transfer button with two or more calls on hold, Communication Manager ignores the transfer attempt since it will not know which call the user wants to transfer. If there are calls on hold and an active call, pressing the Transfer button will start the transfer process for the active call.

- Communication Manager can be administered to display a confirmation message to users upon successful call transfers. The confirmation message is visible to users with DCP, Hybrid, wireless (except for 9601), or Integrated Services Digital Network-Basic Rate Interface (ISDN-BRI) display telephones. These telephones, except for the hybrids, can display the confirmation message in English, Spanish, French, Italian, or a language that you define. Hybrid telephones can display the message in English only.

- You can administer the system to return a transferred call to the originator if the transferred-to party does not answer within a set time limit. To do this, enter a value in the **Station Call Transfer Recall Timer** field on the Feature-Related System Parameters screen.

The following consideration is for Outgoing Trunk to Outgoing Trunk Transfer (OTTOTT):

- OTTOTT is not intended for use in DCS networks, since DCS Trunk Turnaround provides comparable capabilities much more safely. However, use of OTTOTT with DCS is not prohibited, and might be useful when one or more of the trunks goes off the DCS network.

The following considerations are for Trunk to Trunk Transfer:

- Trunk-to-Trunk Transfer is particularly useful when a caller outside the system calls a user or attendant and requests a transfer to another outside number. For example, a worker, away on business, can call in and have the call transferred elsewhere.

- Transferred trunk calls can be administered to receive either music or silence.

- Some CO trunks do not signal the PBX when the CO user disconnects from a call. The system ensures that incoming CO trunks without Disconnect Supervision are not transferred to outgoing trunks or to other incoming CO trunks without Disconnect Supervision.

- An attendant-assisted call connecting an outgoing trunk or incoming trunk without Disconnect Supervision to an outgoing trunk must be held on the console. The system does not allow the attendant to release the call. The attendant can, however, use the Forced Release button and disconnect all parties associated with the call.

- If a user has connected two outgoing trunks or an outgoing call and an incoming call without Disconnect Supervision, the user must remain on the call. Otherwise, the call is dropped. An incoming trunk with Disconnect Supervision can be connected to an outgoing trunk without the user remaining on the call. An incoming trunk can also be connected to another incoming trunk without the user remaining on the call if one of the incoming trunks has Disconnect Supervision.

Interactions for Transfer

This section provides information about how the Transfer feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Transfer in any feature configuration.

- Analog Station Recall Operation and Feature Activation

  When called parties initiate either analog-telephone recall or feature activation, callers are not put on hold for transfer. Instead, callers are transferred by way of Pull Transfer.

- Basic Rate Interface (BRI) telephones

  Callers who use BRI Stations reach desired parties through the intermediate step of calling a party who calls a final destination. Intermediate parties activate pull transfer to complete transfers. Final called parties go off hook as if a new transfer were originated.

- Call Detail Recording (CDR)

  The software checks to ensure that calls are correctly recorded with CDR when Pull Transfer is completed.

- Digital Station Transfer Operation

  When called parties initiate transfer operations, callers are not put on hold for transfer; they are transferred by way of Pull Transfer.

- Non-BRI telephones:

  Callers who use the non-BRI telephones reach desired parties through an intermediate step of calling a party who calls a final destination. Each called party activates pull transfer.

The following interactions are for Outgoing Trunk to Outgoing Trunk Transfer (OTTOTT):

- DCS Trunk Turnaround

  OTTOTT increases the set of cases in which DCS Trunk Turnaround can be accepted. However, use of OTTOTT in combination with a DCS network is strongly discouraged. The following algorithm describes the DCS Trunk Turnaround request process.

  – If any party on the call receives a local-dial, busy, intercept, or reorder tone, deny turnaround.If any remaining party is an answered station or attendant, accept turnaround.

  - If any remaining party is on an incoming trunk, accept turnaround. For the purposes of this check, an outgoing DCS trunk that has been turned around an odd number of times by way of a DCS trunk turnaround is considered an incoming trunk with disconnect supervision. Similarly, an incoming DCS trunk that has been turned around an odd number of times is considered an outgoing trunk.
  - If any remaining party is an outgoing trunk administered for OTTOTT that has received answer supervision, accept turnaround.
  - If any remaining party is an outgoing DCS trunk, forward the turnaround request.
  - If any remaining party is not a DCS trunk, deny turnaround.

- Incoming Disconnect Supervision

  Outside of the US, incoming disconnect supervision is a switching capability that restricts transfers or conferences for certain incoming trunks. In the U.S., all incoming trunks are assumed to provide disconnect supervision. In some countries, this assumption is not valid. Therefore, you must administer whether or not an incoming trunk provides disconnect supervision for each trunk group.

- Personal Central Office Lines (PCOLs)

  Transfer of PCOLs is not subject to the normal restrictions that are applied to transfer of other trunks. These transfers are allowed since the PCOL appearance remains on one or more stations as a feature button. System users must be aware that the DROP button cannot be used to disconnect the transferred-to party from the call. Therefore, if an outgoing PCOL is transferred to an outgoing trunk and neither of the trunks can supply a disconnect signal, the two trunks lock up.

- QSIG Global Networking

  If either call is over an ISDN-PRI trunk that is administered with Supplementary Service Protocol b (QSIG), the system might display additional call information.

- Release-Link Trunks (RLT)

  RLTs are used by CAS. An outgoing RLT at a remote branch is used to access an attendant at the main. The attendant at the main can transfer the incoming caller to a station or a trunk at the branch. The RLT is typically used only for a short period of time and is usually idled after the transfer is established.

  A station at a branch can transfer an outgoing trunk to the attendant at the main. This transfer could be viewed as an OTTOTT (the attendant is accessed by way of an outgoing RLT). Since administering outgoing disconnect supervision for RLT trunks provides no additional capability, this administration is not provided for RLT trunks.

- Restriction

  Restrictions on the transferring party can block a transfer or a drop operation even when Outgoing Disconnect Supervision is provided.

- Trunk-to-Trunk Transfer

  If this feature-related system parameter is set to Restricted, all trunk-to-trunk transfer or release, or drop operations for public trunks (CO, CPE, CAS, DID, DIOD, FX, and WATS) have calls terminated or receive denial. If the parameter is set to None, all trunk-to-trunk transfers (except CAS and DCS) have calls terminated or receive denial.

  Hence, you use All to enable OTTOTT operation for these types of trunks. The number of public network trunks allowed on a conference call is administrable. This number defaults to 1, so if OTTOTT is being used to connect two or more public network trunks, you must increase this limit on the Feature-Related System Parameters screen.

- Trunks (CO, FX, and WATS)

  You cannot have two CO, FX, or WATS trunks in a OTTOTT connection, even if the **Disconnect Supervision - Out** field is set to **y**.

The following interactions are for Trunk to Trunk Transfer:

- Attendant Lockout

  Attendant Lockout does not function on Trunk-to-Trunk Transfer.

- Call Vectoring

  Station control of Trunk-to-Trunk Transfer does not affect routing of incoming trunks to a vector directory number (VDN) that ultimately routes to a destination off-net.

  A route to a number off-switch does *not* require you to enable trunk-to-trunk transfer.

- Tenant Partitioning

  Station control of Trunk-to-Trunk Transfer is prohibited between trunks in different tenant partitions if those partitions are restricted.

The following interaction is for Emergency Transfer:

- Night Service

  If a power failure occurs when the system is in night service, the system automatically returns to night service when power is restored.

Trunk Flash

Use the Trunk Flash feature to allow a user of a multifunction telephone or an attendant console to access far-end customized services or central office (CO) customized services.

Detailed description of Trunk Flash

This section provides a detailed description of the Trunk Flash feature.

With Trunk Flash, a user of a multifunction telephone or an attendant console can gain access to far-end customized services or central office (CO) customized services. To use Flash Trunk, the user presses the flash button or dials the Feature Access Code (FAC) for Trunk Flash.

CO customized services are electronic features, such as conference and transfer, that are accessed by a sequence of flash signal and dial signals from a Communication Manager telephone on an active trunk call. The Trunk Flash feature can help to reduce the number of trunk lines that are connected to the server that runs Communication Manager by performing:

- Trunk-to-trunk call transfers at the far-end or the CO, which eliminates the use of a second trunk line for the duration of the call, and frees the original trunk line for the duration of the call.
- A conference call with a second outside call party, which eliminates the need for a second trunk line for the duration of the call.

Note:

Some analog dual-tone multifrequency (DTMF) telephone sets that are used in Italy and the United Kingdom have a Flash button. When a user presses that Flash button, the button generates a rotary digit 1. When an analog telephone that is administered as a DTMF telephone, for example, as a 2500 or a 71nn-type telephone, transmits a rotary digit 1, the system processes the signal as a recall signal from the telephone set to Communication Manager.

A centralized attendant service (CAS) attendant who is connected to a release line trunk (RLT), the Flash button controls certain CAS features at the branch. For a user of a multifunction telephone or non-CAS attendant connected to a CO, foreign exchange (FX), or a Wide Area Communications Service (WATS) trunk, the flash controls certain features, such as add-on, at the connected CO.

Trunk Flash is not available on Personal Central Office Line (PCOL) groups.

The system supports the Trunk Flash signal for incoming, outgoing, or two-way call directions on selected two-wire analog or digital DS1 trunks, or tie trunks on DS1.

If the trunk group is a DS1 trunk in Italy, the Trunk Flash feature applies only to outgoing calls.

If the trunk is not directly connected to the far-end or the CO that provides the customized services, use of the Trunk Flash signal can cause the far end or the CO to disconnect the call.

The system does not record Call Detail Recording (CDR) information for calls that a user makes with the Trunk Flash feature.

Administering Trunk Flash

This section describes the screens that you use to administer the Trunk Flash feature.

Screens for administering Trunk Flash

Screen name	Purpose	Fields
Feature Access Code (FAC)	Assign a FAC for Trunk Flash.	**Flash Access Code**
Trunk Group	Enable Trunk Flash for the trunk group.	**Trunk Flash**

End-user procedures for Trunk Flash

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Trunk Flash:

- Using Trunk Flash

To use Trunk Flash, perform one of the following actions:

- Press the Flash button.
- Dial the FAC for Trunk flash.

Considerations for Trunk Flash

This section provides information about how the Trunk Flash feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Trunk Flash under all conditions. The following considerations apply to Trunk Flash:

CAUTION:
The Trunk Flash feature allows the telephone user to receive central office (CO) dial tone. A user can place a call that is not monitored by Communication Manager, and is not subject to restrictions such as toll, facilities restriction level (FRL), and class of restriction (COR). Use caution when you enable this feature.

- A Trunk Flash button can be assigned on CAS attendant consoles, non-CAS attendant consoles, and multifunction telephones. For CAS attendants, use of this button is limited to certain CAS features by way of RLT trunks. For multifunction and non-CAS attendant consoles, this button is used for the Trunk Flash feature.
- FAC activation of the trunk flash feature is allowed.
- System features, such as internal conference call, transfer, and call par, can be combined with custom services. The custom services are CO-based features that are activated/ controlled by sending a flash signal over the trunk to the CO. However, mixing Communication Manager features with custom services causes complications for the user when the user tracks a call. Communication Manager cannot give the local telephone user status information on the custom services.
- The Trunk Flash feature can only be accessed if the call has only one trunk. The trunk must be an outgoing trunk and the **Trunk Flash** field on the Trunk Group screen must be set to **y**. The Trunk Flash feature is disabled when the call involves more than one trunk, even if all the trunks have Trunk Flash enabled.
- The system allows five users to participate in a conference call with the trunk line party. However, to access the Trunk Flash feature, at least one of the user telephones must have a Flash button.
- With a call that involves more that one user, one of the users can press the Flash button, and another user can dial the telephone number. The user that dials the telephone number is not required to have a telephone with a Flash button.

  If the far-end or the central office (CO) does not support custom services, the far-end or the CO can ignore the call or drop the call. If the far-end or the CO ignores or drops the call, the user might hear a clicking sound or the user might hear silence.

Uniform Dial Plan

Use the Uniform Dial Plan (UDP) feature to share a common dial plan among a group of servers. The UDP applies both interserver dialing and intraserver dialing. The UDP provides the dial plans from 3 to 18 digits.

UDP provides extension-to-extension dialing between two or more private-switching systems.

You can use UDP with the following entities:

- Main servers
- Tributary servers
- Satellite servers
- Electronic Tandem Networks (ETN)
- Distributed Communication Systems (DCS)

Note:
You must use a 4-digit dial plan or a 5-digit dial plan for DCS.

Detailed description of Uniform Dial Plan

This section provides a detailed description the Uniform Dial Plan (UDP) capability.

The software uses the UDP to route a call off the local server. The user dials an extension that consists of 3 to 18 digits. The software converts the extension that the user dials into a private-network number or a public network number.

To convert the extension, the software substitutes digits at the front of the extension that the user dials. The software supports the following types of extension conversions:

- Automatic Alternate Routing (AAR)

  The system uses AAR routing information to route calls within your company over your own private network.

  The software converts the number that the user dials. The software then analyzes the number, and routes the call as a private-network call.

- Automatic Route Selection (ARS)

  The system uses ARS routing information to route calls that go outside your company over public networks. The system also uses ARS routing information to route calls to remote company locations if you do not have a private network.

  The software converts the number that the user dials. The software then analyzes the number, and routes the call as a public network call.

- Extension number portability (ENP)

  If you want calls on your system to use ENP conversion, you must specify a node number. The software uses the node number to determine the routing pattern for the call. If the user dials an extension that consists of 4 to 6 digits, the software chooses an ENP code that is based on the first 1 or 2 digits of the extension. The software does not use the ENP code for routing. Therefore the ENP code is independent of location.

- Extension (EXT)

  The system uses EXT conversion to analyze the extension that the user dials.

  Unlike AAR conversion or ARS conversion, the system might not change the extension that the user dials, before the system routes the call. If no UDP entry for a particular extension or for a range of extensions exists, the system considers the extensions to be local extensions.

You specify a UDP for individual extensions or groups of extensions that have the same leading digits. For example, if you use a 5-digit UDP, and choose a matching pattern of "123," all 5-digit extensions that begin with "123" have the same UDP conversion scheme. If you use a 5-digit UDP, and want the software to use the UDP for only one extension, you must create a matching pattern that is the same as the extension. For example, if you choose a 5-digit UDP for extension 12345, you must specify 12345 as the matching pattern.

Each user extension can be assigned to one of the following six treatments:

- UDP Code
  - Conversion to AAR with a given location code
  - Further conversion is suppressed
- AAR Code
  - Conversion to AAR with a given location code
  - Further conversion is suppressed
- ENP Code
  - Conversion to a private-network number
  - Route to the given node number routing
- Temp OOS
  - Temporarily out of service
  - Give reorder

- Local

  Local range of extensions

- Blank

  This treatment is similar to local, but the system bypasses the when you perform an **add station** command.

When a user dials an extension that is on a server that is included in a UDP, the software firsts determines if the extension is assigned to a local station on the server. If the extension is assigned to a local station on the server, the software routes the call to the station. The software does not convert the extension numbers.

When a user dials an extension that is not on the server, the software compares the extension with the matching patterns. If the software finds a match between the extension and the matching patterns, the software converts the extension into a private network number. The software then routes the call as specified by the conversion.

When a user dials an extension, and the extension matches more than one matching pattern, the software selects the pattern that has the most matching digits. The software compares the extension and the matching pattern starting with the first digits that the user dials through to the last digits. See Table 120: Matching pattern selections on page 1635, for examples of matching patterns.

If the extension does not match a matching pattern, and Extended Trunk Access (ETA) is enabled on the system, the software uses ETA to route the call. If the extension does not match a matching pattern, and ETA is not enabled on the system, the user receives intercept treatment.

Table 120: Matching pattern selections

Extension dialed	Matching patterns available	Matching pattern selected
123	123 and 1234	123
12345	123 and 1234	1234
12355	123 and 1234	123

Uniform Dial Plan example

The section contains an example of UDP administration, and the processing of several calls that use UDP.

To administer UDP, you must assign each UDP code:

- To a private network location code (RNX) or node number. The RNX is equivalent to the office code of a central office (CO) in a public network. This RNX determines how the system routes a UDP call.

- As either local or remote to Communication Manager.

The same 5-digit extension is used to call a station, regardless of where in the electron tandem network (ETN) that call originates. This example includes three media servers or switches (Table 121: RNX and UDP codes on page 1636). Each media server and switch has a list of RNX and UDP codes.

Table 121: RNX and UDP codes

Media server or switch	RNX code	UDP code
A	224	41
C	223	51
C	223	52
B	222	60
B	222	61

See Figure 416: UDP Example on page 1637 for an example of a UDP scenario.

Figure 416: UDP Example

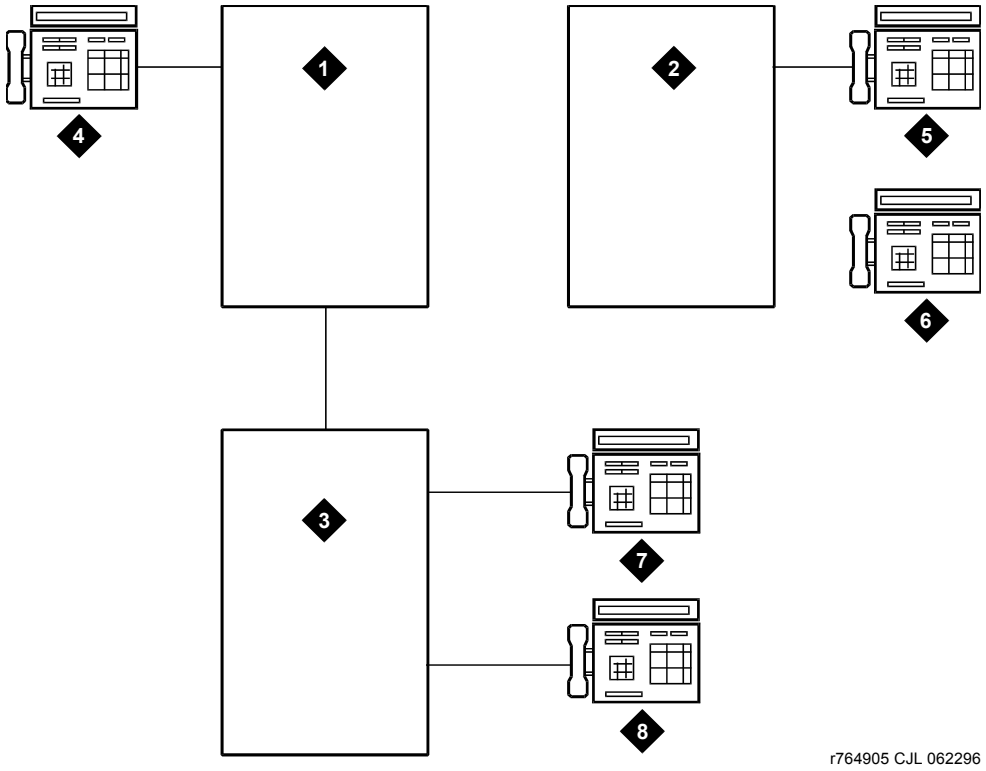


Figure notes:

1. System A.
   The dial plan for the extensions is 41. The RNX is 224.
2. System B.
   The dial plan for the extensions is 60 and 61. The RNX is 222.
3. System C.
   The dial plan for the extensions is 51 and 52. The RNX is 223.
4. Extension 41000
5. Extension 61234
6. Extension 60123
7. Extension 51234
8. Extension 5200

A user at extension 41000 who wants to call extension 61234, has one of the following options:

- Dial 61234
- Dial the AAR access code, and then dial 222-1234

If the user dials 61234, the system:

- Recognizes 61 as a remote UDP
- Determines that the associated RNX is 222
- Uses AAR to route the call to 222-1234

If the user dials the AAR access code and 222-1234, the system:

- Finds the route pattern for RNX 222

- Routes the call to the server that is associated with that RNX

When the software uses UDP to route a call to another server or system, the route pattern provides the correct digit deletion and insertion instructions. The receiving system then gets numbers in the format that the receiving system expects.

You can configure the software several different ways.

- If AAR is available on the receiving media server or switch:
  - Subnetwork trunking can be used to insert the Feature Access Code (FAC) for AAR on the server or switch where the call originates
  - Digit insertion can be used to insert the FAC for AAR on the receiving server

  The receiving server uses AAR digit conversion to delete 3 digits and add the digit 6, thus converting the number 222 with 7 digits to an extension.
- If AAR is unavailable on the receiving media server or switch, subnetwork trunking must be used on the originating server or switch to delete the 222 and insert the digit 6 at the start of the extension number. This conversion ensures that the receiving server can continue to route the call correctly.

If the user at extension 51234 on media server C dials extension 61234, the call must first go through media server A before the call goes to media server B. When the user dials 61234:

- The software recognizes 61 as a UDP code.
- The software determines that the associated RNX is 222, and uses the AAR feature to route the call.
- The FAC for AAR plus the digits 222-1234 are outpulsed to media server A.
- Media server A then recognizes the RNX 222 as a remote server or switch, and routes the call to media server B and extension 61234.

This same type of call routing occurs when an extension at media server B calls an extension at media server C.

If extension 61234 on media server B calls extension 60123, the software recognizes 60 as a local UDP code, and the system routes the call directly to extension 60123.

Administering Uniform Dial Plan

The following steps are part of the administration process for the Uniform Dial Plan (UDP) capability:

- Administering the Uniform Dial Plan table on page 1641
- Administering the Node Number Routing Table on page 1643
- Administering the AAR Digit Conversion Table on page 1644

- Administering the ARS Digit Conversion Table on page 1645
- Administering the AAR Digit Analysis Table on page 1647
- Administering the ARS Digit Analysis Table on page 1650
- Administering the extension number portability numbering plan on page 1653

This section describes:

- Any prerequisites for administering the Uniform Dial Plan capability
- The screens that you use to administer the Uniform Dial Plan capability
- Complete administration procedures for the Uniform Dial Plan capability

Prerequisites for administering Uniform Dial Plan

You must complete the following actions before you can administer the Uniform Dial Plan (UDP) feature:

- Ensure that the Uniform Dial Plan feature is enabled on your system.
- Ensure that a Feature Access Code (FAC) for Automatic Alternate Routing (AAR) and a FAC for Automatic Route Selection (ARS) are available on your system.

To ensure that the Uniform Dial Plan feature is enabled on your system:

- On the Optional Features screen, ensure that the **Uniform Dialing Plan** field is set to **y.** If the **Uniform Dialing Plan** field is set to **n**, your system is not enabled for the Uniform Dial Plan feature. Contact your Avaya representative for assistance before continuing with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

To ensure that FACs for AAR and ARS are available on your system:

1. Type **`change feature-access-codes`**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 417: Feature Access Code (FAC) screen on page 1640).

Figure 417: Feature Access Code (FAC) screen

```
                      FEATURE ACCESS CODE (FAC)

         Abbreviated Dialing List1 Access Code: *00
         Abbreviated Dialing List2 Access Code: *01
         Abbreviated Dialing List3 Access Code: *02
Abbreviated Dial - Prgm Group List Access Code: *03
                      Announcement Access Code: *04
                       Answer Back Access Code: *05

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: *9    Access Code 2: 9
                Automatic Callback Activation: *06    Deactivation: #06
Call Forwarding Activation Busy/DA: *07    All: *08    Deactivation: #09
                         Call Park Access Code: *10
                       Call Pickup Access Code: *11
CAS Remote Hold/Answer Hold-Unhold Access Code: *50
                  CDR Account Code Access Code: *12
                        Change COR Access Code:
                   Change Coverage Access Code: *13
                   Contact Closure   Open Code:          Close Code:
                   Contact Closure  Pulse Code:
```

2. In the **Auto Alternate Routing (AAR) Access Code** field and the **Auto Route Selection (ARS)** field, perform one of the following actions:
   - If the **Auto Alternate Routing (AAR) Access Code** field and the **Auto Route Selection (ARS)** field each contain a FAC**,** press **Cancel**.
   - If the **Auto Alternate Routing (AAR) Access Code** field or the **Auto Route Selection (ARS)** field do not contain a FAC, type a FAC in the field. Press **Enter** to save your changes.

   For more information on Feature Access Codes, including information on how to change or deactivate a FAC, see the "Feature Access Code" feature description.

Screens for administering Uniform Dial Plan

Screen name	Purpose	Fields
Uniform Dial Plan Table	Define the type of conversion, the matching pattern, and the insertion digits.	All
AAR Digit Analysis Table	Define Automatic Alternate Routing (AAR) digit analysis.	All

Screen name	Purpose	Fields
ARS Digit Analysis Table	Define automatic route selection (ARS) digit analysis.	All
AAR Digit Conversion Table	Define AAR digit conversion.	All
ARS Digit Conversion Table	Define ARS digit conversion.	All
Extension Number Portability (ENP) Numbering Plan	Define ENP codes.	All
Number Node Routing	Associate a route pattern with each node in the ENP subnetwork.	**Route Pat**
Route Pattern	Define the route pattern.	All
Optional Features	Ensure that the Uniform Dial Plan feature is enabled on your system.	**Uniform Dialing Plan**

Administering the Uniform Dial Plan table

Beginning with Communication Manager Release.4.0, the Dial Plan was expanded to accept digits up to 13 digits. On the Uniform Dial Plan Table screen,

- The **Matching Pattern** column is expanded to 13 digits.
- The maximum value in the **Len** field is increased to 2 digits. The values are 1-18.
- The maximum value in the **Del** field is increased. The values are 0-9.
- The **Insert Digits** column is expanded to 10 digits.
- The maximum value following an “L” entry in the **Insert Digits** column is increased from 5 to 11. (That is, valid entries are L1, L2, L3, …, L9, L10, L11.)

To administer the Uniform Dial Plan Table for your system:

1. Type **`change uniform-dial plan n`**, where ***n*** is the number of the dial plan that you want to administer. Press **Enter**.

   The system displays the Uniform Dial Plan Table screen (Figure 418: Uniform Dial Plan Table screen on page 1642).

Figure 418: Uniform Dial Plan Table screen

```
display uniform-dialplan 1                                          Page 1 of x
                              UNIFORM DIAL PLAN TABLE

Matching Pattern Len Del Insert Digits Net Conv Node Num
1234567890123    12  1   1234567890    123 n    123
```

Field	Description
Len	Accepts values 1-18
Del	Accepts values 0-9

2. In the **Matching Pattern** field, type the number that you want the software to match to the number that a user dials. Valid values are the digits 0 through 9. You can type a maximum of 7 digits.
3. In the **Len** field, type the number of digits of the user-dialed number, that the software analyzes when the software compares the user-dialed number with the numbers in the matching pattern field. Valid values are the digits 3 through 7.
4. In the **Del** field, type the number of digits that the software deletes before the software routes a call. Valid values are the digits 0 through 3. The number that you type must be less than, or equal to, the number that you type in the **Len** field.
5. In the **Insert Digits** field, type the digits that the software uses to replace the digits that the software deletes from the user-dialed number. If you want the software to delete the digits instead of to replace the digits, leave the **Insert Digits** field blank. Valid values are the digits 0 through 9. You can type a maximum of 4 digits.
6. In the **Net** field, type the server or the system network that the software uses to analyze the number that the software converts. Perform one of the following actions:
   - If you want the software to route the converted digit-string as an extension, type **ext**.
   - If you want the software to route the converted digit-string as its converted AAR address, type **aar**.
   - If you want the software to route the converted digit-string as its converted ARS address, type **ars**.
   - If you want the software to route the converted digit-string as its ENP node number, type **enp**.

     If you type **enp**, you must:

     — Type the extension number portability (ENP) node number in the **Node Number** field.

     — Leave the **Insert Digits** field blank. Type **n** in the **Conv** field.

7. In the **Node Num** field, type the ENP node number. Valid values are the digits 1 through 999.
8. In the **Conv** field, perform one of the following actions:
   - If you want additional digit conversion, type **y**.
   - If you do not want additional digit conversion, type **n**.

Note:
The **Percent Full** field displays the percent of the allocated uniform dial plan data resources that are currently used. You cannot change this field.

9. Press **Enter** to save your changes.

Administering the Node Number Routing Table

To administer node number routing for your system:

1. Type **`change node-number routing n`**, where ***n*** is the number of the node. Press **Enter**.

   The system displays the Node Number Routing screen (Figure 419: Node Number Routing screen on page 1643).

Figure 419: Node Number Routing screen

```
                          NODE NUMBER ROUTING
                        Partitioned Group Number:  1

    Route      Route      Route      Route      Route      Route      Route
     Pat        Pat        Pat        Pat        Pat        Pat        Pat

            15:        30:        45:        60:        75:        90:
 1:         16:        31:        46:        61:        76:        91:
 2:         17:        32:        47:        62:        77:        92:
 3:         18:        33:        48:        63:        78:        93:
 4:         19:        34:        49:        64:        79:        94:
 5:         20:        35:        50:        65:        80:        95:
 6:         21:        36:        51:        66:        81:        96:
 7:         22:        37:        52:        67:        82:        97:
 8:         23:        38:        53:        68:        83:        98:
 9:         24:        39:        54:        69:        84:        99:
10:         25:        40:        55:        70:        85:
11:         26:        41:        56:        71:        86:
12:         27:        42:        57:        72:        87:
13:         28:        43:        58:        73:        88:
14:         29:        44:        59:        74:        89:
```

2. In the **Route Pat** field, type the number of the routing pattern that you want to use.

3. Press **Enter** to save your changes.

Administering the AAR Digit Conversion Table

To administer the AAR Digit Conversion Table for your system:

1. Type **change aar digit-conversion *n***, where ***n*** is the number of the AAR Digit Conversion Table. Press **Enter**.

   The system displays the AAR Digit Conversion Table screen (Figure 420: AAR Digit Conversion Table screen on page 1644).

Note:
The system sorts the screen information by matching pattern. The software displays numbers first, followed by characters in alphabetical order.

Figure 420: AAR Digit Conversion Table screen

```
                    AAR DIGIT CONVERSION TABLE
                              Location: all
                                                    Percent Full: 0

Matching Pattern     Min   Max   Del   Replacement String   Net  Conv ANI Req

1                    4     28    0                          ars   y       n
3035385157           10    10    5     962                  aar   n       n
7                    5     5     0                          ext   n       n
x11                  3     3     0                          ars   y       n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
                                                                         n
```

2. In the **Matching Pattern** column, type the number that you want the system to match to the numbers that the user dials. If you require a prefix digit of 1 for 10-digit DDD, start the matching pattern with a 1. Valid values are the digits **0** through **9**.

   You can type a maximum of 18 digits. You can also type an asterisk (*), a lower case **x**, or an upper case **X** as wildcard characters.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are any number from **1** up to the number that you typed in the **Max** column.
4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are from the number that you typed in the **Min** column to **28**.
5. In the **Del** column, type the number of digits that you want the system to delete from the beginning of the dialed string. Valid values are the digits **0** up to the number that you typed in the **Min** column.
6. In the **Net** column, type the initials of the call-processing server network that the system uses to analyze the converted number.
7. In the **Conv** column, perform one of the following actions:
   - If you want additional digit conversion, type **y**.
   - If you do not want additional digit conversion, type **n**.
8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen.

   If the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:
   - If you require ANI on incoming R2-MFC or Russian MF ANI calls, type **y**.
   - If you do *not* require ANI on incoming R2-MFC or Russian MF ANI calls, type **n**.
   - If the **Allow ANI Restriction on AAR/ARS** field is set to **y** on the Feature-Related System Parameters screen, type **r**. When you set the **ANI Req** field to **r**, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an **r** entry in the **ANI Req** field as a **y**.

   The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.
9. Press **Enter** to save your changes.

Administering the ARS Digit Conversion Table

To administer the ARS Digit Conversion Table for your system:

1. Type **`change ars digit-conversion n`**, where ***n*** is the number of the ARS Digit Conversion Table. Press **Enter**.

   The system displays the ARS Digit Conversion Table screen (Figure 421: ARS Digit Conversion Table screen on page 1646).

Figure 421: ARS Digit Conversion Table screen

```
                    ARS DIGIT CONVERSION TABLE
                              Location: all                Percent Full: 0

 Matching Pattern     Min   Max   Del   Replacement String   Net  Conv ANI Req

 3035385157           10    10    6     962                  aar   n       n
 70555                5     5     5     13035381811          ars   n       n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
                                                                          n
```

2. In the **Matching Pattern** column, type the number that you want the system to match to the numbers that the user dials. If you require a prefix digit of 1 for 10-digit DDD, start the matching pattern with a 1. Valid values are the digits **0** through **9**.

   You can type a maximum of 18 digits. You can also type an asterisk (*****), a lower case **x**, or an upper case **X** as wildcard characters.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are any number from **1** up to the number that you typed in the **Max** column.

4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are from the number that you typed in the **Min** column to **28**.

5. In the **Del** column, type the number of digits that you want the system to delete from the beginning of the dialed string. Valid values are the digits **0** up to the number that you typed in the **Min** column.

6. In the **Net** column, type the initials of the call-processing server network that the system uses to analyze the converted number.

7. In the **Conv** column, perform one of the following actions:

   - If you want additional digit conversion, type **y**.
   - If you do not want additional digit conversion, type **n**.

8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen.

   If the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:

   - If you require ANI on incoming R2-MFC or Russian MF ANI calls, type **y**.
   - If you do not require ANI on incoming R2-MFC or Russian MF ANI calls, type **n**.
   - If the **Allow ANI Restriction on AAR/ARS** field is set to **y** on the Feature-Related System Parameters screen, type **r**. When you set the **ANI Req** field to **r**, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an **r** entry in the **ANI Req** field as a **y**.

   The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.

9. Press **Enter** to save your changes.

Administering the AAR Digit Analysis Table

To administer the AAR Digit Analysis Table for your system:

1. Type **`change aar analysis n`**, where ***n*** is the number of the AAR Digit Analysis Table. Press **Enter**.

   The system displays the AAR Digit Analysis Table screen (Figure 422: AAR Digit Analysis Table screen on page 1647).

Figure 422: AAR Digit Analysis Table screen

```
AAR DIGIT ANALYSIS TABLE
                                  Location:  all           Percent Full:    2

          Dialed           Total      Route    Call    Node  ANI
          String          Min  Max  Pattern   Type    Num   Reqd
    111                   7    7     111      aar           n
    2                     7    7     999      aar           n
```

2. In the **Dialed String** column, type the numbers that the system compares to the number that the user dials. Valid values are the digits **0** through **9**.

   You can type a maximum of 18 digits. You can also type an asterisk (*****), a lower case **x**, or an upper case **X** as wildcard characters.

   The system uses the dialed string that most closely matches the number that the user dials. For example, if a user dials 297-1234, and the AAR Digit Analysis Table contains two dialed strings of 297-1 and 297-123, the system uses the dialed string 297-123 as the match.

   When the system compares a user-dialed number with an entry in the **Dialed String** column that is an exact match and an entry in the **Dialed String** column with one or more wildcard characters, the system chooses the exact match. For example, if a user dials 424, and the AAR Digit Analysis Table contains two dialed strings of 424 and X24, the system uses the dialed string 424 as the match.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are any number from **1** up to the number that you typed in the **Max** column.
4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are from the number that you typed in the **Min** column to **28**.
5. In the **Route Pattern** column, type the route information that you want the server to use for the dialed string. Perform one of the following actions:
   - To specify the route index number that you established on the Partition Routing Table screen, type a value from **p1** to **p2000**.
   - To specify the route pattern that the system uses to route the call, type a number from **1** to **640**.
   - To specify the route pattern that the system uses to route the call, type a number from **1** to **999**. Use this number range only for the S8*XXX* Server.
   - If RHNPA translations are required for the corresponding dialed string, type a value from **r1** to **r32** to specify the remote home numbering plan.
   - To designate node number routing, type **node**.
   - To block the call, type **deny**.
6. In the **Call Type** column, type the call type that is associated with each dialed string. The call types indicate the numbering requirements on different trunk networks. Perform one of the following actions:
   - For regular AAR calls, type **aar**.
   - If the Route Index contains public network ISDN trunks that require the international type of number encodings, type **intl**.
   - If the Route Index contains public network ISDN trunks that require an unknown type of number encodings, type **pubu**.

- To specify the ISDN Private Number Plan (PNP) number formats, type **lev0**, **lev1**, or **lev2**.
- For a UDP numbering plan where extensions are passed (rather than full public network or private-network numbers), type **unku**.

  For more information on ISDN Numbering-Private, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

  Table 122: ISDN protocols on page 1649 describes the ISDN protocols.

Table 122: ISDN protocols

Call type	Numbering plan identifier	Type of numbering
aar	E.164(1)	national(2)
intl	E.164(1)	international(1)
pubu	E.164(1)	unknown(0)
lev0	PNP(9)	local(4)
lev1	PNP(9)	Regional Level 1(2)
lev3	PNP(9)	Regional Level 2(1)
unku	unknown (0)	unkown (0)

7. In the **Node Number** column, type the number of the destination node in a private network if you use node number routing or Distributed Communication System (DCS).
8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen.

   If the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:

   - If you require ANI on incoming R2-MFC or Russian MF ANI calls, type **y**.
   - If you do not require ANI on incoming R2-MFC or Russian MF ANI calls, type **n**.
   - If the **Allow ANI Restriction on AAR/ARS** field is set to **y** on the Feature-Related System Parameters screen, type **r**. When you set the **ANI Req** field to **r**, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an **r** entry in the **ANI Req** field as a **y**.

   The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.
9. Press **Enter** to save your changes.

Administering the ARS Digit Analysis Table

To administer the ARS Digit Analysis Table for your system:

1. Type **change ars analysis *n***, where ***n*** is the number of the ARS Analysis Table. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen (Figure 423: ARS Digit Analysis Table screen on page 1650).

Figure 423: ARS Digit Analysis Table screen

```
                    ARS DIGIT ANALYSIS TABLE
                              Location:  all           Percent Full:    2

      Dialed           Total      Route    Call   Node  ANI
      String          Min  Max  Pattern   Type   Num   Reqd
101xxxx0              8    8     deny     op            n
101xxxx0              18   18    deny     op            n
101xxxx01             16   24    deny     iop           n
101xxxx011            17   25    deny     intl          n
101xxxx1              18   18    deny     fnpa          n
10xxx0                6    6     deny     op            n
10xxx0                16   16    deny     op            n
10xxx01               14   22    deny     iop           n
10xxx011              15   23    deny     intl          n
10xxx1                16   16    deny     fnpa          n
11                    2    2     10       svcl          n
120                   11   11    deny     fnpa          n
1200                  11   11    deny     fnpa          n
121                   11   11    deny     fnpa          n
122                   11   11    deny     fnpa          n
```

The **location** field is a display-only field.

- If the **ARS** field and the **Multiple Locations** field on the Optional Features screen are set to **y**, the **location** field is set to a number between **1** and **250**. The numbers 1 through 64 in the **location** field define the location of the server that uses this ARS Digit Analysis Table.
- If the **ARS** field on the Optional Features screen is set to **y**, but the **Multiple Locations** field on the Optional Features screen is set to **n**, the **location** field is set to **all**. A value of **all** in the **location** field indicates that this ARS Digit Analysis Table is the default for all port network locations.

2. In the **Dialed String** column, type the numbers that the system compares to the number that the user dials. Valid values are the digits **0** through **9**.

   You can type a maximum of 18 digits. You can also type an asterisk (*****), a lower case **x**, or an upper case **X** as wildcard characters.

   The system uses the dialed string that most closely matches the number that the user dials. For example, if a user dials 297-1234, and the AAR Digit Analysis Table contains two dialed strings of 297-1 and 297-123, the system uses the dialed string 297-123 as the match.

   When the system compares a user-dialed number with an entry in the **Dialed String** column that is an exact match and an entry in the **Dialed String** column with one or more wildcard characters, the system chooses the exact match. For example, if a user dials 424, and the AAR Digit Analysis Table contains two dialed strings of 424 and X24, the system uses the dialed string 424 as the match.

3. In the **Min** column, type the minimum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are any number from **1** up to the number that you typed in the **Max** column.
4. In the **Max** column, type the maximum number of user-dialed digits that the system uses to compare with the matching pattern in the **Matching Pattern** column. Valid values are from the number that you typed in the **Min** column to **28**.
5. In the **Route Pattern** column, type the route information that you want the server to use for the dialed string. Perform one of the following actions:
   - To specify the route index number that you established on the Partition Routing Table screen, type a value from **p1** to **p2000**.
   - To specify the route pattern that the system uses to route the call, type a number from **1** to **640**.
   - To specify the route pattern that the system uses to route the call, type a number from **1** to **999**. Use this number range only for the S8*XXX* Server.
   - If RHNPA translations are required for the corresponding dialed string, type a value from **r1** to **r32** to specify the remote home numbering plan.
   - To designate node number routing, type **node**.
   - To block the call, type **deny**.
6. In the **Call Type** column, type the call type that is associated with each dialed string. The call types indicate the numbering requirements on different trunk networks. Perform one of the following actions:
   - To alert attendant consoles or other digital telephones when a user places an emergency call, type **alrt**.

     This call type is a normal China number 1 call type.
   - To designate an emergency call, type **emer**.

     This call type is a normal China number 1 call type.

- To designate a 10-digit North American Numbering Plan (NANP) call, type **fnpa**. NANP calls consist of 11 digits and a prefix digit of 1.

  This call type is an attendant China number 1 call type.
- To designate a 7-digit NANP call, type **hnpa**.

  This call type is a normal China number 1 call type.
- To designate a public network international number, type **intl**.

  This call type is a toll-auto China number 1 call type.
- To designate an international operator, type **lop**.

  This call type is an attendant China number 1 call type.
- To designate a non-NANP call, type **natl**.

  This call type is a normal China number 1 call type.
- To designate a national private call, type **npvt**.

  This call type is a normal China number 1 call type.
- To designate a national service call, type **nsvc**.

  This call type is a normal China number 1 call type.
- To designate an operator call, type **op**.

  This call type is an attendant China number 1 call type.
- To designate a public network number (E.164) unknown call, type **pubu**.

  This call type is a normal China number 1 call type.
- To designate a national(2) call, type **svcl**.

  This call type is a toll-auto China number 1 call type.
- To designate a national(2) call, type **svct**.

  This call type is a normal China number 1 call type.
- To designate a service call, first part control, type **svft**.

  This call type is a local China number 1.
- To designate a service call, first part control, type **svfl**.

  This call type is a toll China number 1 call type.

7. In the **Node Number** column, type the number of the destination node in a private network if you use node number routing or DCS.
8. Use the **ANI Req** column only if the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen.

   If the **Request Incoming ANI (non-AAR/ARS)** field is set to **n** on the Mutifrequency-Signaling-Related System Parameters screen, perform one of the following actions in the **ANI Req** field:

- If you require ANI on incoming R2-MFC or Russian MF ANI calls, type **y**.
- If you do not require ANI on incoming R2-MFC or Russian MF ANI calls, type **n**.
- If the **Allow ANI Restriction on AAR/ARS** field is set to **y** on the Feature-Related System Parameters screen, type **r**. When you set the **ANI Req** field to **r**, the system drops a call on a Russian shuttle trunk or a Russian rotary trunk if the ANI request fails. For calls on other types of trunks, the system processes an **r** entry in the **ANI Req** field as a **y**.

The **Percent Full** column displays the percent of the allocated system memory that is used by AAR and ARS. You cannot change this field.

9. Press **Enter** to save your changes.

Administering the extension number portability numbering plan

To administer the extension number portability numbering plan for your system:

1. Type **`change enp-number-plan`**. Press **Enter**.

   The system displays the Extension Number Portability Numbering Plan screen (Figure 424: Extension Number Portability Numbering Plan screen on page 1653).

Figure 424: Extension Number Portability Numbering Plan screen

```
                        EXTENSION NUMBER PORTABILITY
                              NUMBERING PLAN


    ENP      ENP      ENP      ENP      ENP      ENP      ENP      ENP      ENP      ENP
   Code     Code     Code     Code     Code     Code     Code     Code     Code     Code

0x:      1x:      2x:      3x:      4x:      5x:      6x:      7x:      8x:      9x:

00:      10:      20:      30:      40:      50:      60:      70:      80:      90:
01:      11:      21:      31:      41:      51:      61:      71:      81:      91:
02:      12:      22:      32:      42:      52:      62:      72:      82:      92:
03:      13:      23:      33:      43:      53:      63:      73:      83:      93:
04:      14:      24:      34:      44:      54:      64:      74:      84:      94:
05:      15:      25:      35:      45:      55:      65:      75:      85:      95:
06:      16:      26:      36:      46:      56:      66:      76:      86:      96:
07:      17:      27:      37:      47:      57:      67:      77:      87:      97:
08:      18:      28:      38:      48:      58:      68:      78:      88:      98:
09:      19:      29:      39:      49:      59:      69:      79:      89:      99:
```

For more information on the Extension Number Portability Numbering Plan screen, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Reports for Uniform Dial Plan

The following reports provide information about the Uniform Dial Plan capability:

- The Uniform Dial Plan report shows the details of the Dial Plan.

For detailed information on these reports and the associated commands, or see Avaya Aura™ Communication Manager *Reports,* 555-233-505.

Considerations for Uniform Dial Plan

This section provides information about how the Uniform Dial Plan (UDP) feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Uniform Dial Plan under all conditions.

- In North American network environments, the system routes extensions that start with 0 to an attendant. Avaya recommends that you use a digit other than 0 as the leading digit when you assign extensions.
- When you call an extension that is on another server, you might experience slight delay before you hear call-progress tones. This delay is caused by the trunk signaling that is necessary to complete the call to the remote media server or to the switch.
- When you select the option that causes the software to look at the UDP table first, the system routes calls that might otherwise terminate at a local extension, over the network. If you do not want the system to route calls over the network, you must remove the extensions from the UDP table. Once you remove the extensions from the UDP table, users can dial the local extension.
- If Automatic Alternate Routing (AAR) is active, the software sends facility restriction levels (FRLs) and Traveling Class Marks (TCMs) with the private network number. UDP Code and AAR Code conversions use the FRL that is assigned to the caller. Extension number portability (ENP) Node conversion always raises the FRL to the maximum of seven.

  If an FRL is insufficient to access the facility, the system denies access. The system does not prompt for an authorization code, even if authorization codes are enabled and administered in your system.
- If AAR is not active, do not equip your system to use tandem-tie trunks to transport UDP numbers. You should not use tandem-tie trunks to transport UDP numbers, because the termination server does not recognize the TCM.

  Avaya recommends that you never use tandem-tie trunks to transport UDP numbers. When you use tandem-tie trunks to transport UDP numbers, the receiving media server or the system does not recognize the TCM and the hop count that follow the extension.

Interactions for Uniform Dial Plan

This section provides information about how the Uniform Dial Plan (UDP) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Uniform Dial Plan in any feature configuration.

- Automatic Alternate Routing (AAR)

  AAR routes UDP calls. The AAR subset is included with the UDP. If AAR and UDP are both enabled on your system, the 7-digit AAR number provides the same routing as the UDP.

- Dial Plan
  - Extension numbers on a server do not need to be part of a UDP. When extension numbers are not part of a UDP, the server software uses a non-UDP to handle calls that are associated with those extensions.
  - When you administer the Dial Plan and designate a group of extensions as UDP nonlocal, you can specify either that the software search for local extensions first, or search for local extensions last.

- Direct Inward Dialing (DID) trunk group

  DID calls to a UDP extension number might require the DID trunk group to insert the necessary digits to create the full extension number. For example, if the DID trunk provides 4 digits, but a 5-digit UDP is in place, the DID trunk group must insert the appropriate leading digit.

- Distributed Communications System (DCS)

  UDP is required when DCS is provided. The necessary UDP software is provided with the DCS software.

- Extension Number Portability (ENP)

  If you administer a user extension to use ENP node routing, ENP routes the call to the correct server.

  If you enable both AAR and UDP, the 7-digit AAR number provides the same routing as UDP. The 7-digit AAR number uses ENP to route the call.

Visually Impaired Attendant Service

Use the Visually Impaired Attendant Service (VIAS) feature to provide voice feedback to a visually impaired attendant. Each voice phrase is a sequence of one or more single-voiced messages.

Detailed description of Visually Impaired Attendant Service

This section provides a detailed description of the Visually Impaired Attendant Service (VIAS) feature.

VIAS defines six buttons for the visually impaired attendant:

- Visually impaired service activation and deactivation

  This button activates or deactivates VIAS. When you press the button, the system reenables all ringers that are disabled, such as the recall and incoming call ringers.

- Console status

  When you press this button, the system provides voice feedback of the status of the:

  — Console, for example, busy, available, or night service

  — Attendant queue

  — System alarms

- Display status

  When you press this button, the system provides voice feedback of the information that is on the console display. VIAS is unavailable for some displays, such as Class of Restriction (COR), restriction information, personal names, and the purpose of some calls.

- Last operation

  When you press this button, the system provides voice feedback of the last operation that was performed at the console.

- Last voice message

  When you press this button, the system provides voice feedback of the most recent message at the console.

- Direct trunk group selection status

  When you press this button, the system provides voice feedback of the status of an attendant-monitored trunk group.

A visually impaired attendant can use the Inspect mode to locate each button, to determine the feature that is assigned to the button.

Administering Visually Impaired Attendant Service

This section contains prerequisites and the screens that you use to administer the Visually Impaired Attendant Service (VIAS) feature.

Prerequisites for administering Visually Impaired Attendant Service

You must complete the following actions before you can administer the Visually Impaired Attendant Service (VIAS) feature:

- Set up an attendant console. For information on how to set up an attendant console, see the *Administering Avaya Aura™ Communication Manager*.

Screens for administering Visually Impaired Attendant Service

Screen name	Purpose	Fields
Attendant Console	Administer the Visually Impaired Attendant Service (VIAS) buttons: • vis • con-stat • display • dtgs-stat • last-mess • last-op	Any available button field in the **Feature Button Assignments** area

Interactions for Visually Impaired Attendant Service

This section provides information about how the Visually Impaired Attendant Service (VIAS) feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Visually Impaired Attendant Service (VIAS) in any feature configuration.

- Audible Message Waiting

  The system generates a stutter tone before the dial tone, when a message waits at an extension. A visually impaired attendant can use the stutter tone, instead of a message light, to detect a message that waits at an extension.

- Auto Start and Don’t Split

  If you activate or deactivate VIAS while Auto Start and Don’t Split is active, the system deactivates Auto Start and Don’t Split.

- Automatic Circuit Assurance (ACA)

  When the attendant presses the display button, the system provides the following voice messages:

  – "Automatic Circuit Assurance," if an ACA call is unanswered

  – "Automatic Circuit Assurance," and the extension that is assigned to the ACA call, if the call is answered

- Malicious Call Trace (MCT)

  The system provides voice feedback of the displays that are related to MCT activation, but not of the displays that are related to MCT control.

Voice Message Retrieval

Use the Voice Message Retrieval feature to allow attendants, telephone users, and remote access users to retrieve Leave Word Calling (LWC) messages and Call Coverage messages.

Detailed description of Voice Message Retrieval

This section provides a detailed description of the Voice Message Retrieval feature.

Voice Message Retrieval is used only for the retrieval of messages. When a telephone is in Voice Message Retrieval mode, you cannot use the telephone to make calls or access other features. You can use Voice Message Retrieval to retrieve your own messages, or messages for another user. However, a different user's messages for another user can only be retrieved at a telephone or an attendant console that is in the coverage path. This is done by an administered system-wide message retriever, or by a remote-access user when the extension and the associated security code are known. The number of simultaneous Voice Message Retrieval users that are possible depends on the number of speech-synthesizer circuit packs in the system.

You can designate certain telephones and attendants for system-wide message retrieval. These telephones are the same as that you use for Display Message Retrieval, and have the same privileges. Voice Message Retrieval cannot be accessed from rotary telephones.

You can restrict unauthorized users from retrieving messages. Use the Lock function to restrict a telephone and the Unlock function to release the restriction. To activate Lock, users dial a system-wide access code. To cancel Lock, users dial a system-wide access code, and then an Unlock security code that is unique to the telephone. These functions only apply to the telephone where the function is active. The system-wide access codes and security code that you use for the Lock and Unlock functions are the same as those use for LWC message retrieval by display. You can assign a status lamp to show the Lock status of the telephone.

Administering Voice Message Retrieval

This section describes the screens that you use to administer the Voice Message Retrieval feature.

Screens for administering Voice Message Retrieval

Screen name	Purpose	Fields
Feature Access Code (FAC)	Set up Voice Message Retrieval.	• **LWC Message Retrieval Lock** • **LWC Message Retrieval Unlock** • **Voice Coverage Message Retrieval Access Code** • **Voice Principal Message Retrieval Access Code**
Feature Related System Parameters	Administer Voice Message Retrieval.	• **Stations With System-Wide Retrieval Permission Message** • **Waiting Lamp Indicates Status**
Station	Set up Voice Message Retrieval.	**Security Code**

Reports for Voice Message Retrieval

The following reports provide information about the Voice Message Retrieval feature:

- None

Considerations for Voice Message Retrieval

This section provides information about how the Voice Message Retrieval feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Voice Message Retrieval under all conditions. The following considerations apply to Voice Message Retrieval:

- None

Interactions for Voice Message Retrieval

This section provides information about how the Voice Message Retrieval feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Voice Message Retrieval in any feature configuration.

- CM Messaging Interface

  Retrieval of Leave Word Calling (LWC) messages by way of Voice Message Retrieval is separate and distinct from retrieval of messages by way of CM Messaging. You cannot use Voice Mail Retrieval to access LWC messages on CM Messaging. However, the user who calls Voice Message Retrieval is informed of any new messages for the principal on CM Messaging:

  - The Voice Message Retrieval voices that there are messages on the CM Messaging system.
  - The Display Message Retrieval displays "Message Center AUDIX Call."

  If your system has a voice-synthesizer circuit pack and LWC Activation is active, users can retrieve messages: LWC messages with Voice Message Retrieval and all other messages with CM Messaging.

  If you do not have a TN725B speech-synthesizer board, nondisplay telephone users cannot retrieve LWC messages that are sent by way of the **LWC** button on a telephone.

- Bridged Call Appearance

  Voice Message Retrieval on a Bridged Call Appearance functions the same as if the feature were activated by the primary extension that is associated with the bridged call appearance.

- Leave Word Calling (LWC)

  Voice Message Retrieval enhances LWC by allowing any authorized touchtone telephone user to retrieve messages.

Whisper Paging

Use the Whisper Paging feature to allow one user to interrupt or "barge in" on the call of another user and make an announcement. The paging user dials a Feature Access Code (FAC) or presses a feature button, and then dials the extension of the other user.

Detailed description of Whisper Paging

This section provides a detailed description of the Whisper Paging feature.

With the Whisper Paging feature, the page is unique because only the person on the paged extension can hear the page. Other parties on the call cannot hear the page, and the person who makes the page cannot hear anyone on the call. If the paged user has a display telephone, the paged user can see who makes the whisper page.

For example, users A and B are on a call. User C has an urgent message for user A and makes a whisper page. All three users hear the tone that signals the page, but only user A hears the page itself. User who make the page cannot hear users A or B.

Call redirection overrides

If a paged user is not on an active call, a whisper page is converted to a priority call that overrides any of the following call redirection features:

- Call Forward All Calls
- Call Forward Busy
- Call Forward Don’t Answer
- Send All Calls
- Go To Cover
- Call Coverage

For example, if Call Forward All Calls is activated on a telephone on which no active calls exist, a whisper page to that telephone rings as a priority call.

Group answering environments

Whisper Paging does not work with extensions that are assigned to a group answering environment. You cannot place a whisper page to the main extension that is assigned to a hunt group, a a split, a skill, or a terminating extension group (TEG). You cannot place a whisper page to any extension that is a member of one of these groups.

Network restrictions

Whisper Paging does not work across networks, such as Distributed Communication System (DCS) networks or electronic tandem networks. Both the paging user and the paged user must be on the same server that runs Communication Manager.

Speakerphones

When a call is on the speaker, an incoming whisper page is also heard over the speaker too. When the group listening feature on a 6400-series telephone is active, an incoming whisper page is heard on both the handset and the speaker.

Administering Whisper Paging

The following steps are part of the administration process for the Whisper Paging feature:

This section describes:

- Any prerequisites for administering the Whisper Paging feature
- The screens that you use to administer the Whisper Paging feature

Prerequisites for administering Whisper Paging

You must complete the following actions before you can administer the Whisper Paging feature:

- None

Screens for administering Whisper Paging

Screen name	Purpose	Fields
Station	Activate Whisper Paging buttons.	• **Whisper Page Activation** • **Answerback** • **Whisper Page Off**
Feature Access Code (FAC)	Activate a FAC to Whisper Page.	**Whisper Page Activation Access Code**

Making a whisper page

- To assign a Feature Access Code, enter a code in the **Whisper Page Activation Access Code** field on the Feature Access Code screen.
- To give users a feature button for making a whisper page, use the Station screen and administer a **Whisper Page Activation** button on users' phones.

Allowing users to answer whisper pages quickly

To give users a feature button for answering a whisper page, use the Station screen and administer an **Answerback** button on users' phones.

Note:
You cannot administer an **Answerback** button on an attendant console. Attendants can make whisper pages but cannot receive them.

Normally, before a paged user can answer a whisper page, he or she must complete the active call or put it on hold. However, you can give users the ability to put an active call on hold and speak directly to the person making a whisper page simply by pushing a feature button. Once the **Answerback** button is pressed, the user can treat both the paging call and the original call as separate calls and all call-related features (conference, transfer, and so on) operate normally.

Allowing users to block whisper pages

To give users a feature button to block incoming whisper pages, use the Station screen and administer a **Whisper Page Off** button on users' phones.

Administer this function on a feature button with a lamp so that users can tell whether or not blocking is active. Users can activate blocking even when they are on a call.

Note:
You cannot administer a **Whisper Page Off** button on a soft key.

The Do Not Disturb and Privacy - Attendant Lockout features can also block incoming whisper pages.

End-user procedures for Whisper Paging

End users must perform specific procedures to use certain features. End users can activate or deactivate certain system features and capabilities. End users can also modify or customize some aspects of the administration of certain features and capabilities. This section includes the following end-user procedures for Whisper Paging:

- To make a whisper page, users dial a FAC or press a feature button, then dial the extension of the user they are trying to reach.

Reports for Whisper Paging

The following reports provide information about the Whisper Paging feature:

- None

Considerations for Whisper Paging

This section provides information about how the Whisper Paging feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Whisper Paging under all conditions. The following considerations apply to Whisper Paging:

- The Whisper Page feature currently does not work correctly if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.

Interactions for Whisper Paging

This section provides information about how the Whisper Paging feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Whisper Paging in any feature configuration.

- Attendant

  Attendants cannot intrude on a whisper page. If an attendant is using intrusion to talk to a user, that user cannot receive a whisper page.

  An attendant can use auto-manual splitting to start a whisper page. However, the attendant cannot use Release, Hold, or Split after the page is made.

- Bridged Call Appearances

  Whisper pages are designed to reach a specific user associated with a specific extension.

  - When an extension and one or more of its bridged appearances are in use, parties on the bridged appearances hear the tone that signals an incoming whisper page but only the user on the principle extension hears the announcement. Only the display on the principle extension shows the whisper page message.
  - When all appearances are idle or only a bridged appearance is in use, a whisper page rings the principal extension with priority ringing.
  - If a user makes a whisper page on a call appearance that is a member of a bridge group, then no others users in the bridge group can connect to the call while the whisper page intrusion is active.

- Busy Verification

  You can’t make a whisper page to an extension while it’s being busy-verified. You cannot busy-verify an extension while it’s making or receiving a whisper page.

- Calling Restrictions - Origination

  Telephones with this restriction cannot make whisper pages.

- Calling Restrictions - Termination

  Telephones with this restriction cannot receive whisper pages.

- Class of Restriction (COR)

  A station user must have a COR that allows for station-to-station calling in order to perform Whisper Paging to a member outside of their own COR. Calling and called party restrictions also determine which extensions can make and receive whisper pages.

- Conference

  Everyone on a conference call hears the tone that signals an incoming whisper page. But only the owner of the paged extension hears the page, and only the display on that phone shows the whisper page message.

  If a conference call already has the maximum number of parties and trunks allowed, you cannot make a whisper page to any of the participants. Parties cannot be added to a conference call if an active whisper page is on the call.

- Data Privacy - Permanent or Temporary

  Any station that has Data Privacy activated cannot make a whisper page.

- Data Restriction

  A whisper page to a station is denied when Data Restriction is enabled on a station or trunk.

- Expert Agent Selection

  You cannot make a whisper page by dialing an agent's Logical Agent ID. Pages must be made to a physical extension.

- Go to Cover

  If you make a whisper page and then press your Go To Cover button while the page is in progress, the Go To Cover button does not work. The opposite is true as well. If you activate Go to Cover and then press the whisper page activation button, you will not able to make a whisper page.

- Last Number Dialed

  When you make a whisper page, the page is tracked as the last number dialed.

- QSIG

  This feature does not operate in a QSIG environment.

- Remote Access

  You cannot make a whisper page by remote access. Both the paging party and the paged party must be on the same media server or the attempt is denied.

- Tenant Partitioning

  Whisper paging is permitted across tenant partitions if the assigned classes of restriction allow for intercom calling between members of different partitions. This feature is especially useful to attendants who serve multiple partitions.

  Note:
  System administrators must ensure that this feature is managed appropriately in systems with tenant partitioning. Some tenants might not want other tenants to interrupt their calls.

- Transfer

  A call cannot be transferred during an active whisper page.

- Vector Directory Number (VDN)

  You cannot make a whisper page to a VDN. Pages must be made to a physical extension.

Wideband Switching

Use the Wideband Switching feature to dedicate two or more ISDN-PRI B-channels or digital signal level 0 (DS0) endpoints for applications that require large bandwidth. Wideband Switching provides high-speed end-to-end connectivity between endpoints where dedicated facilities are not economic or appropriate. ISDN-BRI trunks do not support wideband switching.

Detailed description of Wideband Switching

This section provides a detailed description of the Wideband Switching feature.

ISDN-PRI and the emulation of ISDN-PRI by Asynchronous Transfer Mode-Circuit Emulation Service (ATM-CES) divides trunks into information channels and signaling channels for standard narrowband communication.

Certain applications, like video conferencing, require greater bandwidth. For standard narrowband communication, ISDN-PRI divides:

- T1 trunks into 23 information channels, and 1 signaling channel
- E1 trunks into 30 information channels, 1 signaling channel, and 1 framing channel

You can combine several narrowband channels into one wideband channel to accommodate the extra bandwidth requirement. Communication Manager serves as a gateway to many types of high-bandwidth traffic. In addition, DS1 converters are also used for wideband switching at remote locations.

Wideband Switching is also supported by the Expansion Interface (EI) circuit pack and the DS1 Converter circuit pack for Center Stage Switching or directly connected port networks and the ATM-EI circuit pack for Asynchronous Transfer Mode connected port networks. ATM-CES supports wideband switching only for access, tie, and tandem trunks, not for line-side connections.

Wideband Switching supports:

- High-speed video conferencing
- Wide area network (WAN) disaster recovery
- Scheduled batch processing, such as nightly file transfers
- Local area network (LAN) interconnections and imaging
- Other high-bandwidth applications that involve high-speed data transmission, video transmission, and so on.

Channel allocation

Table 123: Wideband Switching channel types on page 1674 provides information on Wideband Switching channel types.

Table 123: Wideband Switching channel types

Channel type	Number of channels	Data rate (kbps)
H0	6	384
H11	24	1536
H12	30	1920
NXDS0 (T1)	2 to 24	128 to 1536
NXDS0 (E1)	2 to 31	128 to 1984

Perform wideband line-side channel allocation with one of three allocation algorithms:

- Fixed allocation. Provides contiguous-channel aggregation. The starting channel is constrained to a predetermined starting point. Fixed allocation is used for H0, H11, and H12 calls only.
- Flexible allocation. Allows a wideband call to occupy noncontiguous positions within a single T1 or E1 facility.
- Floating allocation. Enforces contiguous-channel aggregation. The starting channel is not constrained to a predetermined starting point.

Typical uses

A typical video application uses an ISDN-PRI interface to DS0 1 through 6 of the line-side facility. Figure 425: Typical video broadband application on page 1675 shows an example.

Figure 425: Typical video broadband application

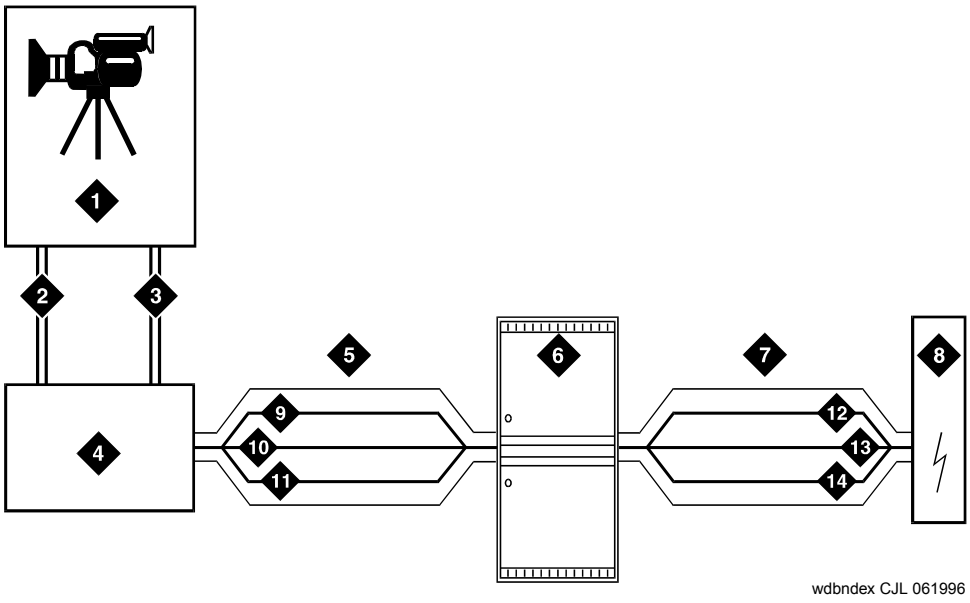


Figure notes:

1. Video application
2. Port 1
3. Port 2
4. ISDN terminal adaptor
5. Line-side ISDN-PRI
6. Avaya S8*XXX* Server
7. ISDN or ATM-CES trunk
8. Network
9. DS0 24 D-channel
10. DS0 23 unused
11. DS0 1-6 wideband
12. DS0 24 D-channel
13. DS0 7-23 narrow bands
14. DS0 1-6 wideband

Endpoint applications with signaling

An endpoint application is the origination point or the destination point of a wideband call. Endpoint applications can be any number of data applications, based on the needs of the customer.

ISDN-PRI terminal adapters

For Wideband Switching with non-ISDN-PRI equipment, you can use an ISDN-PRI terminal adapter. ISDN-PRI terminal adapters translate standard ISDN signaling into a form that can be used by the endpoint application, and vice versa. The terminal adapter also must adhere to the PRI-endpoint boundaries as administered on Communication Manager when handling both incoming applications to the endpoint and outgoing calls.

The terminal adapter passes calls to and receives calls from the line-side ISDN-SETUP messages. These messages indicate the data rate and the specific B-channels (DS0) to be used. The terminal adapter communicates all other call status information by way of standard ISDN messages. For more information, see *DEFINITY Line-Side ISDN Primary Rate Interface Technical Reference*.

Line-side T1 or E1 ISDN-PRI facilities

A line-side T1 or E1 ISDN-PRI facility is comprised of a group of DS0s. In this context, these DS0s are also called channels. T1 facilities have 23 B-channels and a single D-channel. E1 facilities have 30 B-channels, 1 D-channel, and a framing channel. Data flows bidirectionally across the facility between the server that is running Communication Manager and the ISDN-PRI terminal adapter.

PRI endpoints

A PRI-endpoint (PE) is a combination of DS0 B-channels on a line-side ISDN-PRI facility to which an extension is assigned.

A PE can support calls of lower bandwidth. In other words, a PE that has a width of six DS0 channels can handle a call of one channel of 64 Kbps, up to and including six channels totaling 384 Kbps. Also, a PE can support calls on nonadjacent channels. For example, an endpoint application that is connected to a PE that is defined as using B-channels 1 through 6 of an ISDN-PRI facility could use B-channels 1, 3, and 5 successfully to originate a call.

If the PE is administered to use flexible channel allocation, the algorithm for offering a call to the PE starts from the first DS0 that is administered to the PE. Since only one active call is permitted on a PE, contiguous B-channels are always selected unless one or more B-channels are not in service.

A PE remains in service unless all the B-channels are out of service. In other words, if B-channel 1 is out of service and the PE is five B-channels wide, the PE can still handle a wideband call of up to four B-channels wide. A PE can only be active on a single call at any given time. That is, the PE is considered to be idle, active or busy, or out of service.

One facility can support multiple separate and distinct PEs within a single facility. Non-overlapping contiguous sets of B-channel DS0s are associated with each PE.

Universal digital signal level 1 board

The universal digital signal level 1 (UDS1) board is the interface for line-side and network facilities that carries wideband calls.

Nonsignaling endpoint applications

Wideband Switching can also support configurations that use nonsignaling, non-ISDN-PRI line-side T1 or E1 facilities. The endpoint applications are the same as those that are defined for configurations with signaling.

Data service unit/channel service unit

The device service unit (DSU)/channel service unit (CSU) passes the call to the endpoint application. Unlike terminal adapters, the DSU/CSU does not have signaling capability.

Note:
No DSU/CSU is needed if the endpoint application has a fractional T1 interface.

Line-side T1 or E1 facility

This facility, like the ISDN-PRI facility, is composed of a group of DS0s. This group includes 23 DS0s for a T1 facility, and 30 DS0s for an E1 facility. Line-side facilities are controlled solely from the server. Through the access-endpoint command, a specific DS0 or group of DS0s is assigned an extension. This individual DS0 or group, along with the extension, is known as a wideband access endpoint (WAE).

Wideband access endpoint

WAEs have no signaling interface to the media server. These endpoints simply transmit and receive wideband data when the connection is active.

Note:
Communication Manager can determine if the connection is active. An active connection does not necessarily mean that data is actually coming across the connection.

A WAE is treated as a single endpoint and can support only one call.

- If all DS0s that comprise a wideband access endpoint are in service, the wideband access endpoint is considered to be in service.
- If all DS0s are not in service, the wideband access endpoint is considered out of service.
- If an in-service wideband access endpoint has no active calls on its DS0s, the endpoint is considered to be idle.
- If the endpoint has active calls on its DS0s, the endpoint is considered busy.

Multiple WAEs are separate and distinct within the facility, and endpoint applications must be administered to send and receive the correct data rate over the correct DS0s. An incoming call at the incorrect data rate is blocked.

Guidelines and examples

This section examines Wideband Switching and the components of Wideband Switching in relation to the following specific usage scenarios:

- High-speed video conferencing
- Data backup connection
- Scheduled batch processing
- Primary data connectivity
- Networking

High-speed video conferencing

The following table lists some key customer data rates.

Channel type	Number of channels	Data rate (Kbps)
H0	6	384
H11	24	1536
H12	30	1920
NXDS0 (T1)	2-24	128-1536
NXDS0 (E1)	2-31	128-1984

Data backup connection

Using Wideband Switching for data transmission backup provides customers with alternate transmission paths for critical data in the event of primary transmission path failure.

Scheduled batch processing

Scheduled batch processing applications are used for periodic database updates, such as retail inventory, or distributions, such as airline fare schedules. These updates are primarily done after business hours and are often referred to as *nightly file transfers*. Wideband meets the high bandwidth requirements at low cost for scheduled batch processing. Wideband also allows the dedicated-access bandwidth for busy-hour switching traffic to be used for these applications after business hours. Thus, no additional bandwidth costs are incurred.

The non-ISDN backup data connection is also appropriate for scheduled batch processing applications. Administered Connections are used to schedule daily or weekly sessions that originate from this application.

Primary data connectivity

Permanent data connections are well suited for Communication Manager when ISDN-PRI endpoints are used. Permanent data connections, such as interconnections between local area networks (LANs), are always active during business hours. The ISDN end-to-end monitoring and the ability of the endpoint to react to failures provide for critical availability of data. With ISDN, endpoints can detect network failures and initiate backup connections through the server. ISDN endpoints can also establish additional calls when extra bandwidth is needed.

Any failures that Communication Manager does not automatically restore are signaled to the endpoint application. The endpoint application can initiate backup data connections over the same PRI endpoint. Communication Manager routes the backup data connections over alternate facilities if necessary.

Networking

All wideband networking is over ISDN-PRI facilities, and the emulation of ISDN-PRI facilities by ATM-CES. Wideband networking may also connect to a variety of networks, other services of domestic interexchange carriers, private line, RBOC services, and services in other countries.

ISDN-PRI trunk groups and channel allocation

Only ISDN-PRI trunks, and the emulation of ISDN-PRI trunks by ATM-CES, support wideband calls to the network. The bandwidth requirements of wideband calls necessitate modification of the algorithms by which trunks look for clear channels.

The following sections describe the search methods, and the relationship of those methods to the available wideband data services.

Facility lists

A wideband call that accesses the network must reside on a single ISDN-PRI facility. Trunks within a trunk group must be organized based on the facility on which the trunks reside. Trunk organization is accomplished by compiling a facility list at the time that trunks are administered to a trunk group.

If a trunk is added to a trunk group from a facility that is not already on the list of that trunk group, that facility is added to the list in an order that is based on the signaling group number and interface identifier of the facility. In other words, the facility list is compiled in an ascending order that is based first on signaling group number, and second on the interface identifier assigned to the facility within the signaling group.

For example, if three facilities with signaling group/interface identifier combinations of 1/1, 1/2, and 2/1 are associated with a trunk group, a call that is offered to that trunk group searches those facilities in the order that the facilities are shown.

Note:
Since trunks within a given facility can span several trunk groups, a single facility can be associated with several different trunk groups.

With this facility list concept, the algorithms can search for trunks by facility to satisfy the band, the algorithm searches the next facility in the trunk group for the required bandwidth if:

- One facility does not have enough available bandwidth to support a given call
- The facility is not used for a given call due to constraints

Note:
The following section describes these constraints.

In addition to searching for channels based on facilities and required bandwidth, port network (PN) preferential trunk routing is also employed. This PN routing applies within each algorithm at a higher priority than the constraints that are put on the algorithm by the parameters listed later in this section. All facilities that reside on the same PN as the originating endpoint are searched to satisfy the bandwidth of a given call, before searching any facilities on another PN.

Direction of trunk hunting within facilities

With an ISDN facility, the algorithms have the ability to select trunks from low B-channel to high B-channel, or from high B-channel to low B-channel. This trunk selection process is an option for each ISDN trunk group. The process infers the direction of search within all ISDN facilities, or portions of those facilities, that are administered within that trunk group. This option is necessary so that the selection of trunks are not prone to as much glare as the selection process otherwise would be if trunks were chosen in the same direction by both user and network sides of the ISDN interface. For more information, see Glare prevention and resolution on page 1683.

In earlier releases of Communication Manager, the order in which trunks were selected, whether through linear or circular hunting, would always be with respect to the order in which trunks were administered within the trunk group. Now, with the support of wideband services, all trunks within an ISDN trunk group that is optioned for wideband are ordered based on this new "direction of trunk hunt with facilities" parameter. This process occurs without regard to the order in which trunks are administered within the trunk group. If an ISDN trunk group is not optioned for wideband, a cyclical trunk hunt that is based on the administration of trunks within the trunk group is still available.

H11 channels

When a trunk group is administered to support H11, the algorithm to satisfy a call that requires 1,536 Kbps of bandwidth uses a fixed allocation scheme. That is, the algorithm uses the following facility-specific channel definitions to search for an available facility:

- T1. H11 can be carried on a facility only without a D-channel being signaled in a nonfacility-associated signaling (NFAS) arrangement. The system uses B-channels 1 through 24.

- E1. Although the 1,536-Kbps bandwidth could be satisfied using a number of fixed starting points, such as 1, 2, 3, and so on, the only fixed starting point that is supported is 1. Hence, B-channels 1 through 15 and 17 through 25 are always used to carry an H11 call on an E1 facility.

If the algorithm cannot find an available facility within the trunk group that meets these constraints, the call is blocked from using this trunk group. In this case, the call might be routed to a different trunk group preference through Generalized Route Selection (GRS). In this case, based on the wideband options that are administered on that trunk group, the call is subject to another hunt algorithm. That is, the call is subject to either the same H11 algorithm, or perhaps an N x DS0 algorithm as described in a later section.

This same hunt algorithm, when offered any other call other than a 1,920-Kbps call, attempts to preserve idle facilities by selecting one or more trunks in a partially contaminated facility, if such a facility exists. If the bandwidth that this call requires cannot be satisfied by any partially contaminated facility, the call is placed on one or more available trunks within an idle facility, thus contaminating the facility. Again, facilities are selected through the facility list of the trunk group and with PN preference. One or more trunks within a facility are selected based on the direction of channel search that is administered.

Note:

On a T1 facility, a D-channel is not considered to be a busy trunk, and results in a facility with a D-channel always being partially contaminated. On an E1 facility, however, a D-channel is not considered to be a busy trunk because H11 and H12 calls might still be placed on that facility. An E1 facility with a D-channel and idle B-channels is considered to be an idle facility.

H12 channels

Since H12 is 1,920 Kbps, which is comprised of 30 B-channels, a 1,920-Kbps call can be carried only on an E1 facility. As with H11, the hunt algorithm uses a fixed allocation scheme with channel 1 being the fixed starting point. Hence, an H12 call is always carried on B-channels 1 through 15 and 17 through 31 on an E1 facility, as the following table shows. When the system is offered any other call other than a 1,536-Kbps call, the algorithm behaves as it does when H11 is optioned.

		DS0s that comprise each channel	
Facility	**ISDN interface**	**H11**	**H12**
T1	23B + D	-	-
T1	24B (NFAS)	1-24	-
E1	30B + D	1 through 15, 17 through 25	1 through 15, 17 through 31
E1	31B (NFAS)	1 through 15, 17 through 25	1 through 15, 17 through 31

H0 channels

When a trunk group is administered to support H0, the algorithm to satisfy a call that requires 384 Kbps of bandwidth also uses a fixed allocation scheme. Unlike the H11 fixed scheme that only supports a single fixed starting point, the H0 fixed scheme supports four T1 or five E1 fixed starting points.

The H0 algorithm searches for an available quadrant within a facility based on the direction of trunk or hunt that is administered. If the algorithm cannot find an available quadrant within any facility that is allocated to this trunk group, the call is blocked from using this trunk group. Based on GRS administration, the system might route the call to a different trunk group preference. Such a call is subject to another algorithm based on the wideband options that are administered.

This same trunk or hunt algorithm, when offered any narrowband or N x DS0 call, attempts to preserve idle quadrants by choosing one or more trunks in a partially contaminated quadrant, if such a quadrant exists. If a partially contaminated quadrant capable of carrying the call does not exist, the call is placed on one or more available trunks within an idle quadrant, thus contaminating the quadrant. Facilities are selected through the facility list of the trunk group and with PN preference, and one or more trunks within a facility are selected based on the direction that is administered.

Note:
A D-channel is considered to be a busy trunk and results in the top most quadrant of a T1 facility, B-channels 19 to 24, always being partially contaminated. This is not true for NFAS.

If this H0 optioned trunk group is also administered to support H11, H12, or N x DS0, this algorithm also attempts to preserve idle facilities. In other words, when offered a narrowband, H0 or N x DS0 call, the algorithm searches partially contaminated facilities before the algorithm searches idle facilities.

N x DS0 channels

For the N x DS0 multirate service, a trunk group parameter determines whether the system uses a floating or a flexible trunk allocation scheme. The letter N in this channel service is a variable.

The algorithm to satisfy an N x DS0 call is either floating or flexible.

- Floating. In a floating scheme, the system places an N x DS0 call on a contiguous group of B-channels that are large enough to satisfy the requested bandwidth without putting any constraint on the starting channel. There is no fixed starting point trunk.

- Flexible. In a flexible scheme, the system places an N x DS0 call on any set of B-channels as long as the requested bandwidth is satisfied. There is no constraint, such as contiguity of B-channels or fixed starting points. As with all wideband calls, all the B-channels that comprise the wideband call must reside on the same ISDN facility.

  Regardless of the allocation scheme that the system employs, the N x DS0 algorithm, like the H11 and H12 algorithms, attempts to preserve idle facilities when offered B, H0, and N x DS0 calls. For large values of N, N x DS0 calls have a better chance of being satisfied by a given trunk group. However, if one of these calls cannot be satisfied by a partially contaminated facility and an idle facility exists, the system selects a trunk on that idle facility, thus contaminating that facility.

  Note the following additional factors regarding specific values of N and the N x DS0 service:

  - N = 1. This value is considered to be a narrowband call and is treated as any other voice or narrowband data, B-channel call.
  - N = 6. If a trunk group is optioned for both H0 and N x DS0 service, a 384-Kbps call that is offered to that trunk group is treated as an H0 call. The H0 constraints apply. If the H0 constraints cannot be met, the call is blocked.
  - N = 24. If a trunk group is optioned for both H11 and N x DS0 service, a 384-Kbps call that is offered to that trunk group is treated as an H0 call. The H0 constraints apply. If the H0 constraints cannot be met, the call is blocked.
  - N = 24. If a trunk group is optioned for both H11 and N x DS0 service, a 1,536-Kbps call that is offered to that trunk group is treated as an H11 call. The H11 trunk allocation constraints apply.
  - N = 30. If a trunk group is optioned for both H12 and N x DS0 service, a 1,920-Kbps call that is offered to that trunk group is treated as an H12 call. The H12 trunk allocation constraints apply.

Glare prevention and resolution

Glare occurs when both sides of an ISDN interface select the same B-channel for call initiation. For example, a user side of an interface selects the B-channel for an outgoing call and, before Communication Manager receives and processes the SETUP message, the user side interface selects the same B-channel for call origination. Since wideband calls use more channels, the chances of glare are greater. Glare conditions can be limited with proper channel administration, but glare conditions can never be eliminated. The system might still drop some calls.

Some glare situations might not be resolvable. In one case, the network and the user side might simultaneously or nearly simultaneously send SETUP messages. Another glare scenario can occur in the brief window after the SETUP message is sent, but before the first response is received from Communication Manager at the other side of the interface. If an incoming SETUP message arrives during this window, the incoming SETUP message is allowed to proceed. The system drops the outgoing call. Communication Manager does not negotiate channels for wideband calls.

Table 124: Glare resolution on page 1684 describes some glare situations and their resolution.

Table 124: Glare resolution

Outgoing call type	Incoming call type	Switch-supporting user protocol	Switch-supporting network protocol
B-channel	B-channel	No negotiation. • The incoming call from the network wins. • The outgoing call to the network is retried on another trunk.	Negotiation is attempted. • The incoming call from the user is dropped if the negotiation is unsuccessful. • The outgoing call to the user stays up.
One or more B-channels	Wide	No negotiation. • The incoming call from the network is dropped. • The outgoing calls to the network stay up, but likely are dropped by the network because channels are in use. A possibility exists that some media servers or systems might negotiate these calls.	No negotiation. • The incoming call from the user is dropped. • The outgoing calls to the user stay up, and possibly stay up if the other side lets the network call win.
Wide	One or more B-channels	No negotiation. • The incoming call from the network wins. • The outgoing call to the network is retried on another trunk.	Negotiation is attempted. • The incoming call from the user is dropped if the negotiation is unsuccessful. • The outgoing call to the user stays up.
Wide	Wide	No negotiation. • The incoming call from the network is dropped. • The outgoing calls to the network stay up, but likely are dropped by the network because channels are in use.	No negotiation. • The incoming call from the user is dropped. • The outgoing call to the user stays up and might not be dropped by the other end. If the other end is not Communication Manager, the other end might let the network call win.

To reduce glare probability, you must administer the network so that both sides of the interface select channels from the opposite ends of the facilities. For example, on a 23B+D trunk group, you can administer the user side to select B-channels starting at channel 23, while you can administer the network side to start selecting at channel 1. Using this same example, if channel 22 is active and channel 23 is idle, the user side can select channel 23 for re-use. This option is known as *linear trunk hunt*, and is the hunt option used by Communication Manager for wideband.

Blocking prevention

Blocking occurs when an insufficient number of B-channels are available to make a call. Narrowband calls require only one channel, so blocking is less likely than with wideband calls that require multiple B-channels. Blocking also occurs for wideband calls when bandwidth is not available in the appropriate format, such as fixed, floating, or flexible.

To reduce blocking, Communication Manager selects trunks for both wideband calls and narrowband calls to maximize the availability of idle fixed channels for H0, H11, and H12 calls, and idle floating channels for N x DS0 calls that require a contiguous bandwidth. The strategy for preserving idle channels depends on the channel type. The chances for blocking are reduced if you use a flexible algorithm, assuming that the algorithm is supported on the other end.

The following table describes the blocking strategy for the different channel types.

Channel type	Blocking minimization strategy
H0	Preserve idle quadrants
H11	Preserve idle facilities
H12	Preserve idle facilities
Flexible N x DS0	Preserve idle facilities
Floating N x DS0	Preserve idle facilities as first priority

Administering Wideband Switching

The following steps are part of the administration process for the Wideband Switching feature:

This section describes:

- The screens that you use to administer the Wideband Switching feature

Screens for administering Wideband Switching

Screen name	Purpose	Fields
Access Endpoint	Administer Wideband Switching.	All
System Parameters-Customer Options	Administer Wideband Switching.	**Wideband Switching**
PRI Endpoint	Administer Wideband Switching.	All
ISDN Trunk Group	Administer Wideband Switching.	All
Route Pattern	Administer Wideband Switching.	All
Fiber Link Administration	Administer Wideband Switching.	All

Considerations for Wideband Switching

This section provides information about how the Wideband Switching feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of Wideband Switching under all conditions. The following considerations apply to Wideband Switching:

- If the user side is provisioned to start at the high side, such as DS0 23, DS0 22 is idle, and DS0 23 is active, reselect DS0 22 for the next call. This is known as linear trunk hunting. Only the direction of hunt is administrable.

Interactions for Wideband Switching

This section provides information about how the Wideband Switching feature interacts with other features on the system. Use this information to ensure that you receive the maximum benefits of Wideband Switching in any feature configuration.

- Administered Connections

  Administered Connections provides call initiation for wideband access endpoints (WAEs). All Administered Connections that originate from WAEs use the entire bandwidth that is administered for WAE. The destination of an Administered Connection can be a PRI endpoint.

- Automatic Circuit Assurance (ACA)

  ACA treats wideband calls as single-trunk calls so that a single ACA-referral call is made if an ACA-referral call is required. The call is on the lowest B-channel that is associated with the wideband call.

- Call Coverage

  A WAE cannot be administered as a coverage point in a call-coverage path.

- Call Detail Recording (CDR)

  When CDR is active for the trunk group, all wideband calls generate CDR records. The CDR feature flag indicates a data call, and CDR records contain bandwidth and Bearer Capability Class (BCC).

- Call Forwarding

  You must block Call Forwarding through Class of Service (COS).

- Call Management System (CMS) and Basic Call Management System (BCMS)

  Wideband calls can be carried over trunks that are measured by CMS and BCMS. Wideband endpoints are not measured by CMS and BCMS.

- Call Vectoring

  PRI endpoints use a vector directory number (VDN) to dial. For example, PRI endpoint 1001 dials VDN 500. VDN 500 points to Vector 1. Vector 1 can point to other PRI endpoints such as route-to 1002, or route-to 1003, or busy.

  Certain applications use Call Vectoring. When an incoming wideband call hunts for an available wideband endpoint, the call can point to a VDN, that sends the call to the first available PRI endpoint.

- Class of Restriction (COR)

  COR identifies caller and called-party privileges for PRI endpoints. Administer the COR so that account codes are not required. Forced entry of account codes (FEAC) is turned off for wideband endpoints.

- Class of Service (COS)

  COS determines the class of features that a wideband endpoint can activate.

- Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS)

  FAS and NFAS with or without D-Channel Backup requires administration by way of signaling groups for trunk-side wideband interfaces.

- Facility Busy Indication

  You can administer a busy-indicator button for a wideband-endpoint extension, but the button does not accurately track endpoint status.

- Facility Test Calls

  Use Facility Test Calls to perform loop-back testing of the wideband call facility.

- Generalized Route Selection (GRS)

  GRS supports wideband BCC to identify wideband calls. GRS searches a route pattern for a preference that has wideband BCC. Route preferences that support wideband BCC also support other BCCs to allow different call types to share the same trunk group.

- CO Trunk (TTC - Japan) Circuit Pack

  The CO Trunk (TTC - Japan) circuit pack cannot perform wideband switching. No member of the circuit pack should be a member of a wideband group.

World Class Routing

Use the World Class Routing feature to direct outgoing calls. The World Class Routing feature has two capabilities, Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS).

- Automatic Alternate Routing (AAR) routes calls within your company over your own private network.

  The system converts the number that the user dials. The system then analyzes the number, and routes the call as a private-network call.

- Automatic Route Selection (ARS) routes calls that go outside your company over public networks. ARS also routes calls to remote company locations if you do not have a private network.

  The system converts the number that the user dials. The system then analyzes the number, and routes the call as a public network call.

Automatic routing starts when a user dials a Feature Access Code (FAC) and then the number that the user wants to call. The system analyzes the dialed digits, selects the route for the call, and deletes and inserts digits, if necessary. The system then routes the call over the trunks that you specify in your routing tables. AAR and ARS can access the same trunk groups, and share the same route patterns and other routing information. ARS calls can be converted to AAR calls, and AAR calls can be converted to ARS calls.

The FAC for AAR is usually the digit 8. The FAC for ARS is usually the digit 9 in the US and 0 outside the US. When your Avaya technician or business partner sets up AAR on your server that is running Communication Manager, he or she usually assigns the FAC for AAR. You can administer your own FAC for ARS. With Communication Manager 2.0, you can also use ARS without a FAC.

Detailed description of World Class Routing

This section provides a detailed description of the World Class Routing feature:

- Overview of automatic routing
- Understanding ARS analysis
- Examples of digit conversion
- ARS dialing without a FAC
- AAR and ARS partitioning

Overview of automatic routing

The following figure (Figure 426: Automatic Routing Overview on page 1691) shows an overview of automatic routing:

Figure 426: Automatic Routing Overview

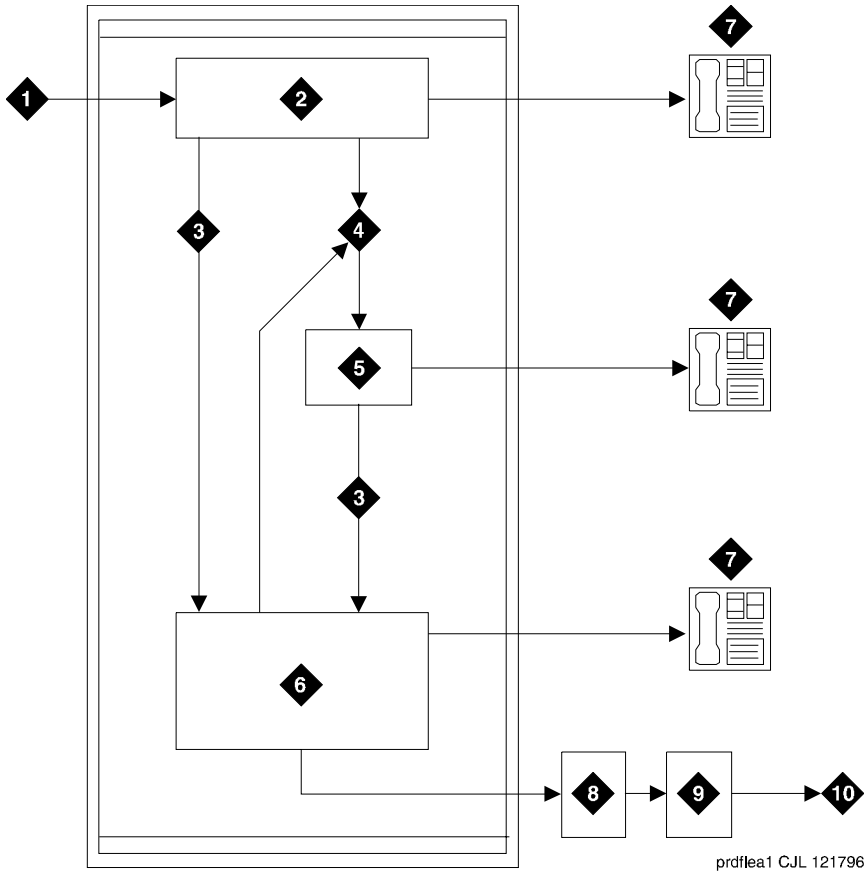


Figure notes:

1. Receive input from a telephone, a public network trunk, or a private network trunk.
2. Analyze the digits to determine the address type from the Dial Plan Analysis Table.
3. Direct the call to Automatic Alternate Routing (AAR) or Automatic Route Selection (ARS).
4. Direct the call to the Uniform Dial Plan (UDP).
5. Use the UDP to determine the route.
6. Delete and insert digits based on the ARS Digit Analysis Table.
7. Terminate the call at the telephone.
8. Analyze the digits based on information from the ARS Digit Analysis Table. Determine the route pattern.
9. Select an outgoing trunk group and delete and insert digits.
10. Send the call to a public network trunk or a private network trunk.

Understanding ARS analysis

With ARS, the system checks the digits in the called number against an ARS Digit Analysis Table to determine how to handle the dialed digits. The system also uses Class of Restriction (COR) and Facility Restriction Level (FRL) to determine the calling privileges.

- Dialed string. Lists the first digits in the dialed string. When a user makes an outgoing call, the system analyzes the digits, and looks for a match in the table. The system then uses the information in the matching row to determine how to route the call.

  For example, if a caller places a call to 1-303-233-1000, the system matches the dialed digits with the digits in the first column of the table. In this example, the dialed string matches the digit 1. Then the system matches the length of the entire dialed string (11 digits) to the minimum (Min) and the maximum (Max) length columns. In this example, the 11-digit call that started with 1 follows route pattern 30 as an fnpa call.

  The first dialed digit for an external call is often an access code. If the digit 9 is defined as the ARS access code, the system drops this digit and uses the ARS Analysis Table to analyze the remaining digits.
- Route Pattern. Indicates the route that handles the calls that match the dial string.
- Call Type. Describes what kind of call is made with this dial string. Call Type helps the system determine how to handle the dialed string.
- Node Num. States the number of the destination node in a private network, if you use node number routing or Distributed Communication System (DCS). Valid values are 1 to 999, or blank.

For more information, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

Examples of digit conversion

The system uses the AAR or ARS Digit Analysis Table to change a dialed number for more efficient routing. Digits can be inserted or deleted from the dialed number. For instance, you can tell the system to delete a 1 and an area code on calls to one of your locations, and avoid long distance charges by routing the call over your private network.

The ARS digit conversion examples in this section use the following values:

- ARS Feature Access Code = 9
- AAR Feature Access Code = 8
- Private Network Office Code (also known as Home RNX) = 222
- Also, in these examples, Prefix 1 is required on all long-distance Direct Department Dialing (DDD) calls, and dashes (-) are for readability only.

The system maps the dialed digits to the pattern that most closely matches the dialed number. For example, if the dialed string is 957-1234 and the table contains the matching patterns 957-1 and 957-123, the match is on pattern 957-123.

ARS dialing without a FAC

The following table (Table 125: ARS digit conversion examples on page 1693) shows examples of how ARS converts dialed digits.

Table 125: ARS digit conversion examples

Operation	Actual digits dialed	Matching pattern	Replacement string	Modified address	Notes
DDD call to an Electronic Tandem Network (ETN)	9-1-303-538-1345	1-303-538	362	362-1345	The system routes the call through AAR for RNX 362.
Long distance call to a specified carrier	9-10222+DDD	10222	(blank)	(blank)	The system routes the call as dialed with DDD over the private network.
Terminating a local DDD call to an internal telephone	9-1-201-957-5567 or 9-957-5567	1-201-957-5 or 957-5	222-5	222-5567	The system routes the call to RNX 222, ext. 5567.
Unauthorized call to intercept treatment	9-1-212-976-1616	1-XXX-976	The pound key (#)	(blank)	The pound key (#) means the end of dialing. ARS ignores the digits that are dialed after 976. The user gets intercept treatment.
International call to an attendant	9-011-91-672530	011-91	222-0111#	222-0111	The system routes the call to the local server (RNX 222), and then to an attendant (222-0111).

1 of 2

Table 125: ARS digit conversion examples (continued)

Operation	Actual digits dialed	Matching pattern	Replacement string	Modified address	Notes
International call to an announcement (This method can also be used to block unauthorized IDDD calls.)	9-011-91-672530	011-91	222-1234#	222-1234	The system routes the call to the local server (RNX 222), and then to an announcement extension (222-1234).
International call from certain European countries that need dial tone detection	0-00-XXXXXXXX	00	+00+	00+XXXX	The first 0 indicates ARS, the second pair of 0s indicates an international call. The plus signs (+) tell the system to wait for dial tone detection.

2 of 2

This feature allows users to place calls without the need to first dial a Feature Access Code (FAC), such as the number 9, to access an outside line. The system recognizes the call as an ARS or an AAR call, and accordingly uses the ARS or the AAR digit analysis and digit conversion tables to route the call. This enhancement was added to the Communication Manager Release 2.0.

This feature provides for the following additional calling options:

- Public network dialing. This feature eliminates the need to enter a FAC to gain access to a public network facility or trunk. The typical application is apartments or assisted living complexes that want to provide the sense that users can directly dial the public network.
- UDP networks. Many customers have large networks with 5-digit UDPs that have that have "run out of numbers." This feature allows you to extend the network dial plan. The DCS feature transparency is available only with 4-digit and 5-digit dialing plans.
- QSIG networks. The QSIG implementation does not require a 4-digit or a 5-digit UDP like DCS. An expanded private-network dial plan makes it easier to integrate the system into existing customer enterprise networks that are made up of non-Communication Manager systems. An expanded dial plan also facilitates those customers who want to convert a large DCS network to QSIG signaling protocol. DCS is not supported for private-network dial plans that are greater than 5-digits.
- 3-Digit UDP. ARS dialing without a FAC allows 3-digit UDP. However, DCS does not work in a dial scheme of less than 4 digits. For feature transparency, QSIG must be used for signaling.

Avaya recommends that you use ARS or AAR Dialing without a FAC only when users dial outside central office (CO) trunks. If you use this feature to expand dial plan lengths beyond 7-digits for internal extensions across a private QSIG or DCS network, some feature interactions might occur. Such interactions can include changes in the information that is shown on display telephones, telephony features, and call center features. ARS and AAR Dialing without a FAC is not tested against all possible feature interactions in an intraswitch networked environment. Avaya does not recommend ARS and AAR Dialing without a FAC for this use.

Extensions

A dialable extension is an extension that is can be dialed without going through ARS or AAR routing.

A nondialable extension is an extension that can only be dialed using ARS or AAR routing. You cannot dial a nondialable extension as it is administered. You must dial a nondialable extension with a prefix as a longer number than the administered extension.

An internal extension is the normal extension of 3 to 5 digits as administered on a telephone.

Use the following general rules to determine how nondialable extensions interact with a particular feature:

- When a user dials an extension directly from a telephone, or the system dials an extension when a feature is invoked, the ARS or AAR Dialing without a FAC feature must be used.
- When a feature, such as Coverage Paths or Security Violation Notification (SVN), is being administered on behalf of a telephone user, the internal extension must be dialed through the administration tool.

AAR and ARS partitioning

You can use AAR and ARS partitioning to change the call routing plan for up to eight different user groups on a single server that is running Communication Manager.You assign a Partition Group Number (PGN) to each user group and identify different call routing treatment for each PGN.

For example, you can partition hotel employees and guests into separate groups and route the calls differently. When a guest makes a long distance call, the guest's PGN and digit analysis tables route the call to a telephone billing system that allocates long distance charges. The system routes a similar call placed by an employee over a DDD trunk.

Partition user groups are used only with AAR, ARS, and UDP. You can assign AAR and ARS partitioning to telephones, attendant consoles, remote-access users, data endpoints, and incoming trunks.

Use partitioning for:

- Groups that have different routing because of special billing needs
- Groups that have dedicated use of a particular network facility

- Groups in different businesses that are serviced by a single system
- Data users who require special facility types on outgoing calls

You can assign a route pattern to just one partitioned user group, or you can assign a route pattern to all partitioned user groups.

Administering World Class Routing

The following steps are part of the administration process for World Class Routing:

- Using COR and FRL to manage calling privileges
- Assigning a FAC for ARS
- Setting up a location ARS FAC
- Displaying ARS analysis information
- Administering the route pattern
- Defining call types
  - Defining operator-assisted calls
  - Defining interexchange carrier calls
- Using restricted area codes and prefixes
- Using wildcards
- Defining local information calls
- Modifying call routing
  - Adding a new area code
  - Adding a new prefix
  - Using ARS to restrict outgoing calls
- Defining ARS partitions
  - Setting up partition groups
  - Assigning a telephone to a partition group
- Setting up Time of Day Routing

This section describes:

- Any prerequisites for administering the ARS feature
- The screens that you use to administer the ARS feature
- Complete administration procedures for the ARS feature

Screens for administering World Class Routing

Screen name	Purpose	Fields
Station	Change the calling privileges of a telephone.	**COR**
Locations	Create a location ARS Feature Access Code (FAC).	**ARS Prefix 1 Required For 10-Digit NANP Calls?**
AAR and ARS Digit Analysis Table	Define call types and interexchange carrier calls.	**Dialed String**
ARS Digit Analysis Table	Use wild cards.	• **Dialed String** • **Total Min and Total Max** • **Route Pattern** • **Call Type**
ARS Digit Analysis Table	Define local information calls.	• **Dialed String** • **Total Min and Total Max** • **Route Pattern** • **Call Type**
• ARS Chosen Report • ARS Digit Analysis Table	Add a new area code or a prefix.	• **Total Min and Total Max** • **Route Pattern** • **Call Type** • **Node Num**
ARS Digit Analysis Table	Restrict outgoing calls.	• **Dialed String** • **Total Min and Total Max** • **Route Pattern** • **Call Type**
• ARS Chosen Report • Partition Routing Table	Set up partition groups.	• **Route Pattern** • **PGN**
• Class of Restriction Information • Authorization Code-COR Mapping	Assign a telephone to a partition group.	• **COR description** • **Partition Group Number**
Time of Day Routing Plan	Set up time of day routing.	• **All** • **PGN**

Using COR and FRL to manage calling privileges

Each time that you set up a telephone, you use the Station screen to assign a Class of Restriction (COR). You can create different CORs for different groups of users. For example, you might want executives in your company to have different calling privileges than receptionists.

When you set up a COR, you specify a facility restriction level (FRL) on the Class of Restriction screen. The FRL determines the calling privileges of the user. FRLs are ranked from 0 to 7, where 7 has the highest level of privileges.

You also assign an FRL to each route pattern preference on the Route Pattern screen. When a user makes a call, the system checks the COR of the user. The call is allowed if the FRL of the caller is higher than or equal to the FRL of the route pattern preference.

Suppose that you are setting up a telephone for a new executive. The current translations assign COR 1, with outward restrictions and an FRL of 0, which is the lowest permission level available. You want to assign a COR with the highest level of permissions, FRL 7.

To change the COR of a telephone:

1. Type **`change station n`**, where ***n*** is the extension. Press **Enter**.

   The system displays the Station screen (Figure 427: Station screen on page 1698).

Figure 427: Station screen

```
change station 1014                                          Page 1 of X

                              STATION

Extension: 1014               Lock Messages? n                      BCC: 0
     Type:                    Security Code:                         TN: 1
     Port:                  Coverage Path 1:                        COR: 7
     Name:                  Coverage Path 2:                        COS: 1
                            Hunt-to Station:

STATION OPTIONS
              Loss Group: 2               Personalized Ringing Pattern: 3
            Data Module? n                          Message Lamp Ext: 1014
          Speakerphone: 2-way                   Mute button enabled? y
       Display Language? English                   Expansion Module?
                   Model:
                                                  Media Complex Ext:
                                                       IP Softphone? y
                                                 Remote Office Phone? n
```

2. In the **COR** field, type the number of the new COR. In this example, the number of the new COR is **7**.

3. Press **Enter** to save your changes.

To change the FRL of a COR:

1. Type **change cor *n***, where ***n*** is the COR that you want to change. In this example, type **change cor 7**. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 428: Class of Restriction screen on page 1699) for COR 7.

Figure 428: Class of Restriction screen

```
change cor 7                                                Page 1 of 4

                          CLASS OF RESTRICTION

               COR Number: 7
          COR Description: supervisor

                      FRL: 7                                    APLT? y
  Can Be Service Observed? n               Calling Party Restriction: none
Can Be A Service Observer? y                Called Party Restriction: none
        Time of Day Chart: 1           Forced Entry of Account Codes? n
         Priority Queuing? n                     Direct Agent Calling? y
     Restriction Override: none             Facility Access Trunk Test? n
     Restricted Call List? n                      Can Change Coverage? n
   Unrestricted Call List? __ __ __ __ __ __ __ __ __ __
           Access to MCT? y                  Fully Restricted Service? n
Group II Category For MFC: 7                 Hear VDN of Origin Annc.? n
         Send ANI for MFE? n_                 Add/Remove Agent Skills? y
            MF ANI Prefix: ______             Automatic Charge Display? n
Hear System Music on Hold? y    PASTE (Display PBX Data on telephone)? n
                            Can Be Picked Up By Directed Call Pickup? n
                                       Can Use Directed Call Pickup? n
                                       Group Controlled Restriction: inactive
```

2. In the **FRL** field, type the number of the new FRL. In this example, the number of the new FRL is **7**.
3. Press **Enter** to save your changes.

   In this example, all users who are assigned COR 7 now have the highest level of calling permissions, FRL 7.

Assigning a FAC for ARS

To access the public network from an extension in your internal system, a FAC for ARS must be set up on your system. In the US, the number 9 is usually the ARS FAC to use to make an outgoing call.

To assign a FAC for ARS:

1. Type **change dialplan analysis**. Press **Enter**.

   The system displays the Dial Plan Analysis Table screen (Figure 429: Dial Plan Analysis Table screen on page 1700).

Figure 429: Dial Plan Analysis Table screen

```
display dialplan analysis                                    Page 1 of 12
                        DIAL PLAN ANALYSIS TABLE
                                                          Percent Full: 7

      Dialed  Total  Call        Dialed  Total  Call       Dialed  Total  Call
      String  Length Type        String  Length Type       String  Length Type
        00      2    attd          ____    _    ____         ____    _    ____
        1       3    dac           ____    _    ____         ____    _    ____
        2       4    ext           ____    _    ____         ____    _    ____
        3       4    ext           ____    _    ____         ____    _    ____
        3       1    aar           ____    _    ____         ____    _    ____
        4       1    ars           ____    _    ____         ____    _    ____
        4       5    ext           ____    _    ____         ____    _    ____
        5       5    ext           ____    _    ____         ____    _    ____
        5       7    ext           ____    _    ____         ____    _    ____
        6       5    ext           ____    _    ____         ____    _    ____
        7210    7    ext           ____    _    ____         ____    _    ____
        8       7    ext           ____    _    ____         ____    _    ____
        9       1    fac           ____    _    ____         ____    _    ____
        *       3    fac           ____    _    ____         ____    _    ____
        #       3    fac           ____    _    ____         ____    _    ____
```

2. In an empty row, type the number in the Dialed String column that you want to use as the FAC for ARS. In this example, the number for the FAC for ARS is **9**.
3. In the Total Length column, type **1**. This number indicates that the total number of digits for the FAC for ARS is 1 digit, the number **9**.
4. In the Call Type column, type **fac**.
5. Press **Enter** to save your changes.
6. Type **change features-access-codes**. Press **Enter**.

   The system displays the Feature Access Code (FAC) screen (Figure 430: Feature Access Code (FAC) screen on page 1701).

Figure 430: Feature Access Code (FAC) screen

```
change feature-access-codes                                    Page 1 of 7

                          FEATURE ACCESS CODE (FAC)

            Abbreviated Dialing List1 Access Code: ____
            Abbreviated Dialing List2 Access Code: ____
            Abbreviated Dialing List3 Access Code: ____
   Abbreviated Dial - Prgm Group List Access Code: ____
                        Announcement Access Code: ____
                         Answer Back Access Code: ____
                           Attendant Access Code: ____
         Auto Alternate Routing (AAR) Access Code: ____
         Auto Route Selection (ARS) Access Code 1: 9     Access Code 2: ____
                    Automatic Callback Activation: ____   Deactivation: ____
   Call Forwarding Activation Busy/DA: ____   All: ____   Deactivation: ____
                           Call Park Access Code: ____
                         Call Pickup Access Code: ____
   CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                     CDR Account Code Access Code: ____
                           Change COR Access Code: ____
                      Change Coverage Access Code: ____

                     Data Origination Access Code: ____
                         Data Privacy Access Code: ____
                 Directed Call Pickup Access Code: ____
```

7. In the **Auto Route Selection (ARS) Access Code 1** field, type the number that you set up in Step 2. In this example, type the number **9**.
8. Press **Enter** to save your changes.

Setting up a location ARS FAC

Prerequisites

You must complete the following actions before you can set up a location ARS FAC:

- On the Optional Features screen, ensure that the **Multiple Locations** field is set to **y**. If this field is set to **y**, you can administer up to 250 locations depending on the configuration of the server that is running Communication Manager. If the **Multiple Locations** field is set to **n**, information for Location No. 1 applies to all your locations.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

To set up a location ARS FAC:

1. Type **change locations**. Press **Enter**.

   The system displays the Locations screen (Figure 431: Locations screen on page 1702).

Figure 431: Locations screen

```
change locations                                              Page 1 of X

                                  LOCATIONS

                  ARS Prefix 1 Required For 10-Digit NANP Calls? y

Loc. Name                Timezone  Rule   NPA   ARS   Attd       Pre-   Proxy Sel
No                        Offset                FAC   FAC        fix    Rte pat
  1  Main                 00:00    0
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
xxx ____________________ __:__    __     ___   ____  __         _____  _________
```

2. In the **ARS Prefix 1 Required For 10-Digit NANP Calls?** field, type **y**.
3. Press **Enter** to save your changes.

Note:
The system uses the ARS access code on the Feature Access Code (FAC) screen when a location ARS does not exist. If a location ARS FAC exists, the ARS access code on the Feature Access Code (FAC) screen is denied from that location. If you use a local ARS code, the ability to administer two ARS codes on the Feature Access Code (FAC) screen is lost.

Displaying ARS analysis information

The ARS Digit Analysis Table controls how the system routes calls.

To display an ARS Digit Analysis Table:

1. Type **display ars analysis *n***, where ***n*** is the first number or numbers of the dialed string that you want to review. In this example, the number is 1. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for dialed strings that begin with the number 1 (Figure 432: ARS Digit Analysis Table screen on page 1703).

   Note that the system displays only as many dialed strings as can fit on one screen at a time.

Figure 432: ARS Digit Analysis Table screen

```
display ars analysis 1                                        Page 1 of X

                          ARS DIGIT ANALYSIS TABLE
                                  Location:  all            Percent Full:  3

      Dialed          Total    Route    Call    Node    ANI
      String        Min Max  Pattern   Type    Num     Reqd
101xxxx0            8   8     deny     op      ___     n
101xxxx0            18  18    deny     op      ___     n
101xxxx01           16  24    deny     iop     ___     n
101xxxx011          17  25    deny     intl    ___     n
101xxxx1            18  18    deny     fnpa    ___     n
1010xxx             14  18    5        ixc     ___     n
10xxx0              6   6     deny     op      ___     n
10xxx0              16  16    deny     op      ___     n
10xxx01             14  22    deny     iop     ___     n
10xxx011            15  23    deny     intl    ___     n
10xxx1              16  16    deny     fnpa    ___     n
11                  2   2     734      alrt    ___     n
120                 11  11    4        fnpa    ___     n
1200                11  11    deny     fnpa    ___     n
121                 11  11    deny     fnpa    ___     n
122                 11  11    deny     fnpa    ___     n
```

2. After you review this information, press **Cancel**.

To see all the dialed strings that are defined for your system and run an ARS Digit Analysis report:

1. Type **list ars analysis**. Press **Enter**.

   The system displays an ARS Digit Analysis Report screen for all dialed strings (Figure 433: ARS Digit Analysis Report screen on page 1704). You might want to print this report for your records.

Figure 433: ARS Digit Analysis Report screen

```
list ars analysis                                              Page 1 of X

                        ARS DIGIT ANALYSIS REPORT

                                    Location:  all

      Dialed          Total    Route    Call    Node
      String        Min Max  Pattern   Type    Num
0                   1   1      deny     op      ___
0                   8   8      deny     op      ___
0                   11  11     deny     op      ___
00                  2   2      deny     op      ___
01                  17  17     deny     op      ___
001                 10  18     deny     op      ___
101xxxx0            8   8      deny     op      ___
101xxxx0            18  18     deny     op      ___
101xxxx01           16  24     deny     iop     ___
101xxxx011          17  25     deny     intl    ___
101xxxx1            18  18     deny     fnpa    ___
10xxx0              6   6      deny     op      ___
```

2. After you review this information, press **Cancel**.

Administering the route pattern

The Route Pattern screen defines the route patterns that the server uses. Each route pattern contains a list of trunk groups that can be used to route the call. The maximum number of route patterns and trunk groups allowed depends on the configuration and the memory that is available on the system.

Use this screen to insert or delete digits so that the system routes AAR or ARS calls over different trunk groups. You can convert an AAR number into an international number, and insert an area code in an AAR number to convert an on-network number to a public network number. Also, when a call directly accesses a local central office (CO), if the long-distance carrier provided by your CO is unavailable, the system can insert the dial access code for an alternative carrier into the digit string.

To administer the route pattern for your system:

1. Type **change route-pattern *n***, where ***n*** is the number of the route pattern. Press **Enter**.

   The system displays the Route Pattern screen (Figure 434: Route Pattern screen on page 1705).

Figure 434: Route Pattern screen

```
                 Pattern Number: 1   Pattern Name:
                                       Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
   No          Mrk Lmt List Del  Digits                                QSIG
                            Dgts                                       Intw
1: 1    0  303               0   9                                     n   user
2:                                                                     n   user
3:                                                                     n   user
4:                                                                     n   user
5:                                                                     n   user
6:                                                                     n   user

    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature BAND  No. Numbering LAR
   0 1 2 3 4 W     Request                                    Dgts Format
                                                           Subaddress
1: y y y y y n  n            rest                                      none
2: y y y y y n  n            rest                                      none
3: y y y y y n  n            rest                                      none
4: y y y y y n  n            rest                                      none
5: y y y y y n  n            rest                                      none
6: y y y y y n  n            rest                                      none
```

Important:
The next step is for US customers only.

2. In the **Band** field, type a number that represents the OUTWATS band number.

   WATS is a voice-grade service that provides both voice and low-speed data transmission calls to defined areas, or bands, for a flat rate charge.

   The system displays the **Band** field when the **Services/Features** field is set to **outwats-bnd**, and when either the **ISDN-PRI** or **ISDN-BRI Trunks** field is set to **y** on the Optional Features screen. The **Band** field is required by Call-by-Call Service Selection.

3. In the **BBC Value** (Bearer Capability Class) area, type the following information in the corresponding columns. The columns are labeled **0**, **1**, **2**, **3**, **4**, and **W**.
   - In the **0** column, perform one of the following actions:
     - If the BCC is appropriate for the associated route pattern, type **y**.
     - If the BCC is not appropriate for the associated route pattern, type **n**.
   - In the **1** column, perform one of the following actions:
     - If the BCC is appropriate for the associated route pattern, type **y**.
     - If the BCC is not appropriate for the associated route pattern, type **n**.
   - In the **2** column, perform one of the following actions:

  - If the BCC is appropriate for the associated route pattern, type **y**.
  - If the BCC is not appropriate for the associated route pattern, type **n**.
- In the **3** column, perform one of the following actions:
  - If the BCC is appropriate for the associated route pattern, type **y**.
  - If the BCC is not appropriate for the associated route pattern, type **n**.
- In the **4** column, perform one of the following actions:
  - If the BCC is appropriate for the associated route pattern, type **y**.
  - If the BCC is not appropriate for the associated route pattern, type **n**.
- In the **W** column, perform one of the following actions:
  - If the BCC is appropriate for the associated route pattern, type **y**.
  - If the BCC is not appropriate for the associated route pattern, type **n**.

Information in the **BCC Value** area identifies the type of call that is appropriate for this trunk group, such as voice calls and different types of data calls. The system displays the **BCC Value** field when either the **ISDN-PRI** field or the **ISDN-BRI Trunks** field is set to **y** on the Optional Features screen.

See Table 126: Entries for the BCC Value area on page 1706 for a description of BCC Values.

Table 126: Entries for the BCC Value area

Entry	Description
0	voice-grade data and voice
1	56-kbps data (mode 1)
2	64-kbps data (mode 2)
3	64-kbps data (mode 3)
4	64-kbps data (mode 0)
W	128-kbps to 1984-kbps data (wideband)

4. In the **BCIE** field, type the value that determines the creation of the ITC codepoint in the setup message. The **BCIE** field applies to ISDN trunks.
   - Type **ept** for endpoint.
   - Type **unr** for unrestricted.

   The system displays the **BCIE** field when the **ITC** field is set to **both**.

5. In the **CA-TSC** field, type the information for ISDN B-channel connections.

   See Table 127: Entries for the CA-TSC field on page 1707 for a description of the entries for the **CA-TSC field.**

Table 127: Entries for the CA-TSC field

Entry	Description
as-needed	The CA-TSC is set up only when needed. This setting causes a slight delay. Avaya recommends this entry for most situations.
at-setup	The CA-TSC is automatically set up for every B-channel call whether or not it is needed.
none	No CA-TSC is set up. This setting permits tandeming of NCA-TSC setup requests.

6. In the **DCS/QSIG Intw**, field perform one of the following actions:
   - To enable CS/QSIG Voice Mail Interworking, type **y**.
   - To disable CS/QSIG Voice Mail Interworking, type **n**.

   The system displays the **DCS/QSIG Intw** field when the **Interworking with DCS** field is set to **y** on the Optional Features screen.

7. In the **FRL** field, type the Facility Restriction Level (FRL) that is associated with the preference.

   Valid values are the digits **0** through **7**.

   0 is the least restrictive FRL, and 7 is the most restrictive FRL. To access the associated trunk-group, the FRL of the calling party must be greater than, or equal to, the FRL that you typed on this screen.

   SECURITY ALERT:
   For system security reasons, Avaya recommends that you use the most restrictive FRL possible.

8. In the **Grp No field**, type the trunk group number that is associated with the preference.
   - Valid values are the digits **1** through **666** for DEFINITY R, CSI, and SI.
   - Valid values are the digits **1** through **2000** for the S8300 Server, IP-PNC, and the S8700 Multi-Connect.

9. In the **Hop Lmt** field, type the number of hops for each preference. A *hop* occurs when a call tandems through a media server or a system to another destination. You limit the number of hops to prevent circular hunting, which ties up trunk facilities without completing a call. The software blocks the number of hops that are equal to or greater than the number that you enter in the **Hop Lmt** field.

   See Table 128: Entries for the Hop Lmt field on page 1708 for the **Hop Lmt** field entries.

Table 128: Entries for the Hop Lmt field

Entry	Description
blank	Indicates that the system does not apply a limit to the number of hops for this preference.
1 to **9**	Limits the number of hops if you use the Tandem Hop capability. Valid values are the digits **1** to **9**.
1 to **32**	Limits the number of hops if you use the Transit capability. Valid values are the digits **1** to **32**.

10. In the **Inserted Digits** field, type the digits that the software inserts for routing.

    Valid values are the digits **0** through **9**. You can type a maximum of 36 digits.

    The software can send a maximum of 52 digits. This number includes the digits that you enter in the **Inserted Digits** field, plus the digits that the user dials. The software counts each special symbol as 2 digits.

    See Table 129: Entries for the Inserted Digits field on page 1708 for the **Inserted Digits** field entries.

Table 129: Entries for the Inserted Digits field

Entry	Description
asterisk (*****)	When an asterisk (*) is in the route pattern and the outgoing trunk is signaling type **mf**, the MFC tone for the "end-of-digits" is sent out to the central office (CO) in place of the asterisk (*).
pound sign (**#**)	When the pound sign (#) is in the route pattern and the outgoing trunk is signaling type **mf**, the MFC tone for the "end-of-digits" is sent out to the central office (CO) in place of the pound sign (#).
comma (**,**)	A comma (,) uses 2 places. A comma (,) creates a 1.5-second pause between the digits that are sent. Do not use a comma (,) as the first character in the string unless it is absolutely necessary. Misuse can result in some calls, such as Abbreviated Dialing or Last Number Dialed calls, not completing.
plus sign (+)	The plus sign (+) waits for dial tone up to the **Off Premises Tone Detection Timer**. The system then sends either digits or intercept tone, based on value in the **Out Pulse Without Tone** field on the Feature-Related System Parameters screen.
percent sign (**%**)	The percent sign (%) starts End-to-End Signaling.
exclamation point (**!**)	An exclamation point (!) waits for dial tone without timeout, and then sends dual-tone multifrequency (DTMF) digits.
	1 of 2

Table 129: Entries for the Inserted Digits field (continued)

Entry	Description
ampersand (&)	An ampersand (&) waits for Automatic Number Identification (ANI). An ampersand (&) is used for Russian pulse trunks.
p	The associated trunk group must be of type "sip." Type the single digit p for fully qualified E.164 numbers. The system translates the p to a plus sign (+). The system then places the plus sign (+) at the front of the digit string.
dollar sign ($)	If ($) sign is in the Inserted Digit String of a routing pattern, the MF Packet does not have ANI information. That is, use "1" S F11 format. If ($) is not in the Inserted Digit String of a routing pattern, the MF Packet shall have the "1" S Cs def xxxx F11 format.
	2 of 2

11. In the **ITC** field, type the Information Transfer Capability (ITC) to identify the type of data transmission or traffic that this routing preference can carry. The ITC applies only to data calls BCC 1 through 4.

    If the **W** column of the **BCC** field is set to **y**, the **ITC** field must be set to either **unre** or **both**.

    See Table 130: Entries for the ITC field on page 1709 for **ITC** field entries.

Table 130: Entries for the ITC field

Entry	Description
both	Calls from restricted and unrestricted endpoints can access the route pattern.
rest	Calls from restricted endpoints can access the route pattern.
unre	Calls from unrestricted endpoints can access the route pattern.

12. In the **IXC** field, type the Inter-Exchange Carrier (IXC). The system uses this information for calls that the system routes through an IXC, and for the Call Detail Recording (CDR) feature.

    The system displays the **IXC** field when the **ISDN-PRI** field or **ISDN-BRI Trunks** field is set to **y** on the Optional Features screen.

    See Table 131: Entries for the IXC field on page 1710 for IXC field entries.

Table 131: Entries for the IXC field

Entry	Description
Valid carrier code	Identifies the carrier for IXC calls.
user	Identifies a presubscribed carrier. Used when an IXC is not specified.
none	The **IXC** field must be **none** for non-ISDN trunk groups and for Bellcore NI-2 Operator Service Access. If you need to send an IXC code for a non-ISDN trunk group, type the IXC code in the **Inserted Digits** field.

13. In the **LAR** field, type the routing-preference for Look Ahead Routing (LAR).

    See Table 132: Entries for the LAR field on page 1710 for LAR field entries.

Table 132: Entries for the LAR field

Entry	Description
next	Go to the next routing preference and attempt the call again.
rehu	Rehunt within the current routing-preference for another trunk to attempt the call again.
none	LAR is not enabled for the preference.

14. In the **No. Del. Digits** field, type the total number of digits that you want the system to delete before the system sends the number out on the trunk.

    Valid values are the digits **0** through **28**. You can also set the field to blank. To set the field to blank, press **Clear**.

    The software uses this information to modify the dialed number so that the system routes an AAR or ARS call over different trunk groups that terminate in media servers or systems with different dial plans. The software uses this information for the calls that use the following routing methods:

    - To or through a remote media server or switch
    - Over tie trunks to a private network server or switch
    - Over CO trunks to the serving CO

15. In the **No. Dgts Subaddress** field, type the number of dialed digits to send in the calling party subaddress information element (IE).

    You can change the **No. Dgts Subaddress** field if the **ISDN Feature Plus** field is set to **y** on the Optional Features screen.

    Valid values are the digits **1** through **5**. You can also set the field to blank. To set the field to blank, press **Clear**.

    The software uses this information to route a call to a number where the media server deletes the dialed number and inserts the listed directory number (LDN). The LDN is then sent to the destination address, and the dialed extension is sent in the calling party subaddress IE. At the receiving end, the call terminates to the user who is indicated by the subaddress number instead of to the attendant.

16. In the **NPA** field, type the 3-digit Numbering Plan Area (NPA) for the terminating endpoint of the trunk group. The NPA is also known as the area code.

    Valid values are the digits **0** through **9**. You can also set the field to blank. To set the to field blank, press **Clear**.

    For WATS trunks, the terminating NPA is the same as the home NPA unless the local exchange carrier (LEC) requires 10 digits for local NPA calls.

    Call your local telephone company to verify the NPA, if you need help.

    You do not need to enter an NPA for AAR.

17. In the **Numbering Format** field, type the information that specifies the format of the routing number that the system uses for the ISDN trunk groups for this preference.

Note:
To access the Bellcore NI-2 Operator Service Access, you must type **unk-unk** in the **Inserted Digits** field.

The system displays the **Inserted Digits** field when the **ISDN-PRI or ISDN-BRI Trunks** field is set to **y** on the Optional Features screen.

See Table 133: Entries for the Numbering Format field on page 1712 for **Numbering Format** field entries.

Table 133: Entries for the Numbering Format field

Entry	Numbering Plan Identifier	Type of Numbering
blank	E.164(1)	1-MAX
natl-pub	E.164(1)	national(2)
intl-pub	E.164(1)	international(1)
locl-pub	E.164(1)	local/subscriber(4)
pub-unk	E.164(1)	unknown(0)
lev0-pvt	Private Numbering Plan - PNP(9)	local(4)
levl0-pvt (use this entry to allow Network Call Redirection / Transfer	-	-
lev1-pvt	Private Numbering Plan - PNP(9)	Regional Level 1(2)
lev2-pvt	Private Numbering Plan - PNP(9)	Regional Level 2(1)
unk-unk	unknown(0)	unknown(0)

The **Pattern Number** field is a display-only field that displays the route pattern number. The route pattern number is from **1** to **640**.

18. In the **Prefix Mark** field, type the prefix mark information for ARS.

    Valid values are the digits **0** through **4**. You can also set the field to blank. To set the field to blank, press **Clear**.

    This entry is not required for AAR.

    Prefix marks set the requirements for sending a prefix digit 1 to indicate a long distance call. Prefix marks apply to 7-digit Direct Distance Dialing (DDD) or 10-digit DDD public network calls. A prefix digit 1 is sent only when the **call type** field is a foreign number plan area (FNPA) or a home numbering plan area (HNPA) in the ARS Digit Analysis Table screen.

    For a WATS trunk, the prefix mark is the same as the local CO trunk.

    See Table 134: Entries for the Prefix Mark field on page 1713 for **Prefix Mark** field entries.

Table 134: Entries for the Prefix Mark field

Entry	Description
0	• Suppress a user-dialed prefix digit 1 for 10-digit FNPA calls. • Leave a user-dialed prefix digit 1 for 7-digit HNPA calls. • Leave a prefix digit 1 on 10-digit calls that are not FNPA or HNPA calls. Do not use Prefix Mark **0** in those areas where all long distance calls must be dialed as 1 plus 10 digits. Check with your local network provider.
1	Send a 1 on all 10-digit calls, but not on 7-digit calls. Use Prefix Mark 1 for HNPA calls that require a 1 to indicate long distance calls.
2	Send a 1 on all 10-digit and 7-digit long distance calls. Prefix Mark 2 uses a Toll Table to define long distance codes.
3	Send a 1 on all long distance calls, and keep or insert the NPA so that all long distance calls are 10-digit calls. The system inserts the NPA when a user dials a prefix digit 1 plus 7 digits. Prefix Mark 3 uses a Toll Table to define long distance codes.
4	Always suppress a user-dialed Prefix digit 1. Use Prefix Mark 4, for example, when the system routes ISDN calls to a media server or a system that rejects calls with a prefix digit 1.
blank	For TIE trunks, leave this field blank.

19. In the **Service/Feature** field, type the IE in a call in this route pattern.

    Valid values are from 1 to 15 characters.

    The **Service/Feature** field is required by Call-by-Call Service Selection, and Network Call Redirection and Transfer.

    The system displays the **Service/Feature** field when the **ISDN-PRI** field or the **ISDN-BRI Trunks** field is set to **y** on the Optional Features screen.

    See Table 135: Entries for the Service/Feature field on page 1713 for **Service/Feature** field entries.

    Table 135: Entries for the Service/Feature field

Entry	Description
accunet	-
i800	-
inwats	-
lds	-
mega800	-

Table 135: Entries for the Service/Feature field

Entry	Description
megacom	-
multiquest	-
operator	-
oper-lds	Operator and lds
oper-meg	Operator and megacon
oper-sdn	Operator and sdn
outwats-bnd	-
sdn	Enter to allow Network Call Redirection/Transfer.
sub-operator	-
sub-op-lds	Suboperator and lds
sub-op-meg	Suboperator and megacom
sub-op-sdn	Suboperator and sdn
wats-max-bnd	-

20. In the **Toll List** field, type the number of the ARS Toll Table that is associated with the terminating NPA of the trunk group. You must complete this field if the **Prefix Mark** is set to **2** or **3**.

    Valid values are the digits **1** through **32**. You can also set the field to blank. To set the field to blank, press **Clear**.

    This entry is not required for AAR.

21. In the **TSC** field, perform one of the following actions:

    - Type **y** if you want:
      - To allow Call-Associated TSCs, and to allow incoming Non-Call-Associated TSC requests to be tandemed out for each preference
      - Feature transparency on DCS+ calls and to use QSIG Call Completion
    - Type **n** if you do not want:
      - To allow Call-Associated TSCs, and to allow incoming Non-Call-Associated TSC requests to be tandemed out for each preference
      - Feature transparency on DCS+ calls and to use QSIG Call Completion

Defining call types

To define call types, you must complete the following procedures:

- Defining operator-assisted calls
- Defining interexchange carrier calls

Defining operator-assisted calls

To define operator-assisted calls, the user first dials 9 to access ARS, then a 0, and the rest of the number.

To see how the system handles a call to an operator:

1. Type **display ars analysis 0**. Press **Enter**.

   The system displays an ARS Digit Analysis Table screen for dialed strings that begin with the number 0 (Figure 435: ARS Digit Analysis Table screen on page 1715). The table in this example shows six translations for calls that begin with the number 0.

Figure 435: ARS Digit Analysis Table screen

```
display ars analysis 1                                        Page 1 of X

                            ARS DIGIT ANALYSIS TABLE
                                   Location:  all             Percent Full:  3

      Dialed          Total    Route    Call    Node    ANI
      String        Min Max  Pattern   Type    Num     Reqd
0                   1   1     deny     op      ___     n
0                   8   8     deny     op      ___     n
0                   11  11    deny     op      ___     n
00                  2   2     deny     op      ___     n
01                  17  17    deny     op      ___     n
001                 10  18    deny     op      ___     n
```

2. After you review this information, press **Cancel**.

Use the ARS Digit Analysis Table screen that is shown in Figure 435: ARS Digit Analysis Table screen on page 1715 to follow the routing, in this example, for an operator-assisted call to New Jersey.

1. A user dials **9 0 908 956 1234**.
2. The system:
   a. Ignores the ARS FAC, which is **9** in this example
   b. Reviews the ARS Digit Analysis Table for **0**

c. Determines that the user dialed more than 1 digit

d. Determines that the user dialed 11 digits

e. Rules out the dialed strings for 00, 01, and 011

3. The system then routes the call as an operator-assisted call.

Defining interexchange carrier calls

Interexchange carrier (IXC) numbers directly access your long distance carrier lines. IXC numbers begin with 1010. After 1010, IXC numbers include 3 digits, plus the number, including 0, 00, or 1 plus10 digits. These numbers are set up on your default translations.

Remember that the user first dials 9 in this example to access ARS, and then dials the rest of the number.

To route an ARS call to an IXC:

1. Type **display ars analysis *n***, where ***n*** is the first number or numbers of the dialed string that you want to review. In this example, the number is 1. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for numbers that begin with the number 1 (Figure 432: ARS Digit Analysis Table screen on page 1703).

   If you use an **x** in the **Dialed String** field, the system recognizes the **x** as a wildcard. The **x** represents any digit from 0 to 9. If you dial 1010, the next 3 digits always match the **x** wildcard in the dialed string.

2. After you review this information, press **Cancel**.

Use the ARS Digit Analysis Table shown in Figure 432: ARS Digit Analysis Table screen on page 1703 to follow the routing, in this example, for an IXC call to AT&T. 1010288 is the carrier access code for AT&T.

1. A user dials **9 1010288**, plus a public network number.
2. The system:

   a. Ignores the ARS FAC, which is **9** in this example

   b. Reviews the ARS Digit Analysis Table for **1010**

   c. Analyzes the number.

3. The system then matches **288** with **xxx*,*** and sends the call over route pattern 5.

Using restricted area codes and prefixes

Certain area code numbers are set aside in the North American Numbering Plan. For example, these numbers are 200, 300, 400, 500, 600, 700, 800, 877, 888, and 900. You must specifically deny calls made to area codes 200 through 900, except 800, 877, and 888.

If you do not want to incur charges, you can also deny access to the 976 prefix. The 976 prefix is set aside in each area code for pay-per-call services. You can block 976 or any other prefix in all Numbering Plan Areas (NPAs) with a single entry in the digit analysis table.

You can set the 200 area code apart from other area codes 201 through 209. We use the digit analysis table 120 because it defines long distance calls that begin with 1 and all area codes from 200 through 209.

To deny long distance calls to a restricted area code:

1. Type **change ars analysis *n***, where ***n*** is the first number or numbers of the dialed string that you want to review. In this example, the number is 120. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for calls that begin with the numbers 120 (Figure 436: ARS Digit Analysis Table screen on page 1717). The table in the example shows two definitions for calls that begin with the numbers 120.

Figure 436: ARS Digit Analysis Table screen

```
change ars analysis 120                                        Page 1 of X

                            ARS DIGIT ANALYSIS TABLE
                                  Location:  all            Percent Full:  6

      Dialed          Total    Route    Call    Node    ANI
      String        Min Max  Pattern   Type    Num     Reqd
120                 11  11    4        fnpa    ___     n
1200                11  11    deny     fnpa    ___     n
```

2. After you review this information, press **Cancel**.

Use the ARS Digit Analysis Table shown in Figure 436: ARS Digit Analysis Table screen on page 1717 for the next two examples.

Follow the routing for the long distance call, in this example, that begins with 120, where the call is permitted. The 120 translation handles all dialed strings from 1201 through 1209.

1. A user dials **9 120**, plus 8 digits, the first of which is not 0.
2. The system:
   a. Ignores the ARS FAC, which is **9** in this example
   b. Reviews the ARS Digit Analysis Table for the numbers **120**
   c. Analyzes the number
   d. Determines that the call is long distance
   e. Sends the call over Route Pattern 4.

Now follow the routing for the call, in this example, that begins with the restricted area code 200:

1. A user dials **9 1200**, plus 7 digits.

2. The system:
   a. Ignores the ARS FAC, which is **9** in this example
   b. Reviews the ARS Digit Analysis Table for the numbers **1200**
   c. Analyzes the number
   d. Determines that the Call Type is **deny**. The call does not go through.

Using wildcards

You can use wildcards to help control calls to certain numbers. When you use the wildcard **x** in the **Dialed String** field, the system recognizes **x** as any digit from 0 to 9.

For this example, use wildcards to restrict users from making calls to a 555 information operator where you might incur charges. The wildcards in this example represent any area code that the user might dial.

To use wildcards to prevent callers from placing calls to a restricted number:

1. Type **`change ars analysis n`**, where ***n*** is the first number or numbers of the dialed string that you want to review. In this example, the number is 1. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for dialed strings that begin with the number 1 (Figure 432: ARS Digit Analysis Table screen on page 1703).
2. Click **Next** if necessary until you see a blank field.
3. In the Dialed String column, type **1xxx555**.

   In this example, the:

   — **1** indicates a long distance call
   — **xxx** indicates any three numbers, or area code, from 000 to 999
   — **555** indicates the extension prefix that you want to restrict
4. In the Total Min and the Total Max columns, type **11**.

   In this example, the number **11** in both columns indicates that total length of the dialed number must be 11 digits.
5. In the Route Pattern column, type **deny**.
6. In the Call Type column, type **fnhp**.
7. Press **Enter** to save your changes.

Defining local information calls

You might want users to access local information. In this example, allow users to dial extension 411 to access local information.

To allow local information calls:

1. Type **change ars analysis *n***, where ***n*** is the first number or numbers of the dialed string that you want to review. In this example, the number is 4. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for dialed strings that begin with the number 4 (Figure 437: ARS Digit Analysis Table screen on page 1719).

Figure 437: ARS Digit Analysis Table screen

```
change ars analysis 4                                          Page 1 of X

                            ARS DIGIT ANALYSIS TABLE
                                  Location:  all            Percent Full:  6

      Dialed          Total    Route    Call    Node    ANI
      String        Min Max  Pattern   Type    Num     Reqd
411                 3   3      1       svcl    ___     n
5                   7   7      2       hnpa    ___     n
6                   7   7      2       hnpa    ___     n
7                   7   7      2       hnpa    ___     n
911                 3   3      1       svcl    ___     n
```

2. Click **Next** if necessary until you see a blank field.
3. In the Dialed String column, type the string of numbers that you want to change.

   In this example, type **411**.
4. In the Total Min and the Total Max columns, type the minimum number of digits, and the maximum number of digits, that you want the system to analyze.

   In this example, the number **3** in both columns indicates that total length of the dialed number must be 3 digits.
5. In the Route Pattern column, type a routing pattern number.

   In this example, type the number **1**.
6. In the Call Type column, type **svcl**.

   The call type **svcl** indicates a service call.
7. Press **Enter** to save your changes.

Modifying call routing

To modify call routing, you must complete the following procedures:

- Adding a new area code
- Using ARS to restrict outgoing calls

If your system uses ARS Digit Analysis to analyze dialed strings and select the best route for a call, you must change the digit analysis table to modify call routing. For example, you need to update this table to add new area codes, or to restrict users from calling specific areas or countries.

Adding a new area code

Sometimes, area codes within a region might change. In this example, area code 415 has split into two area codes, 415 and 650. Add a new nonlocal area code, 650, to have the same values as the existing nonlocal area code on your system, 415.

To add a nonlocal area code:

1. Type **`list ars route-chosen`**, the number ***`1`***, the existing area code, and any 7-digit telephone number. For this example, type **`list ars route-chosen`** ***`14152223333`***. Press **Enter**.

   The system displays the ARS Route Chosen Report screen (Figure 438: ARS Route Chosen Report screen) for number 14152223333.

Figure 438: ARS Route Chosen Report screen

```
list ars route-chosen 14152223333                              Page 1 of X

                          ARS ROUTE CHOSEN REPORT

    Location: 1                        Partitioned Group Number:  1

     Dialed              Total      Route    Call      Node      Location
     String             Min  Max    Pattern  Type      Number
     141                11   11     30       fnpa                all
```

2. Remember the **Total Min**, **Total Max**, **Route Pattern**, and **Call Type** values on this screen. In this example, the **Total Min** is **11**, the **Total Max** is **11**, the **Route Pattern** is **30**, and the **Call Type** is **fnpa**.
3. After you review this information, press **Cancel**.

In this example, add a new area code 650 that has the same values as area code 415.

1. Type **change ars analysis *n***, where ***n*** is the first number or numbers of the dialed string that you want to review. In this example, the number is 1650. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen for dialed strings that begin with the numbers 1650 (Figure 439: ARS Digit Analysis Table screen on page 1721).

Figure 439: ARS Digit Analysis Table screen

```
change ars analysis 1650                                        Page 1 of X

                            ARS DIGIT ANALYSIS TABLE
                                  Location:  all             Percent Full:  6

      Dialed          Total    Route    Call    Node    ANI
      String        Min Max  Pattern    Type    Num     Reqd
1                   11  11     30       fnpa    ___     n
1650                11  11     30       fnpa    ___     n
167                 11  11     30       fnpa    ___     n
1800                11  11     30       fnpa    ___     n
2                   7   7      2        hnpa    ___     n
3                   7   7      2        hnpa    ___     n
4                   7   7      2        hnpa    ___     n
5                   7   7      2        hnpa    ___     n
7                   7   7      2        hnpa    ___     n
8                   7   7      2        hnpa    ___     n
911                 3   3      1        emer    ___     n
976                 11  11     deny     hnpa    ___     n
```

2. Click **Next** if necessary until you see a blank field.

   If the dialed string is already defined in your system, the cursor appears in the appropriate Dialed String column where you can make changes.

3. In the Dialed String column, type **1650**.

4. In the Total Min and the Total Max columns, type the minimum and maximum values from Step 2.

   For this example, the minimum and maximum values are **11**.

5. In the Route Pattern column, type the route pattern from Step 2.

   For this example, the route pattern is **30**.

6. In the Call Type column, type the call type from Step 2.

   For this example, the route pattern is **fnpa**.

7. In the Node Num column, type the node number from Step 2

   For this example, the node number is left blank.

8. Press **Enter** to save your changes.

Adding a new prefix

To add a new prefix, follow the same procedure as you use to add a new area code. The one exception is to use a shorter dial string (such as ***2223333***, where ***222*** is the old prefix,) and a dial type of **hnpa**.

If you do not need to use the number 1 for area code calls, omit the **1** in Step 1, Step 4, and Step 6 in the previous procedure. Also, type **10** instead of **11** in the **Total Min** and the **Total Max** fields in Step 7.

To see if the new area code or prefix number is set up as a toll call, type **display toll *n***, where ***n*** is the prefix that you want to review. Some users might not be allowed to dial toll call numbers.

Using ARS to restrict outgoing calls

With ARS, you can block outgoing calls to specific dialed strings. For example, you can restrict users from making international calls to countries where you do not do business. In the US, you can restrict access to 900 and 976 pay-per-call numbers.

In this example, Colombia is used as the country to restrict. The country code for Colombia is 57.

To prevent callers from placing calls to countries that you want to restrict:

1. Type **change ars analysis *011n***, where ***011*** is the international access code and ***n*** is the country code of the restricted country. In this example, type **change ars analysis 01157**. Press **Enter**.

   The system displays the ARS Digit Analysis Table screen (Figure 440: ARS Digit Analysis Table screen on page 1723).

Figure 440: ARS Digit Analysis Table screen

```
change ars analysis 01157                                      Page 1 of X

                            ARS DIGIT ANALYSIS TABLE
                                  Location:  all            Percent Full:  6

      Dialed          Total    Route    Call    Node   ANI
      String        Min Max  Pattern   Type    Num    Reqd
1                   11  11    30       fnpa    ___    n
1650                11  11    30       fnpa    ___    n
167                 11  11    30       fnpa    ___    n
1800                11  11    30       fnpa    ___    n
2                   7   7     2        hnpa    ___    n
3                   7   7     2        hnpa    ___    n
4                   7   7     2        hnpa    ___    n
5                   7   7     2        hnpa    ___    n
7                   7   7     2        hnpa    ___    n
8                   7   7     2        hnpa    ___    n
911                 3   3     1        emer    ___    n
976                 11  11    deny     hnpa    ___    n
01157               10  23    deny     intl    ___    n
```

2. Click **Next** if necessary until you see a blank field.

   If the dialed string is already defined in your system, the cursor appears in the appropriate Dialed String column. Skip to Step 5 to deny calls to this dialed string.

3. In the Dialed String column, type **011xx**, where **xx** is the country code of the restricted country.

   In this example, type **01157**.

4. In the Total Min and the Total Max columns, type the minimum number of digits, and the maximum number of digits, that you want the system to analyze.

   In this example, type **10** in the Total Min column, and **23** in the Total Min column. The system uses this digit analysis entry if the dialed number:

   — Begins with **01157**

   — Contains at lease 10 digits

   — Contains no more than 23 digits

5. In the Route Pattern column, type an appropriate route pattern.

   In this example, type **deny** to prevent users to complete calls to this dialed string.

6. In the Call Type column , type the category of calls that this dialed string represents.

   In this example, type **intl** to indicate this dialed string represents an international call.

7. Press **Enter** to save your changes.

Defining ARS partitions

You can use ARS partitioning to provide different call routing for a group of users, or for specific telephones.

If you used partitioning on a prior release of Communication Manager and you want to continue to use partitioning, read this section carefully. In Communication Manager Release 2.0, partition groups are defined on the Partition Route Table. Partition groups are no longer defined on the Digit Analysis Table.

Prerequisites

You must complete the following actions before you can define ARS partitions:

- On the Optional Features screen:
  - Ensure that the **Tenant Partitioning** field is set to **y**. If this field is not set to **y**, contact your Avaya representative before you continue with this procedure.
  - Ensure that the **Time of Day Routing** field is set to **n**. If this field is not set to **n**, contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

Setting up partition groups

In this example, your company allows your employees to make local, long distance, and emergency calls. However, you have a telephone in the lobby for visitors. You want to allow visitors to make only local, toll-free, and emergency calls from this telephone.

To restrict the telephone in the lobby, modify the routing for a partition group to enable only specific calls, such as US-based toll-free 1-800 calls. Then assign this partition group to the telephone. In this example, the partition group for the telephone in the lobby is partition group 2.

To enable toll-free 1-800 calls for partition group 2:

1. Type **`list ars route-chosen`** ***`1800n`***, where ***`n`*** is any 7-digit telephone number to create an example of the dialed string. Press **Enter**.

   In this example, type **18002221000**.

   The system displays the ARS Route Chosen Report screen for partition group 1 (Figure 441: ARS Route Chosen Report screen on page 1725).

Figure 441: ARS Route Chosen Report screen

```
list ars route-chosen 18002221000                              Page 1 of X

                          ARS ROUTE CHOSEN REPORT

     Location: 1                        Partitioned Group Number:  1

      Dialed               Total       Route    Call      Node      Location
      String              Min  Max     Pattern  Type      Number
1800                      11   11      p1       fnpa      _____     all
```

2. Note the route pattern for the selected dialed string. In this example, the route pattern for 1800 is **p1**. **p1** indicates that the system uses the Partition Routing Table to determine what route pattern to use for each partition.

   If a number appears in the Route Pattern column without the letter **p**, all partitions use the same route pattern. You need to use the Partition Routing Table only if you want to use different route patterns for different partition groups.

3. After you review this information, press **Cancel**.

4. Type **change partition-route-table index *n***, where ***n*** is the route index number. In this example, type **change partition-route-table index 1**. Press **Enter**.

   The system displays the Partition Routing Table screens (Figure 442: Partition Routing Table screen on page 1726). In this example, partition group 1 (the PGN 1 column) can make 1-800 calls, and these calls use route pattern 30.

Figure 442: Partition Routing Table screen

```
change partition-route-table index 1                          Page 1 of X

                              Partition Routing Table

                                 Routing Patterns
 Route
 Index          PGN 1   PGN 2   PGN 3   PGN 4   PGN 5   PGN 6   PGN 7   PGN 8
 -----          -----   -----   -----   -----   -----   -----   -----   -----
   1              30      30     ____    ____    ____    ____    ____    ____
   2             ____    ____    ____    ____    ____    ____    ____    ____
   3             ____    ____    ____    ____    ____    ____    ____    ____
   4             ____    ____    ____    ____    ____    ____    ____    ____
   5             ____    ____    ____    ____    ____    ____    ____    ____
   6             ____    ____    ____    ____    ____    ____    ____    ____
   7             ____    ____    ____    ____    ____    ____    ____    ____
   8             ____    ____    ____    ____    ____    ____    ____    ____
   9             ____    ____    ____    ____    ____    ____    ____    ____
  10             ____    ____    ____    ____    ____    ____    ____    ____
  11             ____    ____    ____    ____    ____    ____    ____    ____
  12             ____    ____    ____    ____    ____    ____    ____    ____
  13             ____    ____    ____    ____    ____    ____    ____    ____
  14             ____    ____    ____    ____    ____    ____    ____    ____
  15             ____    ____    ____    ____    ____    ____    ____    ____
```

5. In the PGN 2 column that corresponds to Route Index 1, type the same number as in the PGN 1 column. In this example, type **30**.

   This entry tells the system to use route pattern 30 for partition group 2, and allow partition group 2 members to make calls to 1-800 numbers.

6. Press **Enter** to save your changes.

Assigning a telephone to a partition group

Assigning a telephone extension to a partition group is a two-step process. First, assign the partition group to a COR. Then assign that COR to the extension.

To assign a Class of Restriction (COR) to partition group 2:

1. Type **`list cor`**. Press **Enter**.

   The system displays the Class of Restriction Information screen (Figure 443: Class of Restriction Information screen on page 1727).

Figure 443: Class of Restriction Information screen

```
list cor                                                    Page 1 of 7
                        CLASS OF RESTRICTION INFORMATION

                    COR   COR Description

                     0
                     1
                     2
                     3
                     4
                     5
                     6
                     7
                     8
                     9
                    10     Supervisor observer
                    11
                    12
                    13
                    14
```

2. Choose a COR that has not been used.

   In this example, use COR number **3**.

3. After you review this information, press **Cancel**.

4. Type **change cor *x***, where ***x*** is the COR number that you just chose. In this example, type **change cor 3**. Press **Enter**.

   The system displays the Class of Restriction screen (Figure 444: Class of Restriction screen on page 1728).

Figure 444: Class of Restriction screen

```
change cor 3                                                  Page 1 of 4
                              CLASS OF RESTRICTION

               COR Number: 3
          COR Description: lobby

                      FRL: 0                                       APLT? y
  Can Be Service Observed? n                 Calling Party Restriction: none
Can Be A Service Observer? y                  Called Party Restriction: none
 Partitioned Group Number: 2              Forced Entry of Account Codes? n
         Priority Queuing? n                        Direct Agent Calling? y
     Restriction Override: none                Facility Access Trunk Test? n
     Restricted Call List? n                          Can Change Coverage? n

            Access to MCT? y                   Fully Restricted Service? n
Group II Category For MFC: 7                   Hear VDN of Origin Annc.? n
         Send ANI for MFE? n                    Add/Remove Agent Skills? y
            MF ANI Prefix: ______              Automatic Charge Display? n
Hear System Music on Hold? y      PASTE (Display PBX Data on telephone)? n
                              Can Be Picked Up By Directed Call Pickup? n
                                         Can Use Directed Call Pickup? n
                                         Group Controlled Restriction: inactive
```

5. In the **COR Description** field, type a name for this COR.

   In this example, the COR name is **lobby**, named for the telephone in the lobby.
6. In the **Partitioned Group Number** field, type the number of the partition group.

   In this example, the partition group number is **2**.
7. Press **Enter** to save your changes.

To assign the COR to a telephone extension:

1. Type **change station *n***, where ***n*** is the extension. Press **Enter.**

   The system displays the Station screen (Figure 427: Station screen on page 1698).
2. In the **COR** field, type the number of the COR.

   In this example, the COR number is **3**.
3. Press **Enter** to save your changes.

Setting up Time of Day Routing

You can use Time of Day Routing to redirect calls to coverage paths according to the time of the day and the day of the week.You must define the coverage paths that you want to use before you define the time of day coverage plan. You can route calls based on the least expensive route according to the time of day and the day of the week that the call is made. You can also deny outgoing long distance calls after business hours to help prevent toll fraud.

Time of Day Routing applies to all AAR or ARS outgoing calls and trunks that the system uses for call forwarding to external numbers.

Prerequisites

You must complete the following actions before you can set up Time of Day Routing:

AAR or ARS must be administered on the system before you can use Time of Day Routing.

- On the Optional Features screen:
  - For AAR, ensure that either the **Private Networking** field or the **Uniform Dialing Plan** field is set to **y**. If neither field is set to **y**, contact your Avaya representative before you continue with this procedure.
  - For ARS, ensure that the **ARS** field is set to **y**, and the **Time of Day Routing** field is set to **y**. If both these fields are not set to **y**, your system is not enabled for the Time of Day Routing feature. Contact your Avaya representative before you continue with this procedure.

  To view the Optional Features screen, type **`display system-parameters customer-options`**. Press **Enter**.

To display your Time of Day Routing plan:

1. Type **`display time-of-day n`**, where ***n*** is the number of the routing plan. In this example, type **`display time-of-day 1`** to look at your Time of Day Routing plan 1. Press **Enter**.

   The system displays the Time of Day Routing Plan 1 screen (Figure 445: Time of Day Routing Plan 1 screen on page 1730).

Figure 445: Time of Day Routing Plan 1 screen

```
display time-of-day 1                                          Page 1 of 1

                            TIME OF DAY ROUTING PLAN 1

     Act    PGN Act      PGN    Act      PGN    Act      PGN    Act      PGN Act
     Time    #  Time      #     Time      #     Time      #     Time      #  Time
 Sun 00:01   1 __:__      _     __:__     _     __:__     _     __:__     _ __:__ __
 Mon 00:01   1 08:__00    2     12:__00   1     13:__00   2     17:__00   1 __:__ __
 Tue 00:01   1 08:__00    2     12:__00   1     13:__00   2     17:__00   1 __:__ __
 Wed 00:01   1 08:__00    2     12:__00   1     13:__00   2     17:__00   1 __:__ __
 Thu 00:01   1 08:__00    2     12:__00   1     13:__00   2     17:__00   1 __:__ __
 Fri 00:01   1 08:__00    2     12:__00   1     13:__00   2     17:__00   1 __:__ __
 Sat 00:01   1 __:__      _     __:__     _     __:__     _     __:__     _ __:__ __
```

Note the routing plan that is currently in effect. In this example, this plan is for employees who can make only local calls.

In this example, two partition group numbers (PGN) control Time-of-Day routing:

- PGN 1 begins 1 minute after midnight (00:01) every work day of the week until 8:00 a.m.
- PGN 2 begins at 8:00 a.m. every work day of the week until 12:00 p.m.
- PGN 1 begins at 12:00 p.m. every work day of the week until 1:00 p.m. (13:00).
- PGN 2 begins at 1:00 p.m. (13:00) every work day of the week until 5:00 p.m. (17:00).
- PGN 2 begins at 5:00 p.m. (17:00) every work day of the week until 12:00 a.m.
- PGN 1 is also used all day Saturday and Sunday.

2. After you review this information, press **Cancel**.

To create a new Time-of-Day routing plan for long-distance calls for executives in your company:

1. Type **change time-of-day *n***, where ***n*** is the number of the routing plan. In this example, type **change time-of-day 2** to create a Time of Day Routing plan 2. Press **Enter**.

   The system displays the Time of Day Routing Plan 2 screen (Figure 446: Time of Day Routing Plan screen on page 1731).

Figure 446: Time of Day Routing Plan screen

```
change time-of-day 2
                              TIME OF DAY ROUTING PLAN ___          Page 1 of 1

     Act     PGN   Act     PGN   Act     PGN   Act     PGN   Act     PGN   Act     PGN
     Time     #    Time     #    Time     #    Time     #    Time     #    Time     #
Sun  00:00    1    __:__    _    __:__    _    __:__    _    __:__    _    __:__    _
Mon  00:00    1    __:__    _    __:__    _    __:__    _    __:__    _    __:__    _
Tue  00:00    1    __:__    _    __:__    _    __:__    _    __:__    _    __:__    _
Wed  00:00    1    __:__    _    __:__    _    __:__    _    __:__    _    __:__    _
Thu  00:00    1    __:__    _    __:__    _    __:__    _    __:__    _    __:__    _
Fri  00:00    1    __:__    _    __:__    _    __:__    _    __:__    _    __:__    _
Sat  00:00    1    __:__    _    __:__    _    __:__    _    __:__    _    __:__    _
```

2. In the first PGN # column, type **1** in each field as shown on the Time of Day Routing Plan 1 screen.

   In this example, PGN 1 is the partition group that the system uses for after hours and the lunch hour.

3. In the remaining PGN # columns, type **3** in all fields.

   In our example, PGN 3 is the partition group that the system uses to route long distance calls during business hours.

4. Press **Enter** to save your changes.

Now assign your new Time of Day Routing Plan 2 to the COR that is assigned to your executives.

In this example, the following conditions are true:

- Jim is the user at extension 1234.
- Extension 1234 is assigned a COR of 2.
- COR 2 is assigned a Time of Day Plan Number of 1.
- The Time-of-Day Routing Plan 1 is administered as shown in Figure 445: Time of Day Routing Plan 1 screen on page 1730.

When Jim comes into work on Monday morning at 8:30 and dials the ARS access code followed by the number of the person he is calling, the system checks the Time of Day Plan number assigned to the COR for Jim.

Because Jim has been assigned COR 2 with Time of Day Plan Number 1, the system uses Time of Day Routing Plan 1 to route the call.

According to the Time of Day Routing Plan 1, the system routes calls that are made between 8:00 a.m. and 11:59 a.m. according to the route pattern that is set up in the PGN 1 column.

If Jim makes a call between 12:00 p.m. and 1:00 p.m. on Monday, the Time of Day Routing Plan 1 is used again. However, this time the call is routed according to PGN 2.

Reports for World Class Routing

The following reports provide information about the World Class Routing feature:

- None

Considerations for World Class Routing

This section provides information about how the World Class Routing feature behaves in certain circumstances. Use this information to ensure that you receive the maximum benefits of the World Class Routing feature under all conditions:

- None

Interactions for World Class Routing

This section provides information about how the World Class Routing feature interact with other features on the system. Use this information to ensure that you receive the maximum benefits World Class Routing in any feature configuration:

- Bridged Call Appearance

  If a Bridged Call Appearance is used for an Automatic Alternate Routing (AAR) or an Automatic Route Selection (ARS) call, the system uses the partition group number (PGN) of the bridged extension instead of the PGN of the caller.

- Call Forwarding

  The system uses the PGN of the COR of the forwarding party to select the table to look up the route pattern.

- Distributed Communications System (DCS)

  When the system routes a call over DCS, the far-end switch uses the PGN of the incoming trunk to route the call.

- Remote Access

  When a remote-access user dials a barrier code or an authorization code plus an ARS Feature Access Code (FAC), the COR of the barrier code or authorization code determines the PGN.

- Straightforward Outward Completion and Through Dialing

  If the attendant assists or extends a call and dials an ARS FAC, the COR of the attendant determines the PGN if the individual extension is assigned. If the individual extension is unassigned, the COR that is set on the console parameter determines the PGN.

- ARS/AAR Dialing Without FAC interactions

  The following features require entries in the **ARS/AAR Internal Call Prefix** and **Total Length** fields on the Dial Plan Parameters screen, if you intend to dial a "shortcut" ARS/AAR number after the applicable FAC or button push:

  - Add/remove skill
  - Attendant activation of call forwarding
  - Call forwarding activation
  - CDR reports
  - Changeable COR through FAC
  - Coverage Message Retrieval
  - EC500 feature activation
  - Extended call forwarding
  - Leave Word Calling activation/cancellation
  - Station Security Code
  - TTI
  - User/Group Controlled Restriction
  - Whisper Paging

Index

Symbols

. . . . . 804, 1035
* 804, 1035, 1361, 1363

Numerical

2420 DCP telephone 311, 1359, 1399
4620 IP telephone 311, 1359, 1399
58689
  H2
    Overview 938

A

AAA Services 71
  administering 87
  description 71
AAR, *see* Automatic Alternate Routing (AAR)
Abbreviated Dialing (AD) 99
  administering 101
    adding lists 102
    assigning telephones for group lists 103
    prerequisites 101
  commands
    add abbreviated-dialing group 102
    change station 103
    display system-parameters customer-options . 102
  considerations 105
  description 100
    enhanced lists 101
    group lists 100
    personal lists 100
    system lists 101
  end-user procedures 104
  interactions 106
  screens 102
    Abbreviated Dialing List 103
    Optional Features 102
    Station 104
  troubleshooting 107
ACA, *see* Automatic Circuit Assurance (ACA)
ACB, *see* Automatic Callback (ACB)
Access Security Gateway (ASG) 111
  administering 111
    disabling 114
    modifying for lost key 115
    monitoring History Log 116
    prerequisites 112
    restarting 115
    setting up 113
  commands
    change login 113, 114, 115
    change system-parameters customer-options . 112
    change system-parameters security 114
    list asg-history 116
    remove login 115
  description 111
  interactions 117
  screens 112
    Access Security Gateway Session History . . 116
    Login Administration 113
    Optional Features 112
    Security-Related System Parameters 114
AD, *see* Abbreviated Dialing (AD)
Administered Connections 119
  administering 122
    setting up 123
  commands
    change administered-connection 122
    display status-administered connection . . . 121
    set time 126
  description 119
  interactions 125
  screens 123
    Access Endpoint 123
    Administered Connection 123
    Attendant Console 123
    Class of Restriction 123
    Class of Service 123
    Data Modules 123
    Dial Plan Record 123
    DS1 Circuit Pack 123
    Station 123
    Trunk Group 123
Administrable Alternate Gatekeeper List for IP Endpoints 127
Administrable Language Displays 139
  administering 143
    entering translations for user-defined language 146
    prerequisites 144
    setting display language 145
  commands
    change attendant 145, 146
    change display-messages 146
  description 139

Making Standard telephone Features easier to use 148
screens . . . 144
Attendant Console . . . 145
System Parameters Country-Options . . . 144
troubleshooting . . . 147
Administration Change Notification . . . 151
administering . . . 151
initiating . . . 152
commands
notify history . . . 152
description . . . 151
screens . . . 152
Administration Changes . . . 152
Administration Without Hardware (AWOH) . . . 153
administering . . . 154
assigning for hunt-group queue . . . 155
assigning to attendant console . . . 157
assigning to data module . . . 158
assigning to telephone . . . 157
commands
change attendant . . . 157
change data-module . . . 158
change hunt-group . . . 155
change station . . . 157
description . . . 153
association and disassociation . . . 154
disassociated telephones . . . 154
duplicate telephones . . . 153
Personal Station Access (PSA) . . . 154
phantom extensions . . . 154
physical characteristics of telephone . . . 153
Terminal Translation Initialization (TTI) . . . 154
user activated features . . . 154
interactions . . . 160
screens . . . 155
Attendant Console . . . 158
Data Module . . . 159
Hunt Group . . . 156
Station . . . 157
AFRL, *see* Facility Restriction Levels, Alternate Facility Restriction Levels (AFRL)
Alphanumeric Dialing . . . 169
administering . . . 169
considerations . . . 170
description . . . 169
screens . . . 170
ANI, *see* Automatic Number Identification (ANI)
Announcements . . . 171
administering . . . 180
adding announcement extensions . . . 183
adding TN2501AP VAL circuit pack . . . 186
converting announcement files to VAL format . 196
converting for Interactive Voice Response (IVR) 197
deleting and erasing announcements . . . 192
deleting announcement extensions . . . 193
deleting VAL announcements . . . 198
displaying all announcements . . . 188
erasing announcement source . . . 193
file format requirements . . . 195
Interactive Voice Response (IVR) . . . 197
Locally Sourced Announcements and Music . 180
managing VAL announcements using FTP . . 199
prerequisites . . . 194
recording announcements . . . 191
recording announcements for TTY callers . . 205
recording VAL announcements . . . 194
setting up a media gateway . . . 189
setting up continuous-play announcements . 194
using SAT to delete all VAL announcements . 198
using SAT to delete individual VAL announcements 198
commands
busyout board board-location . . . 198
change announcements . 183, 193, 194, 202, 203
delete filename.wav . . . 202
disable filesystem board board-location . . . 204
enable filesystem board . . . 200
erase announcements . . . 193
erase announcements board board-location . 199
ftp val-ip-address . . . 201
get filename.wav . . . 204
list directory board . . . 198, 199
list integrated-annc-boards . . . 189, 199
put filename.wav . . . 203, 204
remove file board board-location . . . 198
description . . . 172
announcement sources in G700, G350, and G250 Media Gateways . . . 178
barge-in . . . 177
compression rates . . . 178
delay announcements . . . 172
devices and types . . . 174
forced announcements . . . 172
information announcements . . . 172
local announcements on media gateways . . 174
sessions . . . 178
VAL Manager . . . 173
virtual Voice Announcements over LAN (virtual VAL) 174
Voice Announcements over LAN (VAL) . . . 173
interactions . . . 208
reports . . . 205
viewing Event Report . . . 206
viewing Voice Announcement Measures . . . 207
screens . . . 181
Announcements/Audio Sources . . . 184
Event Report . . . 206
Events Report . . . 207
Integrated Announcements/Audio . . . 189
Media Gateway . . . 190
Voice Announcement Measurements . . . 208

troubleshooting . . . 209
capacities and load balancing . . . 210
non-volatile storage on VAL . . . 211
Answer Detection, *see* Call Detail Recording (CDR)
ARS, *see* Automatic Route Selection (ARS)
ASG, *see* Access Security Gateway (ASG)
Attendant Auto Start and Don't Split . . . 213
administering . . . 214
assigning Don't Split button . . . 215
prerequisites . . . 214
commands
change attendant . . . 215
considerations . . . 216
description . . . 213
interactions . . . 216
screens . . . 214
Attendant Console . . . 215
Attendant Auto-Manual Splitting . . . 217
administering . . . 217
description . . . 217
screens . . . 218
Attendant Console . . . 218
Attendant Backup . . . 219
administering . . . 220
assigning console permissions to backup telephones 224
configuring your system . . . 222
defining Class of Service console permissions . . . 223
prerequisites . . . 221
setting up telephones . . . 222
commands
change console-parameters . . . 222
change cos . . . 223
change station . . . 224
considerations . . . 226
description . . . 219
end-user procedures . . . 226
interactions . . . 227
screens . . . 221
Class of Service . . . 221, 224
Console Parameters . . . 222, 223
Feature Access Code (FAC) . . . 221
Station . . . 225
Attendant Call Waiting . . . 229
administering . . . 230
modifying timed intervals . . . 233
prerequisites . . . 230
setting up single-line telephones . . . 231, 232
commands
change console-parameters . . . 233
change station . . . 231
change system-parameters features . . . 232
considerations . . . 234
description . . . 229
interactions . . . 234
screens . . . 230
Feature-Related System Parameters . . . 232
Station . . . 231
Attendant Calling of Inward Restricted Stations . . . 237
administering . . . 237
prerequisites . . . 238
setting up Class of Restriction override . . . 238
description . . . 237
screens . . . 238
Class of Restriction . . . 238
Attendant Conference . . . 239
administering . . . 239
prerequisites . . . 239
setting up . . . 240
commands
change system-parameters features . . . 240
considerations . . . 242
description . . . 239
interactions . . . 242
screens . . . 240
Feature-Related System-Parameters . . . 241
Attendant Control of Trunk Group Access . . . 245
administering . . . 246
assigning access buttons . . . 247
prerequisites . . . 246
setting trunk group threshold . . . 247
commands
change attendant . . . 247
change trunk-group . . . 247
description . . . 245
interactions . . . 248
screens . . . 247
Attendant Console . . . 248
Trunk Group . . . 247
Attendant Direct Extension Selection (DXS) . . . 251
administering . . . 253
prerequisites . . . 253
considerations . . . 253
description . . . 251
Enhanced DXS Tracking . . . 252
Group Display button . . . 252
Standard DXS Tracking . . . 252
interactions . . . 254
screens . . . 253
Attendant Console . . . 253
Attendant Direct Trunk Group Selection . . . 255
administering . . . 256
prerequisites . . . 256
considerations . . . 256
description . . . 255
interactions . . . 257
screens . . . 256
Attendant Console . . . 256
Attendant Intrusion . . . 259
administering . . . 259
assigning an intrusion button . . . 260

prerequisites . . . 259
commands
change attendant . . . 260
description . . . 259
interactions . . . 261
screens . . . 260
Attendant Console . . . 260
Attendant Lockout - Privacy . . . 263
administering . . . 263
activating or deactivating . . . 264
prerequisites . . . 263
commands
change console-parameters . . . 264
description . . . 263
interactions . . . 265
screens . . . 264
Console Parameters . . . 264
Attendant Override of Diversion Features . . . 267
administering . . . 267
prerequisites . . . 267
description . . . 267
screens . . . 268
Attendant Console . . . 268
Attendant Priority Queue . . . 269
administering . . . 271
assigning Call Type button . . . 274
prerequisites . . . 271
setting category priorities . . . 272
setting number of calls in queue . . . 273
commands
change console-parameters . . . 272
change display-messages miscellaneous-features . 275
change system-parameters features . . . 273
considerations . . . 276
description . . . 269
interactions . . . 276
priority by call category . . . 269
priority by call type . . . 271
screens . . . 272
Console Parameters . . . 273
Feature-Related System Parameters . . . 274
Language Translations . . . 275
Attendant Recall . . . 277
administering . . . 277
description . . . 277
end-user procedures . . . 278
interactions . . . 279
screens . . . 278
Attendant Console . . . 278
Attendant Serial Calling . . . 281
administering . . . 281
prerequisites . . . 281
description . . . 281
screens . . . 282
Attendant Console . . . 282
Attendant Split Swap . . . 283
administering . . . 283
assigning split-swap button . . . 284
prerequisites . . . 283
commands
change attendant . . . 284
description . . . 283
screens . . . 284
Attendant Console . . . 284
Attendant Timers . . . 285
administering . . . 286
prerequisites . . . 286
setting up . . . 287
commands
change console-parameters . . . 287
description . . . 285
Return Call to (same) Attendant . . . 289
Attendant Overflow Timer . . . 290
interactions . . . 288
screens . . . 287
Console Parameters . . . 287
Attendant Trunk Identification . . . 291
administering . . . 291
prerequisites . . . 291
description . . . 291
screens . . . 292
Attendant Console . . . 292
Station . . . 292
Attendant Vectoring . . . 293
administering . . . 293
assigning VDN extension to console . . . 296
assigning VDN extension to tenant . . . 297
creating VDN extension . . . 295
prerequisites . . . 294
commands
change console-parameters . . . 296
change tenant . . . 297
change vdn . . . 295
change vector . . . 294
display system-parameters customer-options 294
considerations . . . 298
description . . . 293
interactions . . . 299
screens . . . 295
Call Vector . . . 294
Console Parameters . . . 297
Optional Features . . . 294
Tenant . . . 298
Vector Directory Number . . . 296
Audible Message Waiting . . . 301
administering . . . 301
for user . . . 302
prerequisites . . . 302
commands
change station . . . 302

display system-parameters customer-options . 302
considerations 303
description 301
screens 302
Optional Features 302
Station 303
AUDIX One-Step Recording 305, 1393
administering 307
assigning feature button to telephone 312
assigning parameters 308
changing characteristics of zip tone 313
prerequisites 307
translating button label to user-defined language 311, 1399
translating feature display to user-defined language 310, 1398
commands
change display-messages button-labels . 311, 1399
change display-messages view-buttons . 310, 1398
change station 312, 1400
change system-parameters country-options 315, 1402
change system-parameters features . . 308, 1396
change tone-generation 314, 1401
display system-parameters customer-options 308, 872, 1395
considerations 317
description 305
feature button 306
language options 306
periodic alerting tone 306
ready indication tone 306
recording delay timer 307
end-user procedures 316
recording conversation 316
hunt group extension number 306, 1393
initiator 307, 309, 316, 1394, 1397, 1404
interactions 318
screens 308
Feature-Related System Parameters . . 309, 1397
Language Translations . . . 311, 312, 1398, 1399
Optional Features 308, 872, 1395
Station 313, 1400
System Parameters Country-Options . . 315, 1403
Tone Generation Customized Tones . . 314, 1402
troubleshooting 321
zip tone 306, 313, 1394, 1401
Authorization Codes 323
administering 325
creating with specific COR 329
prerequisites 325
setting up 326
commands
change authorization-code 328, 329
change system-parameters features 326
display system-parameters customer-options . 325
considerations 330
description 323
AAR and ARS calls 324
length of codes 323
using codes 324
interactions 330
Listed Directory Numbers (LDN) 330
Remote Access Numbers (RAN) 330
screens 326
Authorization Code - COR Mapping . . . 328, 329
Feature-Related System Parameters 327
Optional Features 325
Automated Attendant 333
administering 333
announcements 336
assigning caller information button on attendant consoles 338
assigning caller information button on multiappearance telephones 337
controlling hunt groups by vector 336
prerequisites 334
setting the prompting timeout 335
vector directory number (VDN) 336
commands
change attendant 338
change hunt-group 336
change station 337
change system-parameters features 335
display system-parameters customer-options 334
considerations 339
description 333
interactions 339
screens 334
Announcements/Audio Sources 334
Attendant Console 339
Feature-Related System Parameters 335
Hunt Group 337
Optional Features 334
Station 338
Vector Directory Number 334
Automatic Alternate Routing (AAR) 1633, 1689
Automatic Callback (ACB) 341
administering 347
assigning Feature Access Code (FAC) . . . 348
assigning feature button 351
enabling Automatic Callback with Called Party Queuing 349
setting no-answer timeout interval 350
setting queue length for Ringback Queuing . 351
commands
add station 351
add trunk-group 351
change feature-access-codes 348
change station 351
change system-parameters features 350
change trunk-group 351
considerations 353

description . . . 341
Analog Busy Automatic Callback Without Flash 343
CCBS for Incoming Calls . . . 345
CCBS Call Flow Scenarios . . . 346
CCBS Routing issue . . . 346
Ringback Queuing . . . 342
interactions . . . 355
screens . . . 348
ars digit-conversion . . . 347
Feature Access Code (FAC) . . . 349
Feature-Related System Parameters . . . 350
Station . . . 351
Supplementary Service Protocol . . . 352
Trunk Group . . . 351, 353
Automatic Circuit Assurance (ACA) . . . 359
administering . . . 360
description . . . 359
audit trail . . . 360
referral calls . . . 359
interactions . . . 361
reports . . . 361
screens . . . 360
Attendant Console . . . 361
Feature-Related System Parameters . . . 360
Station . . . 361
Trunk Features . . . 360
Automatic Exclusion, *see* Privacy
Automatic Number Identification (ANI) . . . 365
administering . . . 366
display incoming ANI calling party information . 368
set up ANI on multifrequency trunk . . . 367
set up ANI request button . . . 371
set up outgoing ANI . . . 369
commands
change aar analysis . . . 369
change aar digit-conversion . . . 371
change ars analysis . . . 370
change ars digit-conversion . . . 371
change multifrequency-signaling . . . 367
change system-parameters features . . . 369
change trunk group . . . 368
description . . . 365
Incoming Automatic Number Identification . . . 365
Outgoing Automatic Number Identification . . . 366
interactions . . . 373
screens . . . 367
AAR Digit Analysis Table . . . 370
AAR Digit Conversion Table . . . 370
ARS Digit Analysis Table . . . 370
ARS Digit Conversion Table . . . 370
Feature-Related System Parameters . . . 369
Multifrequency-Signaling-Related Parameters 367, 368
Station . . . 372
Trunk Group . . . 368
Automatic Route Selection (ARS) . . . 1634, 1689
Avaya support Web site . . . 68
Avaya Video Telephony Solution . . . 375
description . . . 375
AWOH, *see* Administration Without Hardware (AWOH)

B

Bridged Call Appearance . . . 379
administering . . . 381
assigning ringing to each appearance . . . 385
creating on multiappearance telephone . . . 384
creating on single-line telephone . . . 382
prerequisites . . . 381
commands
change coverage path . . . 381
change station . . . 382, 384
display system-parameters features . . . 381
considerations . . . 387
description . . . 379
multiappearance telephone . . . 379
sample uses . . . 380
single-line telephone . . . 379
interactions . . . 388
screens . . . 382
Coverage Path . . . 381
Feature-Related System Parameters . . . 381
Station . . . 383, 384-386
Bulletin Board . . . 399
administering . . . 399
changing bulletin board information . . . 401
setting user permissions . . . 400
commands
change bulletin-board . . . 401
change permissions . . . 400
considerations . . . 404
description . . . 399
capacity . . . 399
high priority messages . . . 399
screens
Bulletin Board . . . 402
Command Permission Categories . . . 401
Busy Indicator . . . 405
description . . . 405
Busy Tone Disconnect . . . 405
interactions . . . 406
Busy Verification . . . 407
administering . . . 409
prerequisites . . . 409
using Busy Verification . . . 410
commands
change station . . . 410
considerations . . . 411
description . . . 407
interactions . . . 411
screens . . . 410

Station 410

C

Call Charge Information 413
administering 415
administering PPM for non-ISDN trunks 427
AOC for ISDN trunks 425
assigning call charge display button for attendant 424
assigning call charge display button for user . . 423
assigning COR 418
charge display 421
Country protocol codes 431
defining CDR 416
frequency of call charge displays 416
PPM for DS1 circuit packs 429
prerequisites 415
translating call charge text 417
commands
add trunk-group 425
change attendant 424
change cor 418
change display-messages miscellaneous-features . 417
change station 423
change system-parameters cdr 416
change system-parameters features 416
change trunk-group 421, 427
considerations 433
description 413
Advice of Charge (AOC) 413
charge displays 414
Periodic Pulse Metering (PPM) 413
end-user procedures 432
interactions 433
screens 419
Attendant Console 425
CDR System Parameters 416
Class of Restriction 419
DS1 Circuit Pack 430
Feature-Related System Parameters 417
ISDN Trunk Group 425, 427
Language Translations 418
Station 423, 424
Trunk Group 421
viewing 414
Call Coverage 437
administering 450
assigning coverage paths 457, 460
assigning internal alerting 466
assigning telephone numbers for off-network coverage 461
assigning time-of-day coverage 464
coverage path for redirected off-network calls . 462
creating coverage answer groups 466
creating coverage paths 454
defining calls redirected off-network 461
defining coverage redirected off-network calls 461
enabling enhanced Redirection Notification . 467
prerequisites 451, 454, 457, 461, 464
commands
add coverage answer-group 466
add coverage path 454
add coverage time-of-day 464
change coverage path 462
change coverage remote 461
change feature-access-codes 451
change station 457, 460, 465
change trunk-group 466
display coverage sender group 455
display system-parameters call coverage/call forwarding 454
display system-parameters customer-options 461
considerations 468
Coverage Subsequent Redirection interval . . . 437
description 437
announcement in coverage path 445
answer groups 445
caller response interval 446
changeable coverage paths 442
conditions that override 449
Consult 447
coverage criteria 442
coverage path 438
Enhanced Redirection Notification 444
enhancements to LNCC 448
Extended User Administration of Redirected Calls 442
features that override 448
hunt group in coverage path 446
interaction for enhanced redirection notification 474
ISDN calls redirected off-net 441
limit number of concurrent calls 447
multiple coverage paths 438
notifying users upon redirection 446
off-network coverage 441
redirection 442
subsequent redirection interval 446
Time-of-Day Coverage 439
VDN in Coverage Path (VICP) 445
Directed Call Pickup 450
interactions 468
remote code numbers 462
reports 468
screens 452
Coverage Answer Group 466
Coverage Path 455, 463
Feature Access Code (FAC) 452
Optional Features 461
Station 458, 465
System-Parameters Call Coverage/Call Forwarding 454

Time of Day Coverage Table 464
Trunk Group 466
Switch Communication Interface (SCI) link 445
troubleshooting 475
Call Detail Recording (CDR) 477
administering 563
assigning FEAC 565
for all calls 565
to COR 566
to users 567
assigning privacy digits for user 568
for data module 582
for paging ports 594
for trunk group. 580
identifying Inter-Exchange Carrier 592
intra-switch CDR 595
port field values 589
prerequisites 563, 565, 568
system parameters 570
commands
change cor 566
change data-module 582
change feature-access-codes 563
change intra-switch-cdr 595
change ixc-codes 592
change loudspeaker paging 594
change station. 567, 569
change system-parameters cdr . . . 565, 568, 570
change trunk-group 567, 580
display system-parameters customer-options 564, 565
considerations 600
data record formats
59 character. 498, 523
enhanced expanded 510, 534
enhanced LSU 506, 531
enhanced printer 502, 527
enhanced TELESEER 497, 522
enhanced unformatted 513, 538
expanded 507, 532
int process 515, 540
int-direct 516, 541
int-ISDN 518, 542
ISDN LSU. 506, 530
ISDN printer. 500, 525
ISDN-TELESEER 496, 521
LSU 505, 530
LSU, LSU-expand, unformatted, and customized 494
LSU-expand. 503, 528
printer 499, 524
printer and expanded 494
TELESEER 495
TELESEER 59 character, int-proc, int-direct, and int-ISDN 495
unformatted 512, 537
description 477
Account Code Dialing 484
Answer Detection 483
Answer Supervision by Timeout 484
attendant call transfer on public network trunk 491
attendant transfer of incoming trunk call . . . 490
call classification 483
call splitting 485
CDR output 492
CDR Privacy 492
CDR record formats 493
customized call record formats 495
date record formats. 493
field descriptions 545
Forced Entry of Account Codes (FEAC) . . . 484
incoming trunk call splitting (ITCS) 485
intraswitch CDR 491
ITCS conference call on same server 487
ITCS transfer on same server 487
ITCS transfer to outgoing trunk 488
ITCS, OTCS, and attendant call recording . . 489
monitor call detail records. 478
Network Answer Supervision 483
OTCS call transfer 489
OTCS conference call 489
outgoing trunk call splitting (OTCS) 488
standard call record formats 495, 520
end-user procedures 599
examples 486, 488, 490
attendant call transfer on public network trunk 490
attendant incoming trunk call transfer 490
ITCS and call transfer on same server 487
ITCS and call transfer to public network . . . 487
ITCS and conference call 486
OTCS and call transfer to public network . . 489
OTCS and conference call on public network. 488
interactions 601
screens
CDR System Parameters . . . 565, 568, 570, 578
Class of Restriction. 566
Data Module 583
Feature Access Code (FAC) 564
Inter-Exchange Carrier Codes. 593
Intra-Switch CDR. 595
Loudspeaker Paging 594
Optional Features 564, 565
Station 567, 569
Trunk Group 567, 580
Call Forwarding 615
administering 619
assigning All Calls 622
assigning Busy/Don't Answer 623
assigning Off-Net. 624
disabling Override 628
enabling Override 627
prerequisites 619, 623, 624

removing Busy/Don't Answer . . . 624
removing Off-Net . . . 626
viewing active users . . . 621
Call Log Enhancements . . . 630
Log Forwarded Calls . . . 630
commands
change station . . . 622-624, 626
change system-parameters coverage-forwarding 620, 623-625, 627, 628
display station . . . 621
display system-parameters customer-options . . . 625
list call-forwarding . . . 621
save translation . . . 632
considerations . . . 632
Coverage of Calls Redirected Off-Net (CCRON) . . . 617
description . . . 615
attendants . . . 616
Busy/Don't Answer . . . 616
Call Forwarding All Calls . . . 615
Call Forwarding Off-Net . . . 617
Call Forwarding Override . . . 617
coverage for unanswered forwarded calls . . . 618
Feature Access Code (FAC) . . . 616
security . . . 618
user notification . . . 618
end-user procedures . . . 628
interactions . . . 633
off-network timer . . . 617
screens . . . 621
Optional Features . . . 624
Station . . . 622
System Parameters Call Coverage/Call Forwarding 620, 623, 626-627
V1, V2, or V3 system . . . 621
Call Offer, *see* Attendant Intrusion
Call Park . . . 637
administering . . . 637
assigning call park button to multiple-call appearance telephone . . . 643
prerequisites . . . 638
commands
change console-parameters . . . 641
change feature-access-codes . . . 638
change station . . . 643
change system-parameters features . . . 639
considerations . . . 646
description . . . 637
end-user procedures . . . 644
interactions . . . 646
screens . . . 642
Console-Parameters . . . 642
Feature Access Code (FAC) . . . 639
Feature-Related System Parameters . . . 640, 641
Station . . . 644
Call Pickup . . . 649
administering . . . 653
adding pickup groups . . . 655
assigning Call Pickup button . . . 657
assigning Call Pickup Feature Access Code . . . 658
assigning COR to users . . . 674
assigning Directed Call Pickup button . . . 675
assigning Directed Call Pickup FAC . . . 675
assigning pickup groups to flexible extended pickup group . . . 669
assigning pickup groups to simple extended pickup group . . . 665
changing Call Pickup button . . . 661
changing extended pickup groups . . . 670
creating COR for Directed Call Pickup . . . 672
creating extended pickup group FAC . . . 663
creating flexible extended pickup groups . . . 667
creating simple extended pickup groups . . . 663
deleting pickup groups . . . 660, 661
enabling Call Pickup Alerting . . . 656, 657
getting list of extended pickup groups . . . 660
pickup numbers . . . 666
prerequisites . . . 671
removing Directed Call Pickup . . . 676
removing pickup group from extended pickup group 660
removing user from pickup group . . . 659
setting up . . . 655
setting up Directed Call Pickup . . . 671
setting up flexible extended pickup groups . . . 666
setting up simple extended pickup groups . . . 662
commands
add pickup-group . . . 655
change cor . . . 673
change extended-pickup-group . . . 661, 665, 669
change feature-access-codes . . . 658, 664, 675
change pickup-group . . . 659, 667
change station . . . 657, 661, 662, 674, 676
change system-parameters features 656, 657, 663, 667, 671
list extended-pickup-group . . . 660
remove pickup-group . . . 661
considerations . . . 678
description . . . 649
call alerting . . . 649
call appearance selection . . . 651
call distribution algorithms . . . 651
Directed Call Pickup . . . 652
Enhanced Call Pickup Alerting . . . 652
Extended Call Pickup . . . 651
end-user procedures . . . 677
interactions . . . 678
screens . . . 654
Class of Restriction . . . 673
Extended Pickup Groups . . . 660
Feature Access Code (FAC) . . . 659, 664, 676
Feature-Related System Parameters 656, 663, 672
Station . . . 658, 674

Call Waiting Termination 681
administering 682
assigning call waiting termination 684
prerequisites 682
commands
change station 684
change system-parameters features 682
considerations 685
description 681
Call Waiting tones 681
interactions 686
screens 683
Feature-Related System Parameters 683
Station 684
Call Waiting, *see* Call Waiting Termination
Call-by-Call Service Selection 687
administering 691
administering network facilities 695
prerequisites 691
setting up a trunk group for CBC 692
Call Detail Recording 690
commands
add trunk-group 692
change isdn network-facilities 696
change route-pattern 694
change trunk-group 692
display system-parameters customer-options . 691
description 687
incoming call-handling treatment 690
interactions 697
ISDN messages and information elements for usage allocation 688
screens 692
CBC Trunk Group Usage Allocation 692
CBC Trunk Group Usage Allocation Plan Assignment Schedule 693
Incoming Call Handling Treatment 694
ISDN Trunk Group 692
Network Facilities 696
Optional Features 691
Route Pattern 695
Usage Allocation Plans 689
Caller ID 699
administering 700
displaying Caller ID information 701
prerequisites 700
commands
add trunk group 701
change trunk group 701
display system-parameters customer-options . 701
considerations 702
description 699
on analog trunks 700
on digital trunks 700
interactions 702
screens 701
Trunk Group 701
Trunk Group Administrable Timers 701
Trunk Group Trunk Features 701
CAS, *see* Centralized Attendant Service (CAS)
CDR System Parameters screen 985
CDR, *see* Call Detail Recording (CDR)
Centralized Attendant Service (CAS) 705
administering 707
prerequisites 707
commands
display system-parameters customer-options 707
considerations 708
description 705
interactions 710
listed directory number (LDN) 705
release link trunks (RLT) 705
screens 708
Optional Features 707
changing configuration sets 948
Class of Restriction (COR) 715
administering 721
allowing users to change 726
displaying administered CORs 722
prerequisites 726
setting up 722
commands
change cor 722
change feature-access-codes 726
change system-parameters features 727
display system-parameters customer-options 726
list cor 722
description 715
called party restrictions 719
calling party restrictions 718
COR-to-COR restrictions 720
fully restricted service 720
strategy for assigning 717
end-user procedures 728
Facility Restriction Level (FRL) 717
interactions 729
screens 721
Class of Restriction 718, 723-725
Class of Restriction Information 722
Feature Access Code (FAC) 727
Feature-Related System Parameters 728
Optional Features 726
Trunk Group 718
Class of Service (COS) 733
administering 733
assigning a COS 738
defining COS for your system 734
descriptions of the COS features 735
commands
change cos 734
considerations 739

description . . . 733
interactions . . . 739
screens . . . 734
Class of Service . . . 735
Code Calling Access, *see* Loudspeaker Paging, chime paging
commands, *see* commands *under individual feature names*
Conference . . . 741
administering . . . 744
assigning feature buttons . . . 748
assigning feature buttons to attendant . . . 751
assigning feature buttons to user . . . 750
assigning toggle-mute feature button . . . 748
prerequisites . . . 744, 748
commands
change attendant . . . 751
change station . . . 748, 750
change system-parameters features . . . 744
display system-parameters customer-options . . . 749
considerations . . . 753
description . . . 741
No Dial Tone Conferencing . . . 742
No Hold Conference . . . 743
Selective Conference Party Display, Drop, and Mute 743
Transfer Toggle/Swap . . . 742
end-user procedures . . . 752
displaying participants on call . . . 752
interactions . . . 753
number of participants on a call . . . 741
screens . . . 747
Attendant Console . . . 751
Class of Restriction . . . 749
Feature-Related System Parameters . . . 745, 746
Optional Features . . . 749
Station . . . 748, 750
Configuration Set screen . . . 986
configuration sets . . . 948
considerations, *see* considerations *under individual feature names; see also* interactions *under individual feature names*
considerations, *see* considerations *under individual feature names; see also* interactions *under individual feature names*
console-parameters screen (with extension) . . . 290
COR, *see* Class of Restriction (COR)
Co-residency with SIP . . . 761
description . . . 761
Co-Resident DEFINITY LAN Gateway (DLG) . . . 755
administering . . . 756
prerequisites . . . 756
commands
add data-module . . . 757
add ip-interface . . . 756, 757
change node-names ip . . . 756
display ip-interfaces . . . 756, 757
display node-names ip . . . 756
display system-parameters customer-options 756, 757
list data-modules . . . 757
description . . . 755
screens . . . 757
COS, *see* Class of Service (COS)
Crisis Alert, *see* Enhanced 911 (E911)

D

Data Call Setup . . . 763
administering . . . 766
assigning data extension feature button . . . 781
defining data module . . . 768
prerequisites . . . 767
specifying port location . . . 780
commands
add data-module . . . 768
change feature-access-codes . . . 767
change modem-pool . . . 780
change station . . . 781
considerations . . . 785
description . . . 763
call progress messages . . . 765
cause code . . . 764
reason code . . . 764
special characters . . . 763
end-user procedures . . . 782
interactions . . . 785
screens . . . 768
Data Module . . . 769, 770
Feature Access Code (FAC) . . . 767
Modem Pool Group . . . 781
Station . . . 782
Data Privacy, *see* Privacy
Data Restriction, *see* Privacy
DCS. *See* Distributed Communications System (DCS)
Default Dialing . . . 787
administering . . . 787
description . . . 787
screens . . . 788
Demand Print . . . 789
administering . . . 789
description . . . 789
screens . . . 789
Dial Access to Attendant . . . 791
administering . . . 791
changing attendant access code . . . 792
commands
change dialplan analysis . . . 792
description . . . 791
interactions . . . 794
screens . . . 792
Dial Plan Analysis Table . . . 793

Dial Plan . . . 795
administering . . . 806
adding extension ranges . . . 812
displaying your dial plan . . . 806, 807
commands
change dialplan analysis . . . 807, 813
display system-parameters customer-options . 813
considerations . . . 813
description . . . 795
Dial Plan Analysis Table . . . 803
Dial Plan Parameters . . . 805
Multi-Location Dial Plan . . . 805
other options . . . 806
interactions . . . 814
screens . . . 807
Dial Plan Analysis Table . . . 803, 808
Dial Plan Parameters . . . 805
Feature Related System Parameters . . . 814
Optional Features . . . 813
Trunk Group . . . 804
Dial Plan Transparency (DPT) . . . 821
administering . . . 821
considerations . . . 826
description . . . 821
interactions . . . 827
maintenance . . . 825
screens . . . 822
Distinctive Ringing . . . 837
administering . . . 837
defining . . . 838
commands
change system-parameters features . . . 838
considerations . . . 841
description . . . 837
Personalized Ringing . . . 837
interactions . . . 841
screens . . . 838
Feature-Related System Parameters . . 839, 840
Distributed Communications System (DCS) . . . 1002
DLG, *see* Co-Resident DEFINITY LAN Gateway (DLG)
Dual Homing, *see* Multiple Level Precedence and Preemption (MLPP)
DXS, *see* Attendant Direct Extension Selection (DXS)

E

E911, *see* Enhanced 911
Edit Dialing
description . . . 108
Edit Dialing on 96xx H.323 Terminals
field description . . . 109
feature interactions . . . 108
Edit Dialing System Parameters screen . . . 109
Emergency Calls from Unnamed IP Endpoints . . . 867
administering . . . 871
prerequisites . . . 872
description . . . 867
interactions . . . 876
reports . . . 874
screens . . . 874
Enbloc Dialing and Call Type Digit Analysis . . . 891
administering . . . 893
prerequisites . . . 893
description . . . 891
interactions . . . 894
End Office Access Line Hunting, *see* Multiple Level Precedence and Preemption (MLPP)
endpoints, *see* telephones
end-user procedures, *see* end-user procedures *under individual feature names*
end-user procedures, *see* end-user procedures *under individual feature names*
Enhanced 911 (E911) . . . 843
administering . . . 850
prerequisites . . . 851, 853, 855, 857
setting up CAMA numbering . . . 861
setting up Crisis Alert to attendant or display telephone 852
setting up Crisis Alert to notify digital pager . 857
setting up emergency extension forwarding . 859
Automatic Location Information (ALI) database . 844
Automatic Number Identification (ANI) . . . 864
Avaya IP Softphone . . . 844
Caller Emergency Service Identification (CESID) number 844
Calling Party Number (CPN) . . . 843
Centralized Automatic Message Accounting (CAMA) trunks . . . 843
commands
change ars analysis location . . . 845
change attendant . . . 854
change cama-numbering . . . 861
change station . . . 853, 855
change system-parameters crisis-alert . . 856, 858
change system-parameters features . . . 860
display system-parameters customer-options 853
list emergency . . . 850
considerations . . . 863
Crisis Alert . . . 849
description . . . 843
Location Specific Routing . . . 845
media gateways in different locations . . . 845
Emergency Location Information Number (ELIN) 847
Integrated Services Digital Network (ISDN) trunks 843
interactions . . . 864
public safety answering point (PSAP) . . . 843
reports . . . 863
screens . . . 851
ARS Digit Analysis Table . . . 853
Attendant Console . . . 855, 856
CAMA Numbering - E911 Format . . . 862

Class of Restriction . . . 851
Crisis Alert System Parameters . . . 857, 858
Feature Access Code (FAC) . . . 851
Feature-Related System Parameters . . . 860
Optional Features . . . 853
Route Pattern . . . 851
Station . . . 844, 855
Universal Emergency Number (UEN) . . . 843
wired IP telephones . . . 847
Enhanced Call Forwarding . . . 897
administering
enabling chained call forwarding . . . 901
enabling FACs for enhanced call forwarding . . . 900
enhanced call forwarding . . . 899
specifying coverage path . . . 902
viewing enhanced call forwarding . . . 899
description . . . 897
chained call forwarding . . . 898
feature button . . . 898
end-user procedures . . . 902
interactions . . . 908
screens
General Status . . . 899
Enterprise Mobility User . . . 877
administering
Enterprise Mobility User . . . 882
options for calling party identification . . . 888
setting EMU options for stations . . . 887
description . . . 877
EMU call processing . . . 881
EMU station lock feature . . . 881
EMU supported telephone buttons . . . 880
EMU use and activation . . . 879
feature name . . . 877
system requirements EMU . . . 879
end-user procedures . . . 889
Feature Name
administering
name of the first procedure . . . 883
prerequisites . . . 882
screens . . . 883
screens
Class of Service . . . 884
Feature Access Code . . . 885
Feature-Related System Parameters for EMU . . . 878
Station . . . 887
System Parameters Feature for Emergency Extension Forwarding timer . . . 886
System Parameters Feature screen for EMU . . . 886
Trunk Group . . . 888
ETA, *see* Uniform Dial Plan (UDP), Extended Trunk Access (ETA)
Expanded Meet-me Conferencing . . . 913
administering . . . 916
prerequisites . . . 916
description . . . 913
end-user procedures . . . 921
interactions . . . 922
screens . . . 917
Extended User Administration of Redirected Calls . . . 923
administering
assigning a Station Security Code to a user . . . 931
prerequisites . . . 926
commands
add telecommuting-access . . . 926
change feature-access-codes . . . 927
change station . . . 931
display system-parameters customer-options . . . 926
description . . . 923
COR . . . 925
COS . . . 924
DCS . . . 924
disabling the telecommuting access extension . . . 924
off-site locations . . . 925
end-user procedures . . . 932
interactions . . . 934
screens . . . 931
Class of Restriction . . . 930
Class of Service . . . 929
Feature Access Code (FAC) . . . 928
Station . . . 932
Telecommuting Access . . . 926
Extension to Cellular . . . 937
administering . . . 960
barge-in tone . . . 988
call detail recording (CDR) . . . 983
call filtering . . . 980
caller identification . . . 979
configuration sets . . . 986
creating a self administration feature (SAFE) access code . . . 970
enable/disable FACs . . . 972
enable/disable feature button . . . 974
extend a call feature button . . . 977
Feature Access Codes (FACs) . . . 966
feature button assignments . . . 977
Feature Name Extensions (FNEs) . . . 968
prerequisites . . . 961
Station Security Code FAC . . . 972
telecommuting access number . . . 967
voice mail . . . 981
commands
add off-pbx-telephone station-mapping 964, 970, 980
add trunk-group . . . 984
change coverage path . . . 982
change display-messages button-labels . . . 978
change display-messages view-buttons . . . 977
change feature-access-codes . . . 966, 971, 972, 973
change intra-switch-cdr . . . 986
change off-pbx-telephone configuration-set 981, 985, 986, 988

change off-pbx-telephone feature-name-extensions 968
change public-unknown-numbering 979
change station 975, 977, 996, 997, 998, 999, 1000
change system-parameters cdr 985
change system-parameters security 973
change telecommuting-access 967
display system-parameters customer-options . 962
list ars route-chosen 1015
list bridged-extensions 999
list mappings-acquired 992
status station 1014
considerations 995
description 937
ARS/AAR routing 942
Call Detail Recording 944
Call Filtering 946
capacity 947
Conditional Call Extending 940
Shared Voice Connections 940
Sharing Mappings 941
support of one-X Mobile Server 941
enable and disable 1002
end-user procedures 995
interactions 1001
screens 963
configuration set 982, 985, 986, 988
coverage path 983
Feature Access Code (FAC) 967
Feature Access Code (FAC) page 2 971
Feature Access Code (FAC) page 3 973
language translations buttons 978
language translations labels 979
numbering-public/unknown format 980
security-related system parameters 974
station 976
stations with off-pbx telephone integration . . . 965
stations with off-pbx telephone integration page 2 965
telecommuting access 968
trunk group 984
troubleshooting 1004

F

FAC, *see* Feature Access Codes (FAC)
Facility and Non-Facility Associated Signaling . . . 1017
administering 1019
implementing FAS and NFAS 1021
reviewing guidelines for coordinating FAS and NFAS 1020
description 1017
D-Channel backup activation 1019
D-Channel backup with NFAS 1017
screens 1020
DS1 Circuit Pack 1022
Interface Links 1020
ISDN-PRI Trunk Group 1024
Processor Channel 1020
Signaling Group 1023
Facility Restriction Levels 1025
administering 1028
considerations 1030
description 1025
AAR and ARS calls 1025
Alternate Facility Restriction Levels (AFRL) . 1027
alt-frl feature button 1027
authorization codes 1027
end-user procedures 1029
interactions 1030
screens 1028
toll fraud prevention 1027
Traveling Class Marks (TCM) 1025
Facility Test Calls 1031
administering 1032
considerations 1033
description 1031
interactions 1033
screens 1033
Fax, Modem, Clear Channel over IP 64
FEAC, *see* Call Detail Recording (CDR), Forced Entry of Account Codes (FEAC)
Feature Access Codes (FAC) 1035
administering 1036
assigning 1037
changing or deleting 1038
prerequisites 1036
analog rotary dial telephones 1035
commands
change feature-access-codes 1037, 1038
description 1035
* and # 1035
access codes 1035
activate and deactivate codes 1035
lock and unlock codes 1035
send and cancel codes 1035
screens 1036
Feature Access Code (FAC) 1037, 1038
troubleshooting 1039
feature interactions
Extension to Cellular enable and disable 1002
Extension to Cellular with office caller ID calling another Extension to Cellular user 1003
Feature Name 375, 761, 877
administering
mapping phones 964
name of the second procedure 882, 888
FRL, *see* Facility Restriction Levels

G

generating two CDR records . . . 985
Group Paging . . . 1041
  administering . . . 1042
    changing paging group . . . 1044
    creating paging group . . . 1042
    viewing all paging groups . . . 1044
  commands
    add group-page . . . 1042
    change group-page . . . 1044
    list group-page . . . 1044
  description . . . 1041
  interactions . . . 1045
  screens . . . 1042
    Group Paging Using Speakerphone . . . 1043
    Speakerphone Page Groups . . . 1044
  troubleshooting . . . 1047

H

H.248 Gateways . . . 64
H0 channels, *see* Wideband Switching, H0 channels
H11 channels, *see* Wideband Switching, H11 channels
H12 channels, *see* Wideband Switching, H12 channels
Hold . . . 1049
  administering . . . 1050
    assigning FAC for CAS remote hold and answer 1052
    enabling Automatic Hold . . . 1051
    prerequisites . . . 1050
  commands
    change feature-access-codes . . . 1052
    change system-parameters features . . . 1051
  considerations . . . 1054
  description . . . 1049
    Automatic Hold . . . 1050
    Hard Hold . . . 1049
    multiappearance telephones . . . 1049
    single-line telephones . . . 1049
    Soft Hold . . . 1049
  interactions . . . 1054
  screens . . . 1051
    Feature Access Code (FAC) . . . 1053
    Feature-Related System Parameters . . . 1052
Hot Line Service . . . 1057
  administering . . . 1058
  considerations . . . 1059
  description . . . 1057
  interactions . . . 1059
  screens . . . 1058
Hunt Groups . . . 1061
  administering . . . 1068
    adding announcements . . . 1070
    changing . . . 1069
    setting up groups . . . 1069
    setting up night service . . . 1071
    setting up queues . . . 1070
  commands
    add hunt-group . . . 1069
    change hunt-group . . . 1069-1071
    display announcements . . . 1070
  considerations . . . 1071
  description . . . 1061
    announcements . . . 1062
    call coverage . . . 1063
    call distribution methods . . . 1064
    Call Forwarding All Calls . . . 1066
    delay announcement intervals . . . 1062
    extension unavailability . . . 1065
    Hunt Group Busy option . . . 1066
    queues . . . 1067
    Send All Calls . . . 1066
    TTY . . . 1067
  forced first announcement . . . 1071
  interactions . . . 1073
  screens . . . 1068

I

IAA, *see* Internal Automatic Answer (IAA)
IAS, *see* Inter-PBX Attendant Service (IAS)
ICLID, *see* Caller ID
IGAR (Inter-Gateway Alternate Routing) . . . 64
Incoming Call Line Identification (ICLID), *see* Caller ID
Individual Attendant Access . . . 1075
  administering . . . 1075
    assigning extension to attendant console . . . 1076
    prerequisites . . . 1075
  commands
    add attendant . . . 1076
  description . . . 1075
  screens . . . 1076
    Attendant Console . . . 1076
interactions, *see* interactions *under individual feature names; see also* considerations *under individual feature names*
interactions, *see* interactions *under individual feature names; see also* considerations *under individual feature names*
Intercom . . . 1077
  administering . . . 1078
  description . . . 1077
    groups . . . 1077
    telephones . . . 1078
  interactions . . . 1078
Internal Automatic Answer (IAA) . . . 1079
  administering . . . 1080
  considerations . . . 1081
  description . . . 1079
  interactions . . . 1081

screens . . . 1080
Inter-PBX Attendant Service (IAS) . . . 1085
administering . . . 1085
enabling Inter-PBX Attendant Service . . . 1086
prerequisites . . . 1085
commands
change console-parameters . . . 1086
display system-parameters customer-options 1086
description . . . 1085
interactions . . . 1088
screens . . . 1086
Console Parameters . . . 1086
Optional Features . . . 1086
ISDN Service . . . 1089
administering . . . 1100
description . . . 1089
ISDN interworking . . . 1096
national ISDN-2 services . . . 1095
private network services . . . 1093
transmission rate and protocols . . . 1090
interactions . . . 1101
screens . . . 1100
ITCS, *see* Call Detail Recording (CDR), incoming trunk call splitting (ITCS)
IVR, *see* Announcements, Interactive Voice Response (IVR)
IXC, *see* World Class Routing, interexchange carrier (IXC)

L

Last Number Dialed . . . 1103
administering . . . 1103
considerations . . . 1104
description . . . 1103
interactions . . . 1104
screens . . . 1103
Attendant Console . . . 1103
Feature Access Code (FAC) . . . 1103
Station . . . 1103
LDN, *see* Listed Directory Number (LDN)
Leave Word Calling (LWC) . . . 1105
considerations . . . 1107
description . . . 1105
voice synthesis . . . 1106
end-user procedures . . . 1106
interactions . . . 1107
Line Load Control (LLC), *see* Multiple Level Precedence and Preemption (MLPP)
Line Lockout . . . 1109
administering . . . 1109
considerations . . . 1110
description . . . 1109
screens . . . 1110
linear trunk hunt, *see* Wideband Switching, linear trunk hunt
Listed Directory Number (LDN) . . . 1113
administering . . . 1114
assigning incoming destination to trunk . . . 1116
assigning listed directory numbers . . . 1115
commands
change listed-directory-number . . . 1115
change trunk-group . . . 1116
considerations . . . 1117
description . . . 1113
routing incoming DID trunk calls to attendant groups 1113
routing incoming FX and CO trunk calls to attendant groups . . . 1113
interactions . . . 1117
screens . . . 1114
Listed Directory Numbers . . . 1115
Trunk Group . . . 1116
Locally Sourced Announcements and Music . . . 1119
administering . . . 1120
considerations . . . 1130
description . . . 1119
interactions . . . 1131
reports . . . 1130
screens . . . 1121
Loss Plans . . . 1133
administering . . . 1134
guidelines using loss groups . . . 1134
prerequisites . . . 1134
commands
display location-parameters . . . 1134
display system-parameters customer-options 1134
description . . . 1133
screens . . . 1135
Location Parameters . . . 1134
Optional Features . . . 1134
Loudspeaker Paging . . . 1137
administering . . . 1139
prerequisites . . . 1140
setting up chime paging over loudspeakers . . . 1142
setting up voice paging over loudspeakers . . . 1141
commands
change paging code-calling-ids . . . 1144
change paging loudspeaker . . . 1141, 1142
change system-parameters features . . . 1140
description . . . 1137
chime paging . . . 1138
deluxe paging . . . 1137
restrictions . . . 1139
interactions . . . 1145
screens . . . 1140
Code Calling IDs . . . 1144
Feature-Related System Parameters . . . 1140
Loudspeaker Paging . . . 1141, 1143
troubleshooting . . . 1146

M

Magic-on-Hold system, *see* Tenant Partitioning
Malicious Call Trace (MCT) . . . 1147
administering
assigning feature buttons for attendant . . . 1153
assigning feature buttons for user . . . 1153
defining on system . . . 1150
prerequisites . . . 1149
commands
add ds1 . . . 1154
change attendant . . . 1153
change bri-trunk-board . . . 1156
change mct-group-extensions . . . 1152
change station . . . 1153
change system-parameters features . . . 1150
display system-parameters customer-options 1149
considerations . . . 1159
description . . . 1147
activating . . . 1147
controlling . . . 1147
deactivating . . . 1148
using voice recorder . . . 1148
end-user procedures . . . 1157
interactions . . . 1160
reports . . . 1159
screens . . . 1150
Attendant Console . . . 1153
DS1 Circuit Pack . . . 1155
Feature-Related System Parameters . . . 1151, 1152
ISDN-BRI Trunk Circuit Pack . . . 1156
Optional Features . . . 1149
Station . . . 1154
Manual Exclusion, *see* Privacy
Manual Message Waiting . . . 1163
administering . . . 1163
assigning feature button . . . 1164
commands
change station . . . 1164
description . . . 1163
screens . . . 1164
Station . . . 1164
Manual Originating Line Service, *see* Hot Line Service
Manual Signaling . . . 1167
administering . . . 1167
assigning manual signaling button for multiple-call appearance telephone . . . 1168
commands
change station . . . 1168
description . . . 1167
end-user procedures . . . 1169
interactions . . . 1169
screens . . . 1168
Station . . . 1168
Meet-me Conference . . . 1171
administering . . . 1171
accessing as attendee . . . 1179
changing access code . . . 1180
creating or changing vector . . . 1173
creating vector directory number (VDN) . . . 1177
options for creating vector steps . . . 1175
prerequisites . . . 1172
using Selective Conference Party Display, Drop, and Mute . . . 1180
commands
add vdn . . . 1177
change vector . . . 1173
display system-parameters customer-options 916, 1172
list meet-me vdn . . . 1178
considerations . . . 1181
description . . . 1171
end-user procedures . . . 1179
interactions . . . 1184
screens . . . 1172
Call Vector . . . 1173, 1174
Meet-me Vector Directory Number . . . 1179
Optional Features . . . 916, 1172
Vector Directory Number . . . 1177, 1178
troubleshooting . . . 1185
MLPP, *see* Multiple Level Precedence and Preemption (MLPP)
Modem Pooling . . . 1187
administering . . . 1188
considerations . . . 1189
description . . . 1187
interactions . . . 1189
screens . . . 1188
Data Module . . . 1188
Feature Access Code (FAC) . . . 1188
Modem Pool Group . . . 1188
Multifrequency Signaling . . . 1191
considerations . . . 1194
description . . . 1191
guidelines . . . 1192
MF Shuttle . . . 1192
MFE . . . 1192
R2 multifrequency compelled (MFC) signaling 1192
interactions . . . 1195
screens . . . 1194
Multi-Location Dial Plan . . . 1259
administering . . . 1263
changing extensions . . . 1265
prepending numbers . . . 1267
prerequisites . . . 1264
setting up announcements . . . 1268
setting up local centralized answering point (LCAP) 1269
setting up multiple FACs – ARS . . . 1270
setting up multiple FACs for attendants . . . 1270
commands

change daylight-savings-rules 1264
display system-parameters customer-options 1264
description 1260
announcements 1262
Feature Access Codes (FACs) 1261
location prefix 1260
maintenance 1263
distributed communication system (DCS). . . . 1259
interactions. 1270
local centralized answering point (LCAP) 1269
screens 1264
Change Station Extension 1265
Daylight Savings Rules 1264
Optional Features 1264
Uniform Dial Plan Table 1268
Multiple Level Precedence and Preemption (MLPP) 1199
administering. 1216
adding extensions 1228
announcements for Precedence Calling. . . 1228
assigning announcement types. 1229
assigning attendant queue priorities. . 1227, 1244
assigning digit analysis 1234
assigning digit conversion 1238
assigning Feature Access Codes 1233
assigning hot line number 1224, 1243
assigning LLC level to COR 1241
assigning LLC level to system 1241
assigning maximum precedence levels . . . 1222
assigning MLPP Feature Access Code . . . 1220
assigning Precedence Calling system parameters . 1221
assigning Preemption to COR 1240
assigning route patterns 1237
assigning trunks. 1223, 1241
assigning WNDP Feature Access Codes . . 1243
assigning WNDP system parameters 1242
deleting announcements 1230
Dual Homing 1239
enabling Precedence Call Waiting 1231
End Office Access Line Hunting 1240
Line Load Control (LLC) 1241
Precedence Call Waiting. 1231
Precedence Calling 1220
Precedence Routing. 1234
Preemption 1240
prerequisites 1218
recording announcements 1229
saving announcements 1230
setting Precedence Call timeout . . . 1232, 1241
Worldwide Numbering and Dialing Plan (WNDP)1242
Attendant Diversion Timing 1202, 1203
Call Purpose Indicators 1203
commands
add abbreviated-dialing group 1224, 1244
add station 1225, 1244
add trunk-group 1223
change announcements 1228, 1230
change console-parameters 1227
change cor. 1222, 1240, 1241
change feature-access-codes . . 1220, 1233, 1243
change precedence-routing analysis. 1234
change precedence-routing digit-conversion . 1238
change route-pattern 1237
change station 1231
change system-parameters mlpp1221, 1229, 1232, 1241, 1242
display system-parameters customer-options 1218
considerations 1245
Default Route Digit 1215
Defense Switched Network (DSN) 1199
description 1199
announcements for Precedence Calling . . . 1209
Dual Homing. 1210
End Office Access Line Hunting. 1211
Line Load Control (LLC) 1212
Precedence Call Waiting 1210
Precedence Calling. 1200
Precedence Routing 1210
Preemption 1211
Worldwide Numbering and Dialing Plan (WNDP)1213
Generic Switching Center Requirements (GSCR) 1199
interactions 1247
Joint Interoperability Test Command (JITC) . . . 1199
Line Load Control (LLC) 1241
lockdown 1212
Precedence Call Timeout 1203
Precedence calling tones 1202
Remote Attendant Route String 1202
Route Control Digit 1246
screens. 1218
Abbreviated Dialing List. 1224, 1244
Announcements/Audio Sources 1228
Class of Restriction. 1222, 1240, 1241
Console Parameters 1227
Feature Access Code (FAC) . . 1220, 1233, 1243
Multiple Level Precedence & Preemption Parameters 1221, 1229, 1232, 1241, 1242
Optional Features 1218
Pattern Number 1237
Precedence Routing Digit Analysis Table . . 1234
Precedence Routing Digit Conversion Table . 1238
Station 1225, 1231, 1244
Trunk Features. 1223
WNDP Emergency 911 Route String 1256
Multiple Music-on-Hold, *see* Tenant Partitioning
Music-on-Hold 1273
administering 1274
assigning music source port 1278
assigning music tones, music ports, and music for transferred trunks. 1275
connecting music source to server 1278
defining COR 1277

American Society of Composers, Artists, and Producers (ASCAP) . . . 1273
Broadcast Music Incorporated (BMI) . . . 1273
commands
add trunk-group . . . 1278
change cor . . . 1277
change music-sources . . . 1278
change system-parameters features . . . 1275
considerations . . . 1279
description . . . 1273
copyrighted material . . . 1273
options for music, silence, and tone . . . 1273
interactions . . . 1280
screens . . . 1274
Class of Restriction . . . 1277
Feature-Related System Parameters . 1127, 1275
Music Sources . . . 1278

N

N x DS0 channels, *see* Wideband Switching, N x DS0 channels
Night Service . . . 1281
administering . . . 1283
setting up external alerting . . . 1291
setting up external alerting Night Service . . 1291
setting up night console service . . . 1287
setting up Night Service for hunt groups . . . 1294
setting up Night Service for trunk groups . . 1293
setting up night station service . . . 1288
setting up night station service to voice mail . 1284
setting up trunk answer from any station . . 1290
commands
add hunt group . . . 1284
change attendant . . . 1287
change console-parameters 1286, 1289, 1291, 1292, 1293
change feature-access-codes . . . 1290
change hunt-group . . . 1294
change listed-directory-numbers 1285, 1288, 1291
change tenant . . . 1285
change trunk-group . . . 1293
considerations . . . 1295
description . . . 1281
Hunt Group Night Service . . . 1281
Night Console Service . . . 1281
Night Station Service . . . 1282
Trunk Answer from Any Station (TAAS) . . . 1282
Trunk Group Night Service . . . 1283
interactions . . . 1297
screens . . . 1284
Attendant Console . . . 1288
Console Parameters 1286, 1289, 1291, 1292, 1293
Feature Access Code (FAC) . . . 1290
Hunt Group . . . 1285, 1294
Listed Directory Numbers . . . 1286, 1289, 1292
Trunk Group . . . 1293
nightly file transfers, *see* Wideband Switching, scheduled batch processing

O

Off-Premises Station . . . 1301
administering . . . 1302
activating for a user . . . 1302
commands
change station . . . 1302
description . . . 1301
interactions . . . 1304
screens . . . 1302
Station . . . 1303
OTCS, *see* Call Detail Recording (CDR), outgoing trunk call splitting (OTCS)
OTTOTT, *see* Transfer, outgoing trunk to outgoing trunk transfer (OTTOTT)
Overriding of SAC/CF . . . 1305
administering . . . 1305
enabling by Dialing or Priority calling . . . 1306
enabling for station with or without display . . 1307
enabling protection . . . 1307
description . . . 1305
using SAC/CF Override . . . 1307

P

paging, *see* Group Paging
PE, *see* Wideband Switching, PRI endpoints (PE)
Personal Station Access (PSA) . . . 1317
administering . . . 1320
prerequisites . . . 1320
commands
change feature-access-codes . . . 1321
description . . . 1317
button mapping . . . 1318
dissociated telephones . . . 1319
invalid attempts using . . . 1317
preferences and permissions . . . 1318
security . . . 1320
telecommuting . . . 1317
unanswered calls . . . 1318
end-user procedures . . . 1323
Hot Desking interaction with PSA . . . 1327
interactions . . . 1326
screens . . . 1322
Feature Access Code (FAC) . . . 1321
System Parameters Features . . . 1328
Personalized Ringing . . . 1329
administering . . . 1330
assigning to user telephone . . . 1330
commands
change station . . . 1330

description . . . 1329
power failures . . . 1329
ringing patterns . . . 1329
interactions . . . 1332
screens . . . 1330
Station . . . 1331
PIN Checking for Private Calls . . . 1333
description . . . 1333
Call Detail Recording . . . 1339
screens
Authorization Code . . . 1335
Feature Access Code . . . 1337
PIN Checking for Private Calls . . . 1338
System Parameters Features . . . 1336
Port Network Recovery from Control Network Outages 1341
description . . . 1341
configuration impacts on availability . . . 1343
improved Port Network Recovery from Control Network Outages . . . 1341
Post Connect Dialing Options field . . . 987
Posted Messages . . . 1345
* . . . 1361, 1363
administering . . . 1348
activating the Posted Messages security code 1352
creating custom messages . . . 1355
defining Feature Access Code (FAC) . . . 1350
prerequisites . . . 1348
sending custom messages through QSIG . . . 1353
setting up a telephone security code . . . 1352
translating button label to user-defined language 1359
translating feature button to user-defined language 1358
translating softkey button label to user-defined language . . . 1358
translating system messages to user-defined language . . . 1354
translating telephone feature buttons and labels 1357
attendant consoles . . . 1361
commands
change display-messages button-labels . . . 1359
change display-messages posted-messages 1355
change display-messages softkey-labels . . . 1358
change display-messages view-buttons . . . 1358
change feature-access-codes . . . 1350, 1353
change station . . . 1352
change system-parameters features . . . 1352
display system-parameters customer-options 1348
considerations . . . 1364
description . . . 1345
custom messages . . . 1347
fixed messages . . . 1346
language options . . . 1345
QSIG support . . . 1347
end-user procedures . . . 1360
interactions . . . 1365
message posting mode . . . 1346, 1365, 1366
screens . . . 1349
Custom Posted Messages . . . 1357
Feature Access Code (FAC) . . . 1351
Feature-Related System Parameters . . . 1353, 1354
Language Translations . . . 1358-1360
Optional Features . . . 1348
Station . . . 1352
System Posted Messages . . . 1355
security code . . . 1351, 1361
selection display mode . . . 1346, 1364, 1365, 1367
special dial tone . . . 1346
PPM, *see* Call Charge Information, description, Periodic Pulse Metering (PPM)
Precedence Call Waiting, *see* Multiple Level Precedence and Preemption (MLPP)
Precedence Calling, *see* Multiple Level Precedence and Preemption (MLPP)
Precedence Routing, *see* Multiple Level Precedence and Preemption (MLPP)
Preemption, *see* Multiple Level Precedence and Preemption (MLPP)
Priority Calling . . . 1369
administering . . . 1370
assigning priority feature button to attendant console 1373
assigning priority feature button to telephone . . . 1374
Class of Service . . . 1371
Feature Access Code . . . 1371
prerequisites . . . 1370
commands
change attendant . . . 1373
change feature-access-codes . . . 1371
change station . . . 1374
change system-parameters features . . . 1370
description . . . 1369
end-user procedures . . . 1375
interactions . . . 1375
screens . . . 1372
Attendant Console . . . 1373
Feature Access Code (FAC) . . . 1372
Feature-Related System Parameters . . . 1371
Station . . . 1374
Privacy . . . 1377
administering . . . 1378
activating Data Restriction for trunk group . . . 1382
for user . . . 1379
prerequisites . . . 1378
commands
change cos . . . 1379
change feature-access-codes . . . 1379
change station . . . 1379
change system-parameters features . . . 1378
change trunk-group . . . 1382
considerations . . . 1383
description . . . 1377
Automatic Exclusion . . . 1378

Data Privacy . . . 1377
Data Restriction . . . 1377
Manual Exclusion . . . 1378
end-user procedures . . . 1383
interactions . . . 1383
screens . . . 1379
Class of Service . . . 1379
Feature Access Codes (FAC) . . . 1379
Feature-Related System Parameters . . . 1378
Station . . . 1380, 1381, 1382
Trunk Group . . . 1382
PSA, *see* Personal Station Access (PSA)
Public Network Call Priority . . . 1385
administering . . . 1387
description . . . 1385
China . . . 1385
Russia . . . 1387
Spain . . . 1387
interactions . . . 1389
China . . . 1389
Russia . . . 1391
screens . . . 1388

Q

QSIG
Call Forwarding . . . 635
definition . . . 1347
Multi-Location Dial Plan . . . 1259
Posted Messages . . . 1347-1354
World Class Routing . . . 1694

R

Record on Messaging . . . 1393
administering . . . 1395
assigning feature button to telephone . . . 1400
assigning parameters . . . 1396
changing characteristics of zip tone . . . 1401
prerequisites . . . 1395
considerations . . . 1405
description . . . 1393
feature button . . . 1393
language options . . . 1394
periodic alerting tone . . . 1394
ready indication tone . . . 1394
recording delay timer . . . 1395
end-user procedures . . . 1404
recording conversation . . . 1404
interactions . . . 1406
screens . . . 1396
troubleshooting . . . 1408
Recorded Telephone Dictation Access . . . 1411
administering . . . 1411
assigning call park button to multiple-call appearance telephone . . . 1412
commands
change station . . . 1412
description . . . 1411
interactions . . . 1413
screens . . . 1412
Station . . . 1413
Release 1 upgrade . . . 1000
Release 2 upgrade . . . 999
Release 3 upgrade . . . 998
Release 4 upgrade . . . 997
Remote Access . . . 1415
administering . . . 1419
assigning authorization codes . . . 1423
disabling Remote Access . . . 1423
enabling Remote Access . . . 1420
prerequisites . . . 1423
Remote Access for trunk group . . . 1426
Remote Access screen . . . 1420
commands
change authorization-codes . . . 1425
change remote-access . . . 1420, 1423
change system-parameters features . . . 1423
change trunk-group . . . 1426
display capacity . . . 1426
display system-parameters customer-options 1423
status remote-access . . . 1416, 1417
considerations . . . 1427
description . . . 1415
alternate facility restriction levels (AFRL) . . . 1418
authorization codes . . . 1418
barrier codes . . . 1417
COR . . . 1418
logoff notification . . . 1418
Night Service . . . 1416
security . . . 1416
end-user procedures . . . 1427
interactions . . . 1428
screens . . . 1419
Authorization Code - COR Mapping . . . 1426
Feature-Related System Parameters . . . 1424
Optional Features . . . 1423
Remote Access . . . 1421
Security-Related System Parameters . . . 1422
System Copyright . . . 1422
Trunk Group . . . 1426
reorder tone . . . 179
reports, *see* reports *under individual feature names*
Restriction - Controlled . . . 1429
administering . . . 1430
considerations . . . 1431
description . . . 1429
end-user procedures . . . 1430
interactions . . . 1432
screens . . . 1430

Return Call to (same) Attendant
Attendant Overflow Timer . . . 290
description . . . 289
Ringing - Abbreviated and Delayed . . . 1433
administering . . . 1434
assigning abbreviated ringing button to user . 1437
assigning ring control to user . . . 1436
prerequisites . . . 1434
commands
change station . . . 1436, 1437
change system-parameters features . . . 1435
considerations . . . 1439
description . . . 1433
ringing types . . . 1433
interactions . . . 1439
screens . . . 1435
Feature-Related System Parameters . . . 1435
Station . . . 1436, 1438
RNX, *see* Uniform Dial Plan (UDP), network location code (RNX)
RTL, *see* Centralized Attendant Service (CAS), release link trunks (RLT)

S

SBS,*see*Separation of Bearer and Signaling (SBS)
screens
CDR System Parameters . . . 985
Configuration Set . . . 986
console-parameters . . . 290
Edit Dialing System Parameters . . . 109
screens, *see* screens *under individual feature names*
screens, *see* screens *under individual feature names*
Security Violation Notification (SVN) . . . 1441
administering . . . 1444
prerequisites . . . 1445
setting up . . . 1445
commands
change remote-access . . . 1447
change station . . . 1448
change system-parameters security . . . 1445
clear measurements security-violations . . . 1443
disable login . . . 1444
disable remote-access . . . 1444
display svn-button-location . . . 1443
enable login . . . 1444
enable remote-access . . . 1444
monitor security-violations . . . 1442
considerations . . . 1450
description . . . 1441
dealing with security violations . . . 1443
disable login IDs . . . 1444
disabling remote access . . . 1444
enabling login ID . . . 1444
enabling remote access . . . 1444
event sequence . . . 1442
reporting . . . 1442
security violation thresholds and notification . 1442
SVN - halt buttons . . . 1443
SVN referral call with announcement . . . 1443
interactions . . . 1450
reports . . . 1450
screens . . . 1445
Login Administration . . . 1447
Remote Access . . . 1448
Security Related System Parameters . . . 1446
Station . . . 1449
Separation of Bearer and Signaling . . . 1453
administering . . . 1461
administering routing for SBS . . . 1468
administering SBS extensions . . . 1470, 1471
local country code and international access code . 1464
prerequisites . . . 1462
SBS trunks and trunk groups . . . 1465
verifying system capacities . . . 1474
commands
add signaling-group . . . 1466
add station . . . 1470
add trunk group . . . 1466
change dialplan analysis . . . 1471
change isdn public-unknown-numbering . . . 1472
change route-pattern . . . 1469
change system-parameters features . . . 1464
change trunk-group . . . 1468
display capacities . . . 1474
display system-parameters customer-options 1462
considerations . . . 1476
description . . . 1453
interworked SBS calls . . . 1461
Tandem SBS calls . . . 1460
typical call connections . . . 1455
typical call setup . . . 1458
interactions . . . 1478
screens . . . 1463
Dial Plan Analysis Table . . . 1472
Feature-Related System Parameters . . . 1465
ISDN Numbering-Public/Unknown Format . . 1473
Route Pattern . . . 1469
Signaling Group . . . 1467
Station . . . 1470
System Capacity . . . 1474, 1475
Trunk Features . . . 1466
Trunk Group . . . 1468
Trunk Groups . . . 1466
Separation of Bearer and Signaling (SBS) . . . 1453
Service Observing . . . 1491
administering . . . 1493
description . . . 1491
listen and talk modes . . . 1492
restrictions . . . 1492

telephone displays . . . 1493
trunk calls . . . 1493
warning and conference tones . . . 1493
end-user procedures . . . 1495
interactions . . . 1496
screens . . . 1494
speed dialing, *see* Abbreviated Dialing (AD)
Station Hunting . . . 1499
administering . . . 1501
assigning hunt-to station to extension . . . 1503
assigning Station Hunting after Coverage . . . 1502
enabling before Coverage . . . 1504
commands
change coverage-path . . . 1502
change station . . . 1503
change system-parameters coverage-forwarding 1504
description . . . 1499
duplicating station . . . 1501
removing station . . . 1500
routing calls through Station Hunting chain . . . 1500
Station Hunting and Call Coverage . . . 1500
interactions . . . 1506
reports . . . 1505
screens . . . 1502
Coverage Path . . . 1503
Station . . . 1504
System Parameters Call Coverage/Call Forwarding 1505
Station Lock . . . 1511
description . . . 1511
end-user procedures . . . 1513
Hot Desking Enhancement . . . 1514
interaction with PSA . . . 1327
Station Lock restrictions . . . 1515
interactions . . . 1514
screens . . . 1513
COR . . . 1513
Feature Access Code (FAC) . . . 1513
Station . . . 1513
Station Security Code . . . 1517
administering . . . 1517
creating Station Security Code . . . 1518
commands
change feature-access-codes . . . 1518
change station . . . 1518
change system-parameters security . . . 1518
description . . . 1517
interactions . . . 1519
screens . . . 1518
Feature Access Codes (FAC) . . . 1518
Security-Related System Parameters . . . 1518
Station . . . 1519
stations, *see* telephones
Supporting TTY Callers . . . 1523
administering . . . 1526
description . . . 1523
handling TTY calls with vectors . . . 1525
setting up announcements for TTY callers . . . 1524
setting up hunt groups for TTY callers . . . 1525
SVN, *see* Security Violation Notification (SVN)

T

TAAS, *see* Night Service, Trunk Answer from Any Station (TAAS)
TCM, *see* Facility Restriction Levels, Traveling Class Marks (TCM)
Team Button . . . 1527
administering . . . 1530
administering audible ringing . . . 1533
administering Call Pickup by going off hook . . . 1535
administering display of station name . . . 1534
administering Priority Ring for speed dialing . . . 1534
configuring the Team Button . . . 1530
viewing status of Team Button . . . 1531
viewing system capacity for Team Button . . . 1532
description . . . 1527
Override Send All Calls/Call Forward . . . 1535
No Overriding of SAC/CFWD . . . 1537
Overriding of SAC/CFWD by Asking . . . 1538
Unconditional Overriding of SAC/CFWD . . . 1537
TEG, *see* Terminating Extension Group (TEG)
Telephone Display . . . 1539
administering . . . 1571
description . . . 1539
button display modes . . . 1540
call-related information display . . . 1544
enhanced telephone display . . . 1548
feature information displays . . . 1547
Integrated Directory . . . 1541
Integrated Directory Data Base . . . 1542
Integrated Directory Mode Button . . . 1542
mapping enhanced display characters . . . 1566
message retrieval . . . 1547
Unicode "Native Name" support . . . 1548
interactions . . . 1573
screens . . . 1572
Date/Time Mode and Formats - English . . . 1552
Date/Time Mode and Formats - French, Italian, Spanish, and User-Defined . . . 1552
Language Translations . . . 1555
Leave Word Calling Formats - English . . . 1556
Leave Word Calling Formats - French, Italian, Spanish, and User-Defined . . . 1556
telephones, use of term . . . 65
Temporary Bridged Appearance . . . 1575
administering . . . 1575
considerations . . . 1576
description . . . 1575
interactions . . . 1577
screens . . . 1576
Tenant Partitioning . . . 1579

administering . . . 1584
assigning sources of music for tenant partitions 1599
assigning tenant partition number to
access telephone . . . 1588
agent login ID . . . 1589
announcement . . . 1590
attendant . . . 1591
data module . . . 1592
hunt group . . . 1593
loudspeaker paging zone . . . 1594
remote access extension . . . 1595
terminating extension group . . . 1597
trunk group . . . 1598
user extension . . . 1596
vector directory number . . . 1598
defining tenant partition . . . 1586
prerequisites . . . 1585
commands
change access-endpoint . . . 1588
change agent loginid . . . 1589
change announcements . . . 1590
change attendant . . . 1591
change data-module . . . 1592
change hunt-group . . . 1593
change music-sources . . . 1599
change paging loudspeaker . . . 1594
change remote-access . . . 1595
change station . . . 1596
change tenant . . . 1586
change term-ext-group . . . 1597
change trunk-group . . . 1598
change vdn . . . 1598
display system-parameters customer-options 1585
description . . . 1579
access control . . . 1581
attendant services . . . 1581
examples . . . 1582
Magic-on-Hold system . . . 1579
Multiple Music-on-Hold . . . 1583
network route selection . . . 1582
Offer B . . . 1579
partitioning tenants . . . 1580
interactions . . . 1601
screens . . . 1585
Access Endpoint . . . 1589
Agent LoginID . . . 1590
Announcements/Audio Sources . . . 1591
Attendant Console . . . 1592
Data Module . . . 1593
Hunt Group . . . 1594
Loudspeaker Paging . . . 1595
Music Sources . . . 1600
Optional Features . . . 1585
Remote Access . . . 1596
Station . . . 1597
Tenant . . . 1586, 1588
Terminating Extension Group . . . 1598
Trunk Group . . . 1598
Vector Directory Number . . . 1599
Terminal Translation Initialization (TTI) . . . 1607
administering . . . 1611
description . . . 1607
analog queue warning ports and external alert ports 1609
attendant consoles . . . 1607
data modules . . . 1608
ISDN-BRI telephones . . . 1608
security . . . 1610
voice and data telephones . . . 1608
interactions . . . 1612
screens . . . 1611
Attendant Console . . . 1611
Data Module . . . 1611
Feature Access Codes (FAC) . . . 1611
Feature-Related System Parameters . . . 1611
Station . . . 1611
Terminating Extension Group (TEG) . . . 1615
administering . . . 1615
considerations . . . 1616
description . . . 1615
interactions . . . 1616
screens . . . 1616
Terminating Extension Group . . . 1616
Time-of-Day Routing, *see* Call Coverage
Transfer . . . 1619
administering . . . 1622
considerations . . . 1623
description . . . 1619
abort transfer . . . 1620
emergency transfer . . . 1621
outgoing trunk to outgoing trunk transfer (OTTOTT) 1621
pull transfer . . . 1619
transfer recall . . . 1620
transfer upon hangup . . . 1620
trunk-to-trunk transfer . . . 1620
interactions . . . 1625
screens . . . 1623
troubleshooting
Abbreviated Dialing (AD) . . . 107
Administrable Language Displays . . . 147
Announcements . . . 209
AUDIX One-Step Recording . . . 321
Call Coverage . . . 475
Extension to Cellular . . . 1004
Feature Access Codes (FAC) . . . 1039
Group Paging . . . 1047
Loudspeaker Paging . . . 1146
Meet-me Conference . . . 1185
Record on Messaging . . . 1408
Trunk Flash . . . 1629

administering . . . 1630
considerations . . . 1631
description . . . 1629
end-user procedures . . . 1630
screens . . . 1630
TTI, *see* Terminal Translation Initialization (TTI)

U

UDP, *see* Uniform Dial Plan (UDP)
Uniform Dial Plan (UDP) . . . 1633
administering . . . 1638
BCC Value field entries . . . 1706
CA-TSC field entries . . . 1707
Hop Lmt field entries . . . 1708
Inserted Digits field entries . . . 1708
ISDN protocols . . . 1649
ITC field entries . . . 1709
IXC field entries . . . 1710
LAR field entries . . . 1710
Numbering Format field entries . . . 1712
Prefix Mark field entries . . . 1713
prerequisites . . . 1639
Service Feature field entries . . . 1713
setting up AAR Digit Analysis Table . . . 1647
setting up AAR Digit Conversion Table . . . 1644
setting up ARS Digit Analysis Table . . . 1650
setting up ARS Digit Conversion Table . . . 1645
setting up extension number portability numbering plan . . . 1653
setting up node number routing . . . 1643
setting up Uniform Dial Plan Table . . . 1641
commands
add station . . . 1635
change aar analysis . . . 1647
change aar digit-conversion . . . 1644
change ars analysis . . . 1650
change ars digit-conversion . . . 1645
change enp-number-plan . . . 1653
change feature-access-codes . . . 1639
change node-number routing . . . 1643
change route-pattern . . . 1704
change uniform-dial plan . . . 1641
display system-parameters customer-options 1639
considerations . . . 1654
description . . . 1633
AAR code extension treatment . . . 1634
administration and processing example . . . 1635
Automatic Alternate Routing (AAR) . . . 1633
Automatic Route Selection (ARS) . . . 1634
code extension treatment . . . 1634
ENP code extension treatment . . . 1634
extension . . . 1634
extension conversion . . . 1633
Extension Number Portability (ENP) . . . 1634
local extension treatment . . . 1635
matching pattern selections . . . 1635
RNX and UDP codes . . . 1636
temporary out of service extension treatment. 1634
Extended Trunk Access (ETA) . . . 1635
interactions . . . 1655
network location code (RNX) . . . 1635
reports . . . 1654
screens . . . 1640
AAR Digit Analysis Table . . . 1647
AAR Digit Conversion Table . . . 1644
ARS Digit Analysis Table . . . 1650
ARS Digit Conversion Table . . . 1646
Extension Number Portability Numbering Plan 1653
Node Number Routing . . . 1643
Optional Features . . . 1639
Route Pattern . . . 1705
Uniform Dial Plan Table . . . 1642
upgrades
from Release 1 . . . 1000
from Release 2 . . . 999
from Release 3 . . . 998
from Release 4 . . . 997

V

v VAL, *see* Announcements, virtual Voice Announcements over LAN (virtual VAL)
VAL, *see* Announcements, Voice Announcements over LAN (VAL)
VIAS, *see* Visually Impaired Attendant Service (VIAS)
virtual VAL, *see* Announcements, virtual Voice Announcements over LAN (virtual VAL)
Visually Impaired Attendant Service (VIAS) . . . 1657
administering . . . 1658
prerequisites . . . 1658
description . . . 1657
interactions . . . 1659
screens . . . 1658
Voice Message Retrieval . . . 1661
administering . . . 1661
description . . . 1661
interactions . . . 1663
screens . . . 1662
voice terminals, *see* telephones

W

WAE, *see* Wideband Switching, wideband access endpoint (WAE)
Whisper Paging . . . 1665
administering . . . 1666
prerequisites . . . 1666
description . . . 1665
call redirection overrides . . . 1665

group answering environment 1666
network restrictions 1666
speakerphones 1666
end-user procedures 1668
interactions 1669
screens 1667
Wideband Switching 1673
administering 1685
considerations 1686
description 1673
blocking prevention 1685
channel allocation 1674
data backup connection 1678
data service unit/channel service unit 1677
direction of trunk hunting within facilities . . . 1680
endpoint applications with signaling 1675
facility lists 1679
glare prevention and resolution 1683
guidelines and examples 1678
H0 channels 1682
H11 channels 1680
H12 channels 1681
high-speed video conferencing 1678
ISDN-PRI terminal adapters 1675
ISDN-PRI trunk groups and channel allocation 1679
linear trunk hunt 1685
line-side T1 or E1 facility 1677
line-side T1 or E1 ISDN-PRI facilities 1676
N x DS0 channels 1682
networking 1679
nightly file transfers 1678
nonsignaling endpoint applications 1677
PRI endpoints (PE) 1676
primary data connectivity 1679
scheduled batch processing 1678
universal digital signal level 1 board 1676
uses for 1674
wideband access endpoint (WAE) 1677
interactions 1686
port network (PN) preferential trunk routing . . . 1680
screens 1686
World Class Routing 1689
administering 1696
adding new area code 1720
adding new prefix 1722
assigning FAC for ARS 1699
assigning telephone to partition group 1726
defining interexchange carrier calls 1716
defining local information calls 1719
defining operator-assisted calls 1715
displaying ARS analysis information 1702
prerequisites 1701, 1724, 1729
setting up location ARS FAC 1701
setting up partition groups 1724
setting up route pattern 1704
setting up Time of Day Routing 1729
using ARS to restrict outgoing calls 1722
using COR and FRL to manage calling privileges. 1698
using restricted area code prefixes 1716
using wildcards 1718
commands
change ars analysis 1717, 1718, 1719, 1721, 1722
change cor 1699, 1727
change dialplan analysis 1700
change features-access-codes 1700
change locations 1702
change partition-route-table 1725
change station 1698, 1728
change time-of-day 1730
display ars analysis 1703, 1715, 1716
display system-parameters customer-options 1701, 1724, 1729
display time-of-day 1729
display toll 1722
list ars analysis 1703
list ars route-chosen 1720, 1724
list cor 1726
description 1689
ARS analysis 1692
ARS dialing without FAC 1693
Automatic Alternate Routing (AAR) 1689
Automatic Route Selection (ARS) 1689
digit conversion 1692
overview 1690
partitioning 1695
extensions 1695
dialable extensions 1695
internal extensions 1695
nondialable extensions 1695
interactions 1732
interexchange carrier (IXC) 1716
screens 1697
ARS Digit Analysis Report 1704
ARS Digit Analysis Table 1703, 1715, 1717, 1719, 1721, 1723
ARS Route Chosen Report 1720, 1725
Class of Restriction 1699, 1728
Class of Restriction Information 1727
Dial Plan Analysis Table 1700
Feature Access Code (FAC) 1701
Locations 1702
Optional Features 1701, 1724, 1729
Partition Routing Table 1726
Station 1698, 1728
Time of Day Routing Plan 1730, 1731
wildcards 1716, 1718
Worldwide Numbering and Dialing Plan (WNDP), *see* Multiple Level Precedence and Preemption (MLPP)