Migrating to Avaya S8xxx Servers and Media Gateways

03-300412
Issue 5.0
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 support information, please see the complete document, *Avaya Support Notices for Hardware Documentation*, document number 03-600759.

To locate this document on our Web site, 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

Chapter 1: Introduction 31
Port network connectivity 32
Reliability and availability 33
Resources 35
How this book is designed and organized 37
Migrating LSPs and ESS servers 41
S8400 Server 42
Hardware migrations 42
DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway . . 42
Avaya IP600 in a G600 42
S8500-Series Server 43
Hardware migrations 43
DEFINITY Server SI in an MCC 44
DEFINITY Server SI in an SCC 44
DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway . . 44
Avaya IP600/S8100 in a G600 45
S8700-Series Server 45
Hardware migrations 46
DEFINITY Server SI in an MCC 46
DEFINITY Server SI in an SCC 46
DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway . . 47
Avaya IP600/S8100 in a G600 47
License and Avaya authentication files 47
Generating and retrieving license and authentication files 48
Logins and passwords 48
Caution about platform/PNC license settings for the S8700-series Server 48
Server Migration Paths 50
Server Migration Paths for Communication Manager Release 5.2 50

Chapter 2: Migrating to an Avaya S8400 Server 53
Migration paths for S8400 Servers 53
Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway with a Linear Flash53
Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway using Xmodem 54
Migrating from an S8100 using ftp 54
Migrating all other systems 54
Migrations from existing DEFINITY and Linux platforms 54
Hardware migrations 55
DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway . . 55

Migration modules 55

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Linear flash) 57

Migration paths 57
Installing the linear card reader software 58
Checklists 58
Premigration setup checklist 61
Presite migration checklist 62
On site migration checklist 63
Documentation checklist for migrations 65
Performing a migration 65
Premigration administration 66
Accessing Remote Feature Activation 66
Computer requirements 66
User requirements 66
Going to the Remote Feature Activation web site 67
Connecting to the processor 68
Removing netcon data modules 68
Verifying system status 69
Recording all busyouts 69
Recording node names and IP addresses 70
Saving translations 70
Migration tasks. 70
Verifying hardware. 71
Turning off power to all cabinets 71
Removing circuit packs 71
Inserting circuit packs. 72
Connecting cables. 72
Replacing the TN799C C-LAN circuit pack 73
Installing TN771 Maintenance/Test 73
Translation migrations 73
Installing the software load 74
Configuring the server 75
Installing the license and authentication file 77
Copying translation files to the server 78
Post-migration administration 79
Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs 80
Using static addressing 80
Logging in to the TN8412AP Server IP Interface (SIPI) 81
Setting the control interface 82

Resetting the TN8412AP Server IP Interface (SIPI) 83
Enabling control of the TN8412AP Server IP Interface (SIPI) 84
Verifying TN8412AP Server IP Interface (SIPI) translations. 85
Verifying TN8412AP Server IP Interface (SIPI) connectivity 85
Verifying the customer data. 85
Verifying circuit pack locations. 86
Verifying circuit pack insertion 86
Verifying the IP addresses 86
Checking the link status. 87
Upgrading firmware 87
Testing the installation 88
Busying out previously busied-out trunks. 88
Troubleshooting the migration 88
Returning replaced equipment 88

Migrating from an IP600 or S8100 to an S8400 Server 91
Migration paths 91
Replacement of INTUITY AUDIX Messaging with Communication Manager Messaging92
Installation of Communication Manager Messaging software 92
INTUITY AUDIX data that can be reused in Communication Manager Messaging and data that must be reinput 92
Removing unused INTUITY AUDIX ports or hunt groups. 93
Checklists 94
Premigration setup 97
Presite migration checklist 98
On site migration checklist 99
Performing a migration 101
Premigration administration 101
Connecting to the processor 102
Saving translations 102
Verifying system status 102
Recording all busyouts 103
Recording node names and IP addresses 103
Migration tasks. 104
Verifying hardware. 104
Opening a SAT session 104
Copying translation files 105
Opening an ftp session 105
Moving the translation files 106
Turning off power to all cabinets 106

Removing circuit packs 106
Inserting circuit packs 107
Connecting cables 107
Replacing the TN799C C-LAN circuit pack 108
Installing TN771 Maintenance/Test 108
Translation migration 108
Setting telnet parameters 109
Installing the software load 109
Configuring the server 111
Installing the license and authentication file 113
Copying translation files to the server 113
Post-migration administration 114
Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs 115
Using static addressing 115
Logging in to the TN8412AP Server IP Interface (SIPI) 116
Setting the control interface 116
Resetting the TN8412AP Server IP Interface (SIPI) 118
Enabling control of the TN8412AP Server IP Interface (SIPI) 119
Verifying TN8412AP Server IP Interface (SIPI) translations 119
Verifying TN8412AP Server IP Interface (SIPI) connectivity 120
Verifying the customer data 120
Verifying circuit pack locations 120
Verifying circuit pack insertion 121
Verifying the IP addresses 121
Checking the link status 121
Upgrading firmware 122
Administering Communication Manager Messaging 122
Testing the installation 122
Busying out previously busied-out trunks 123
Troubleshooting the migration 123
Returning replaced equipment 123

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (ATA flash card) 125

Migration paths 125
Checklists 125
Premigration setup 128
Presite migration checklist 129
On site migration checklist 129
Documentation checklist for migrations 131

Performing a migration 131
Premigration administration 132
Connecting to the processor 132
Removing netcon data modules 132
Verifying system status 133
Recording all busyouts 134
Recording node names and IP addresses 134
Saving translations 134
Migration tasks. 135
Verifying hardware. 135
Turning off the power to the control cabinet 136
Removing circuit packs 136
Inserting circuit packs. 136
Connecting cables. 137
Replacing the TN799C C-LAN circuit pack 137
Installing TN771 Maintenance/Test 138
Translation migrations 138
Installing the software load 138
Configuring the server 140
Installing the license and authentication file 142
Copying translation files to the server 143
Post-migration administration 144
Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs 144
Using static addressing 144
Logging in to the TN8412AP Server IP Interface (SIPI) 145
Setting the control interface 146
Resetting the TN8412AP Server IP Interface (SIPI) 147
Enabling control of the TN8412AP Server IP Interface (SIPI) 148
Verifying TN8412AP Server IP Interface (SIPI) translations. 149
Verifying TN8412AP Server IP Interface (SIPI) connectivity 149
Verifying the customer data. 149
Verifying circuit pack locations. 150
Verifying circuit pack insertion 150
Verifying the IP addresses 150
Checking the link status. 151
Upgrading firmware 151
Testing the installation 152
Busying out previously busied-out trunks. 152
Troubleshooting the migration 152

Chapter 3: Migrating to an Avaya S8500C and S8510 Server. 153
Migrations from existing DEFINITY and Linux platforms 153
Hardware migrations 154
DEFINITY Server SI in an MCC 154
DEFINITY Server SI in an SCC 154
DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway . . 155
Avaya IP600/S8100 in a G600 155
Migration modules 155

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Xmodem) 157
Migration paths 157
Checklists 158
Premigration setup 161
Presite migration checklist 162
On site migration checklist 163
Documentation checklist for migrations 165
Performing a migration 166
Premigration administration 166
Connecting to the processor 166
Removing netcon data modules 167
Saving translations 167
Verifying system status 168
Recording all busyouts 168
Recording node names and IP addresses 169
Migration tasks. 169
Verifying hardware. 169
Connecting to the SAT 170
Copying translation files 170
Turning off power to all cabinets 171
Removing circuit packs 171
Inserting circuit packs. 171
Connecting cables. 172
Replacing the TN799C C-LAN circuit pack 172
Installing TN771 Maintenance/Test 173
Translation migrations 173
Installing the software load 173
Configuring the server 175
Installing the license and authentication file 177
Copying translation files to the server 178

Closing all sessions 179
Post-migration administration 179
Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs 180
Using static addressing 180
Logging in to the TN8412AP Server IP Interface (SIPI) 181
Setting the control interface 181
Resetting the TN8412AP Server IP Interface (SIPI) 183
Enabling control of the TN8412AP Server IP Interface (SIPI) 184
Verifying TN8412AP Server IP Interface (SIPI) translations. 184
Verifying TN8412AP Server IP Interface (SIPI) connectivity 185
Verifying the customer data. 185
Verifying circuit pack locations. 185
Verifying circuit pack insertion 186
Verifying the IP addresses 186
Checking the link status. 186
Upgrading firmware 187
Testing the installation 187
Busying out previously busied-out trunks. 188
Troubleshooting the migration 188
Returning replaced equipment 188

Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8500-Series Server 189
Migration paths 189
Checklists 190
Premigration setup 192
Presite migration checklist 195
On site migration checklist 196
Documentation checklist for migrations 196
Performing a migration 197
Premigration administration 198
Connecting to the processor 198
Verifying system status 198
Recording all busyouts 199
Recording node names and IP addresses 199
Saving translations 199
Translation migration 200
Accessing the System Management Interface (SMI) 200
Copying translation files to server 200
Restoring translation files 201

Administering the IPSIs 201
Adding IPSI translations to Communication Manager 202
Setting the alarm activation level 202
Backing up translations 203
Migration tasks. 203
Verifying hardware. 203
Changing the control cabinet to a port network 204
Turning off the power to the control cabinet 204
Replacing the processor circuit pack 205
Replacing the TN799C C-LAN circuit pack 205
Installing TN771 Maintenance/Test circuit pack 206
Connecting the IPSI to the network 206
Postmigration administration 206
Assigning IP addresses to the IPSI circuit packs 207
Using static addressing 207
Logging in to the IPSI 208
Setting the control interface 208
Setting the VLAN and diffserv parameters 209
Resetting the IPSI 210
Verifying IPSI translations 211
Verifying IPSI connectivity 211
Enabling control of the IPSI 212
Verifying the customer data. 212
Verifying circuit pack locations 213
Verifying circuit pack insertion 213
Verifying the IP addresses 213
Checking the link status. 214
Upgrading firmware 214
Testing the installation 215
Busying out previously busied-out trunks 215
Troubleshooting the migration 215
Returning replaced equipment 215

Migrating a DEFINITY ONE/S8100 to an S8500-Series Server 217
Migration paths 217
Checklists 218
Premigration setup checklist 220
Premigration setup 220
Presite migration checklist 223
On site migration checklist 224

Documentation checklist for migrations 224
Performing a migration 225
Premigration administration 226
Connecting to the processor 226
Recording node names and IP addresses 227
Saving translations 227
Recording IP settings 227
Translation migration 228
Accessing the server command line interface with ssh protocol 228
Clearing the ARP cache on the laptop computer 230
Clearing the Web browser cache on the laptop 230
Accessing the System Management Interface (SMI) 231
Copying translation files to server 232
Restoring translation files 232
Administering the IPSIs 233
Adding IPSI translations to Communication Manager 233
Setting the alarm activation level 234
Backing up translations 234
Migration tasks. 234
Verifying hardware. 235
Changing the control cabinet to a port network 235
Turning off the power to the control cabinet 236
Replacing the processor circuit pack 236
Replacing the TN799C C-LAN circuit pack 237
Installing TN771 Maintenance/Test circuit pack 237
Connecting the IPSI to the network 238
Post-migration administration 238
Assigning IP addresses to the IPSI circuit packs 238
Using static addressing 238
Logging in to the IPSI 239
Setting the control interface 240
Setting the VLAN and diffserv parameters 241
Resetting the IPSI 241
Verifying IPSI translations 242
Verifying IPSI connectivity 243
Verifying the license file. 243
Verifying the customer data. 243
Verifying circuit pack locations. 244
Verifying circuit pack insertion 244
Verifying the IP addresses 244

Checking the link status 245
Upgrading firmware 245
Testing the installation 246
Busying out previously busied-out trunks 246
Troubleshooting the migration 246
Returning replaced equipment 246

Migrating an Avaya IP600/S8100 to an S8500-Series Server 247
Migration paths 247
Checklists 247
Premigration setup 250
Presite migration checklist 253
On site migration checklist 254
Documentation checklist for migrations 255
Performing a migration 256
Premigration administration 257
Connecting to the processor 257
Recording node names and IP addresses 257
Saving translations 258
Recording IP settings 258
Translation migration 259
Accessing the server command line interface with ssh protocol 259
Clearing the ARP cache on the laptop computer 261
Clearing the Web browser cache on the laptop 261
Accessing the System Management Interface (SMI) 262
Copying translation files to server 262
Restoring translation files 262
Administering the IPSIs 263
Adding IPSI translations to Communication Manager 264
Setting the alarm activation level 264
Backing up translations 264
Migration tasks 265
Verifying hardware 265
Changing the IP600 control chassis to a port network 265
Turning off the control chassis 266
Replacing I/O cables 267
Replacing the processor circuit pack 269
Replacing the TN799C C-LAN circuit pack 270
Installing TN771 Maintenance/Test circuit pack 270
Connecting the IPSI to the network 270

Post-migration administration 271
Assigning IP addresses to the IPSI circuit packs 271
Using static addressing 271
Logging in to the IPSI 272
Setting the control interface 273
Setting the VLAN and diffserv parameters 274
Resetting the IPSI 274
Verifying IPSI translations 275
Verifying IPSI connectivity 276
Enabling control of the IPSI 276
Verifying the license file 277
Verifying the customer data 277
Verifying circuit pack locations 277
Verifying circuit pack insertion 277
Verifying the IP addresses 278
Checking the link status 278
Upgrading firmware 278
Testing the installation 279
Busying out previously busied-out trunks 279
Troubleshooting the migration 280
Returning replaced equipment 280

Migrating an Avaya S8500A or S8500B Server to an S8500C or S8510 Server 281
Enterprise Survivable Servers (ESS) 281
Local Survivable Processor (LSP) 282
Prerequisites 282
Pre-migration administration 283
Upgrading media gateways and LSPs 283
Upgrading firmware 284
Upgrading software on the LSP 284
Performing the migration 285
On the S8500 Server 285
Clearing the Web browser cache on the laptop 285
Connecting to the S8500 Server 286
Starting a SAT session (main server only) 286
Disabling scheduled maintenance 287
Checking for translation corruption 287
Saving translations (main only) 287
Obtaining the product ID on the S8500 Server 288
Obtaining the cluster ID 288

Run almcall 288
Run almenable 288
Run modserve 289
Copy the configuration information for the S8500 289
How to copy the configuration screens 289
Viewing the configuration screens to copy or print 290
Backing up the translation files to the compact flash card 291
Shutting down the S8500 Server 291
Disconnecting the cables 292
Remove the S8500 from the rack 292
On the S8510 Server 292
Install the S8510 in the rack 292
Inserting the Communication Manager CD in the CD-ROM drive 292
Turning on the S8510 Server 293
Accessing the S8510 Server 293
Setting up a Telnet session 293
Installing Communication Manager 294
Accessing the System Management Interface (SMI) 295
Verify date, time, and timezone 296
Copying files to the S8510 Server 296
Installing service pack updates, if any 296
Creating a super-user login 297
Configuring the S8510 Server 298
About the Avaya Installation Wizard 298
Configuring the S8510 using the Avaya Installation Wizard 299
Configuring the S8510 using the Configure Server web pages 299
License File (if not installed with AIW) 300
Authentication File (if not installed with AIW) 300
Product ID (if not installed with AIW) 300
Reboot the server 301
Connecting the network cables 301
Connecting the SAMP cables 302
Verifying the server connection to the customer LAN 302
Enabling firewall settings 303
Restoring SNMP configuration (if needed) 303
Installing SAMP firmware 303
Restoring the translations (main server only) 303
Reset the system 304
Testing the system using SAT commands 304
Testing the system using the System Management Interface (SMI) 304
Resolving alarms 305

Enabling alarms to INADS by way of a modem 305
Enabling alarms to INADS by way of the SNMP module 305
Enable the modem to receive calls 306
Enabling scheduled maintenance 306
Checking for translation corruption with the SAT 306
Saving translations (main server only) 306
Backing up files to the network 306
Releasing alarm suppression (optional) 307
Logging off all administration applications 307
Disconnecting from the S8510 Server 307

Migrating an Avaya S8400 Server to an S8500-Series Server 309
Checklists 310
Premigration setup 312
On site migration checklist 315
Documentation checklist for migrations 315
Performing a migration 316
Premigration administration 317
Connecting to the server 317
Verifying system status 317
Recording all busyouts 318
Recording node names and IP addresses 318
Saving translations 318
Accessing the System Management Interface (SMI) 319
Backing up recovery system files 319
Migration tasks 320
Verifying hardware 320
Turning off the power to the port network 320
Shutting down the Avaya S8400 Server and powering down the Media Gateway 321
Removing the TN circuit packs 323
Installing the IPSI 323
Turning on power to the port network 324
Turning on G650 Media Gateway 324
Assigning IP addresses to the IPSI circuit packs 325
Using static addressing 325
Clearing the ARP cache on the laptop computer 326
Logging in to the IPSI 326
Setting the control interface 327
Resetting the IPSI 328
Postmigration administration 329

Clearing the Web browser cache on the laptop 329
Connecting to the server 330
Clearing the ARP cache on the laptop computer 330
Accessing the System Management Interface (SMI) 331
Migrating translation files 331
Starting a SAT session 332
Verifying IPSI translations 332
Verifying IPSI connectivity 333
Verifying the customer data. 333
Verifying circuit pack locations. 333
Verifying circuit pack insertion 334
Verifying the IP addresses 334
Checking the link status. 334
Upgrading firmware 335
Testing the installation 335
Busying out previously busied-out trunks. 335
Checking for translation corruption 336
Resolving alarms 336
Backing up system files. 336
Logging off all administration applications 337
Registering Communication Manager 337
Troubleshooting the migration 337
Returning replaced equipment 337

Chapter 4: Migrating to an Avaya S8730 Server. 339
Migrations from existing DEFINITY and Linux platforms 339
Hardware migrations 340
DEFINITY Server R or SI in an MCC 340
DEFINITY Server SI in an SCC 341
DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway . . 341
Avaya IP600/S8100 in a G600 341
Migration modules. 342

Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8730 Server with IP-PNC 343
Migration paths 343
Checklists 344
Premigration setup 346
Presite migration checklist 350
On site migration checklist 351

Documentation checklist for migrations 353
Performing a migration 353
Premigration administration 354
Connecting the IPSI to the network 354
Verifying system status 354
Recording all busyouts 355
Recording node names and IP addresses 355
Saving translations 355
Translation migrations 356
Accessing the server 356
Checking system status. 356
Verifying the license file. 357
Restoring data for a migration 357
Accessing the server from your laptop 357
Verifying the license file. 357
Copying the translation files to the server 358
Restoring the translation files 358
Connecting to the standby server 358
Connecting to the active server. 358
Installing the translations 359
Enabling the system for IPSI translations 359
Adding IPSI information 360
Setting IPSI duplication (high-reliability critical-reliability only) 360
Setting the alarm activation level 361
Backing up translations on the S8700-series server 361
Migration tasks. 361
Verifying hardware. 362
Changing the IP600 control chassis to a port network 362
Turning off the power to the control cabinet 363
Replacing the processor circuit pack 363
Replacing the TN799C C-LAN circuit pack 365
Installing TN771 Maintenance/Test circuit pack 365
Connecting the IPSI to the network 365
Post-migration administration 366
Assigning IP addresses to the IPSI circuit packs 366
Using static addressing 366
Logging in to the IPSI 367
Setting the control interface 368
Setting the VLAN and diffserv parameters. 369
Resetting the IPSI 369

Verifying IPSI translations 370
Verifying IPSI connectivity 371
Enabling control of the IPSI 371
Verifying the customer data. 372
Verifying circuit pack locations. 372
Verifying circuit pack insertion 372
Verifying the IP addresses 373
Checking the link status. 373
Upgrading firmware 373
Testing the installation 374
Busying out previously busied-out trunks. 374
Troubleshooting the migration 375
Returning replaced equipment 375

Migrating a DEFINITY ONE/S8100 to an S8730 Server with IP-PNC . . . 377
Migration paths 377
Checklists 378
Premigration setup 380
Presite migration checklist 384
On site migration checklist 385
Documentation checklist for migrations 387
Performing a migration 387
Premigration administration 388
Connecting to the processor 388
Recording node names and IP addresses 389
Saving translations 389
Recording IP settings 389
Translation migrations 390
Accessing the System Management Interface (SMI) 390
Checking system status. 391
Verifying the license file. 391
Restoring data for a migration 391
Accessing the server from your laptop 391
Verifying the license file. 392
Copying the translation files to the server 392
Restoring the translation files 392
Connecting to the standby server 392
Connecting to the active server. 393
Installing the translations 393
Enabling the system for IPSI translations 393

Adding IPSI information 394
Setting IPSI duplication (high-reliability critical-reliability only) 394
Setting the alarm activation level 395
Backing up translations on the S8700-series server 395
Migration tasks. 395
Verifying hardware. 396
Changing the control cabinet to a port network. 396
Turning off the power to the control cabinet 397
Replacing the processor circuit pack 398
Replacing the TN799C C-LAN circuit pack 398
Installing TN771 Maintenance/Test circuit pack. 399
Connecting the IPSI to the network 399
Post-migration administration 399
Assigning IP addresses to the IPSI circuit packs 399
Using static addressing 400
Logging in to the IPSI 401
Setting the control interface 401
Setting the VLAN and diffserv parameters. 402
Resetting the IPSI 403
Verifying IPSI translations 404
Verifying IPSI connectivity 404
Enabling control of the IPSI. 405
Verifying the customer data. 405
Verifying circuit pack locations. 406
Verifying circuit pack insertion 406
Verifying the IP addresses 406
Checking the link status. 407
Upgrading firmware 407
Testing the installation 408
Busying out previously busied-out trunks. 408
Troubleshooting the migration 408
Returning replaced equipment 408

Migrating an Avaya IP600/S8100 to an S8730 Server with IP-PNC . . . 409
Migration paths 409
Checklists 410
Premigration setup 412
Presite migration checklist 416
On site migration checklist 417
Documentation checklist for migrations 418

Performing a migration 418
Premigration administration 419
Connecting to the processor 419
Recording node names and IP addresses 420
Saving translations 420
Recording IP settings 421
Migrating the translation files. 421
Accessing the System Management Interface (SMI) 421
Checking system status. 422
Verifying the license file. 422
Restoring data for a migration 422
Accessing the server from your laptop 423
Verifying the license file. 423
Copying the translation files to the server 423
Restoring the translation files 423
Connecting to the standby server 424
Connecting to the active server. 424
Installing the translations 424
Enabling the system for IPSI translations 425
Adding IPSI information 425
Setting IPSI duplication (high-reliability critical-reliability only) 426
Setting the alarm activation level 426
Backing up translations on the S8700-series server 426
Migration tasks. 427
Verifying hardware. 427
Changing the IP600 control chassis to a port network 427
Turning off the control chassis 428
Replacing I/O cables 429
Replacing the processor circuit pack 431
Replacing the TN799C C-LAN circuit pack 432
Installing TN771 Maintenance/Test circuit pack 432
Connecting the IPSI to the network 432
Post-migration administration 433
Assigning IP addresses to the IPSI circuit packs 433
Using static addressing 433
Logging in to the IPSI 434
Setting the control interface 435
Setting the VLAN and diffserv parameters. 436
Resetting the IPSI 436
Verifying IPSI translations 437

Verifying IPSI connectivity 438
Enabling control of the IPSI 438
Verifying the customer data. 439
Verifying circuit pack locations 439
Verifying circuit pack insertion 439
Verifying the IP addresses 439
Checking the link status. 440
Upgrading firmware 440
Testing the installation 441
Busying out previously busied-out trunks 441
Troubleshooting the migration 441
Returning replaced equipment 442

Migrating an Avaya S8400 Server to an S8730 Server 443
Migration paths 443
Checklists 444
Premigration setup 446
On site migration checklist 448
Performing a migration 449
Premigration administration 449
Connecting to the server 449
Verifying system status 449
Recording all busyouts 450
Recording node names and IP addresses 450
Saving translations 451
Accessing the System Management Interface (SMI) 451
Backing up recovery system files 451
Migration tasks. 452
Verifying hardware. 452
Turning off the power to the port network 452
Shutting down the Avaya S8400 Server and powering down the Media Gateway 454
Removing the TN circuit packs 455
Installing the IPSI 456
Turning on power to the port network 456
Turning on G650 Media Gateway 456
Assigning IP addresses to the IPSI circuit packs 457
Using static addressing 457
Clearing the ARP cache on the laptop computer 458
Logging in to the IPSI 459
Setting the control interface 459

Resetting the IPSI 461
Postmigration administration 462
Clearing the Web browser cache on the laptop 462
Connecting to the active server 463
Accessing the System Management Interface (SMI) 463
Clearing the ARP cache on the laptop computer 463
Busying-out the server 464
Migrating translation files 464
Verifying IPSI translations 465
Verifying IPSI connectivity 465
Verifying the customer data. 466
Verifying circuit pack locations. 466
Verifying circuit pack insertion 466
Verifying the IP addresses 467
Checking the link status. 467
Upgrading firmware 467
Testing the installation 468
Busying out previously busied-out trunks. 468
Checking for translation corruption 469
Resolving alarms 469
Backing up system files. 469
Logging off all administration applications 470
Registering Communication Manager 470
Releasing the standby server. 470
Troubleshooting the migration 470
Returning replaced equipment 470

Migrating an S8500-Series Server to an S8730 Server 471
Upgrading media gateways LSPs and ESS servers. 471
Enterprise Survivable Servers (ESS). 471
Local Survivable Servers (LSP). 472
Prerequisites. 472
Premigration administration 473
Hardware verification 473
Upgrading firmware 474
Upgrading G150, G250, G350, G430, G450, G700, J4350, or J6350 Media Gateways and local survivable processors (if being used) 474
Upgrading software on the LSP 475
Migration tasks on the S8500-Series Server. 476
Connecting to the server 476

Checking for translation corruption 476
Disabling scheduled maintenance 476
Saving translations (main only). 477
Obtaining the product ID on the S8500-Series Server 477
Obtaining the Cluster ID. 477
Run almcall. 478
Run almenable 478
Run modserve 478
Copy the configuration information for the S8500-Series Server 478
How to copy the configuration screens 479
Viewing the configuration screens to copy or print 479
Backing up the translation files to the compact flash. 480
Shutting down the S8500-Series Server 481
Disconnecting the cables 481
Remove the S8500-Series Server and the side rails from the rack. 482
On the first S8730 Server 483
Removing a DAL1 or installing a DAL2 card. 483
Installing the first S8730 Server in the rack 483
Inserting the Communication Manager software distribution CD 483
Connecting the cables to the first S8730 Server 484
Accessing the first S8730 Server 486
Setting up a Telnet session 488
Installing Communication Manager 488
Insert the USB flash drive in the USB port. 490
Accessing the System Management Interface (SMI) 490
Checking the software version 491
Verifying date and time 491
Copying files to the server (if any) 491
Installing security and service pack updates, if any 492
Stopping Communication Manager on the first S8730 Server 493
Configuring the first S8730 Server 493
Configuring the server using AIW 493
Configuring the first server using the Configure Server web pages 494
Verifying connectivity from the first S8730 Server to the network server 494
Restoring the translations 495
Verifying the first S8730 Server configuration. 495
Confirming the product ID on the first S8730 Server 496
Rebooting the first S8730 Server 496
Accessing the first S8730 Server 496
Initializing and busyout on the first S8730 Server. 497

Configuring the ESS and the LSP for compatibility with S8730 497
Performing an integrity check on the first S8730 Server 498
Making the first S8730 Server active 499
Accessing the first S8730 Server 499
Releasing the first S8730 Server 499
Verifying the first S8730 Server is active. 499
Creating a super-user login 500
Installing the license and authentication files 501
Stopping and starting the ESS servers 501
Verifying server operation 502
On the second S8730 502
Verifying the DAL2 card 502
Installing the second S8730 Server in the rack 502
Inserting the Communication Manager software distribution CD 503
Connecting the cables to the second S8730 Servers 504
Accessing the server 507
Installing Communication Manager 507
Insert the USB flash drive in the USB port. 508
Accessing the second S8730 Server 509
Checking the software version 509
Verifying date and time 509
Copying files to the second S8730 Server (if any). 509
Installing security and service pack updates, if any 510
Stopping Communication Manager on the second S8730 Server 511
Configuring the second S8730 Server 511
Configuring the server using AIW 511
Configuring the first server using the Configure Server web pages 512
Verifying connectivity from the second S8730 Server to the network server 512
Restoring the translations 513
Verifying the second S8730 Server configuration. 513
Confirming the product ID on the second S8730 Server 514
Rebooting the second S8730 Server 514
Accessing the second S8730 Server 515
Performing an integrity check on the second S8730 Server 515
Connecting the duplication cables 516
Releasing the second S8730 Server 517
Verifying the second S8730 Server is in standby state 518
Releasing alarm suppression (optional) 518
Logging off all administration applications 518
Disconnecting from the second S8730 Server. 518

On the active (first) S8730 Server 519
Accessing the active server 519
Resolving alarms 519
Enabling scheduled maintenance 519
Saving translations 520
Backing up files on the active S8730 Server 520
Releasing alarm suppression (optional) 520
Logging off all administration applications 520
Disconnecting from the active S8730 Server 520
On the standby S8730 Server 521
Accessing the standby server 521
Resolving alarms 521
Backing up files on the standby S8730 Server 521
Releasing alarm suppression (optional) 522
Logging off all administration applications 522
Disconnecting from the standby server 522
Completing the migration 523
Registering the system 523
Removing customer files from the Services laptop 523
Interchanging servers (optional) 523
Accessing the standby server 523
Interchanging servers (optional) 523
Performing an integrity check on the active S8730 Server 524

Migrating from an S8700, S8710 or S8720 to an S8730 Server 525
Enterprise Survivable Servers (ESS) 525
Local Survivable Servers (LSP) 526
Checklists 527
Presite checklists 527
Additional tasks 529
Presite migration checklist 530
On site migration checklist 531
Documentation checklist for migrations 531
Premigration administration 533
Upgrading media gateways, LSPs, and ESS servers (if being used) 533
Duplex ESS migration workflow 533
Upgrading software on the LSP 534
Hardware verification 534
Enterprise Survivable Servers resetting 535

Local survivable processors 535
Migration tasks. 535
On the active S8700, S8710, or S8720 Server 535
Configuring Telnet for Windows 2000 or WindowsXP 536
Connecting to the active server 537
Accessing the System Management Interface (SMI) 539
Checking the software release 539
Clearing alarms 539
Starting a SAT session 540
Recording all busyouts 540
Checking clock synchronization 540
Disabling scheduled maintenance 541
Busying out MMI circuit packs with SAT for a duplicated control network only (main server only). 541
Checking for translation corruption 542
Saving translations (main only). 542
Checking the CNC status 543
Backing up the active S8700, S8710, or S8720 Server 543
Backing up the configuration data and translations to the USB-connected Compact Flash card 545
Backing up the configuration data and translations to a server on the network546
Backing up the configuration data and translations using Linux Migration Backup to the USB-connected Compact Flash card 546
Backing up the configuration data and translations using Linux Migration Backup to a server on the network 547
Obtaining the Product ID on the active server. 548
Looking up server configuration on the active server 548
Disconnecting from the active S8700, S8710, or S8720 Server. 549
On the standby S8700, S8710, or S8720 Server 549
Connecting to the standby server 549
Accessing the standby server 550
Checking the software release 550
Checking the CNC status 550
Backing up the standby S8700, S8710, or S8720 Server 551
Backing up the configuration data and translations to the USB-connected Compact Flash card 553
Backing up the configuration data and translations to a server on the network553
Backing up the configuration data and translations using Linux Migration Backup to the USB-connected Compact Flash card 554
Backing up the configuration data and translations using Linux Migration Backup to a server on the network 554
Obtaining the Product ID on the standby server 555

Looking up server configuration information on the standby server 555
Busying out the standby S8700, S8710, or S8720 Server 557
Shutting down the standby S8700, S8710, or S8720 Server 557
Removing the duplication cables 557
Removing the standby S8700, S8710, or S8720 Server from the rack 557
Removing the DAL2 card, if necessary 558
On first S8730 Server 558
Installing the DAL2, if necessary 558
Installing the first S8730 Server in the rack 558
Inserting the Communication Manager software distribution CD 559
Connecting the cables to the first S8730 Server 559
Accessing the first S8730 Server 561
Installing Communication Manager 563
Insert the USB flash drive in the USB port 564
Accessing the System Management Interface (SMI) 565
Checking the software version 565
Verifying date and time 565
Copying files to the server (if any) 565
Installing security and service pack updates, if any 566
Stopping Communication Manager on the first S8730 Server 567
Configuring to allow restoring configuration data and translations from a server on the network 567
Verifying connectivity from the first S8730 Server to the network server 568
Configuring to allow restoring configuration data and translations from the USB flash card 568
Restoring configuration data and translations to the first S8730 Server 569
Restoring data backed up to the Compact Flash card 570
Restoring data backed up to the customer network 571
Verifying the first S8730 Server configuration 571
Configuring the Processor Ethernet interface (on the ESS) 572
Confirming the product ID on the first S8730 Server 573
Enabling CNC, if necessary 573
Rebooting the first S8730 Server 573
Accessing the first S8730 Server 574
Initializing and busyout the first S8730 Server 574
Configuring the ESS and the LSP for compatibility with S8730 574
Performing an integrity check on the first S8730 Server 575
Making the first S8730 Server active 577

Shutting down the active S8700, S8710, or S8720 Server 577
Accessing the first S8730 Server 577
Releasing the first S8730 Server 578
Verifying the first S8730 Server is active. 578
Creating a super-user login 578
Installing the license and authentication files 579
Stopping and starting the ESS servers 580
Verifying server operation 580
Verifying connectivity between the first S8730 Server and port networks, LSPs, and ESS servers 581
Removing the remaining S8700, S8710, or S8720 Server. 581
Removing the S8700, S8710, or S8720 Server from the rack 581
Removing the DAL2 card, if necessary 582
On the second S8730 Server 582
Verifying the DAL2 card 582
Installing the second S8730 Server in the rack 582
Inserting the Communication Manager software distribution CD 582
Connecting the cables to the second S8730 Servers 583
Accessing the server 585
Installing Communication Manager 586
Insert the USB flash drive in the USB port. 587
Accessing the second S8730 Server 588
Checking the software version 588
Verifying date and time 588
Copying files to the second S8730 Server (if any). 588
Installing security and service pack updates, if any 589
Stopping Communication Manager on the second S8730 Server 590
Configuring to allow restoring configuration data and translations from a server on the network 590
Verifying connectivity to the network server 591
Configuring to allow restoring configuration data and translations from the USB flash card. 591
Restoring configuration data and translations to the second S8730 Server 592
Restoring data backed up to the Compact Flash card 593
Restoring data backed up to the customer network 594
Verifying the second S8730 Server configuration. 594
Configuring the Processor Ethernet interface (on the ESS) 595
Confirming the product ID on the second S8730 Server 596
Enabling CNC, if necessary 596
Rebooting the second S8730 Server 596

Accessing the second S8730 Server 597
Performing an integrity check on the second S8730 Server 597
Connecting the duplication cables 598
Releasing the second S8730 Server 599
Verifying the second S8730 Server is in standby state 599
Setting Server A/Server 1 active for ESS, if necessary 600
Administering the node name for the IP-alias address for the duplicated ESS servers (after ESS upgrade and pre-upgrade Main) 601
Administering the node name for Server A (main server only). 602
Releasing alarm suppression (optional) 602
Logging off all administration applications 603
Disconnecting from the second S8730 Server. 603
On the active (first) S8730 Server. 603
Accessing the active server. 603
Resolving alarms 603
Enabling scheduled maintenance 604
Saving translations 604
Backing up files on the active S8730 Server. 604
Releasing alarm suppression (optional) 604
Logging off all administration applications 605
Disconnecting from the active S8730 Server 605
On the standby S8730 Server 606
Accessing the standby server 606
Resolving alarms 606
Backing up files on the standby S8730 Server 606
Releasing alarm suppression (optional) 607
Logging off all administration applications 607
Disconnecting from the standby server 607
Completing the migration 607
Registering the system 607
Removing customer files from the Services laptop 607
Interchanging servers (optional) 608
Accessing the standby server 608
Interchanging servers (optional) 608
Performing an integrity check on the active S8730 Server 608

Appendix A: Accessing the server 611
Connecting to the server directly 611
Connecting the G700 Media Gateway directly 616
Computer specifications 617

Network configuration 617
Connecting to the server remotely over the network 618
Connecting to the server remotely over a modem 618
Setting up a dial-up connection 618
Dialing up to the server 619
Finding the IP address of the active server (duplicated servers) 619
Accessing the System Management Interface (SMI) 619
Using the command line interface 620
Accessing the server command line interface with ssh protocol 620
Accessing the command line interface with terminal emulation 622
Logins 622
Network configuration 623
Browser settings 624
Connecting directly to the server 624
Connecting remotely through the network 624

Index 627

Chapter 1: Introduction

This document describes procedures for migrations of Avaya telecommunication products that use Communication Manager.

A *migration* is a change in hardware. The types of migration include a:

- non-Linux-based system to a Linux-based server
- Linux-based server to a different Linux-based server
- media gateway to a different media gateway

An upgrade usually accompanies a migration.

Important:

S8300A Server cannot be upgraded to Communication Manager 5.0 or later releases. For Communication Manager 5.0 and later releases, an S8300A Server must migrate to an S8300C/D Server.

S8500A Servers cannot be upgraded to Communication Manager 5.0 or later releases. For Communication Manager 5.0 and later releases, an S8500A Server must migrate to an S8500C, S8510 or S8730 Server.

S8700 Servers cannot be upgraded to Communication Manager 5.0 or later releases. For Communication Manager 5.0 and later releases, an S8700 Server must migrate to an S8730 Server.

For more information on how to migrate the S8700 Server, see:

- Migrating from an S8700, S8710 or S8720 to an S8730 Server on page 525.

The most common migrations are from non-Linux-based systems to Linux-based servers. Non-Linux-based systems include systems such as the DEFINITY ONE/S8100. Less common migrations include migrations from one Linux-based server to another. Not all non-Linux-based systems can migrate to a Linux-based server. Whether you can migrate a system depends on the supported migration path. A *migration path* refers to the platform and the software release from which you can migrate to the new platform.

Important:

To migrate a system, you need a new license file. You cannot migrate a license file as part of a hardware migration. You must use Remote Feature Activation (RFA) to generate a brand new license.

Note:

For Release 5.2 of Communication Manager, Internet Explorer 6 and 7 are supported for use with the System Management Interface (SMI) and with Avaya Installation Wizard (AIW).

For Pre-Release 5.2 use the Maintenance Web Interface, and for Release 5.2 use the System Management Interface (SMI).

The term *IA770 INTUITY AUDIX* messaging application refers to Pre-Release 5.2 and the term *Communication Manager Messaging* (CMM) refers to Release 5.2 or later.

- For information on *upgrades* and upgrade paths, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, (03-602885).
- For information on *conversions*, see *Converting Avaya Servers and Media Gateways*, (03-602884).

Port network connectivity

Port networks are connected to each other either by an IP connection or a fiber connection.

IP connections use CAT-5 (category 5) or better Ethernet cables to connect port networks to an IP network for the transmission of bearer (voice) traffic. Both the control traffic and the bearer traffic are provided over the IP network.

Fiber-PNC connections are sometimes called *multiconnect* connections. These connections use fiber-optic cables to connect port networks for the transmission of bearer traffic. The three types of fiber connections are direct connect, center stage switch (CSS), and asynchronous transfer mode (ATM).

Direct connect is a special case of fiber connection in which fiber-optic cables connect two or three port networks without the use of a CSS or an ATM switch.

A configuration can include Internet Protocol port network connectivity (IP-PNC) and fiber port network connectivity (fiber-PNC) port networks. Migrations and conversions can often result in this combination of port network connectivity.

Reliability and availability

The reliability of a telecommunications system is defined by the extent of duplication of certain components. The traditional *standard*, *high*, and *critical* reliability levels apply to the pre-Linux-based switches. For Linux-based servers, the standard reliability level includes *single server* for S8500-Series Server and *duplicated server* for S8700-Series Server.

The availability of a telecommunications system is the time the system is ready and able to process calls as a percentage of the scheduled time. Availability depends on reliability.

The standard feature provides the ability to combine types of port network connectivity (PNC) and to apply reliability designations separately to the IP-PNC portion and the fiber-PNC portion of the system. The reliability level is defined *per port network* for the IP-PNC portion and collectively for the fiber-PNC portion. Therefore, combined PNC systems can have combined reliabilities. For pure IP-PNC configurations, the reliability designation is also per port network.

The standard feature also provides the ability to add, to an IP-PNC port network, duplicated bearer reliability, in addition to duplicated control reliability, which together constitute critical reliability.

Note:

Duplicated bearer can be implemented without duplicated control for both the SS8500-Series Server and S8700-Series Server. Unlike Release 3.0 and earlier releases, duplicated control is not a prerequisite for duplicated bearer.

Table 1: Reliability levels (per system) for Linux-based systems on page 34 and Table 2: Reliability levels (per PN) for Release 3.1 Linux-based systems on page 34 summarize reliability levels for systems with Linux-based servers. Reliability definitions for pre-Linux-based CSI switch are unchanged.

Note:

The terms *control* and *bearer* mean *control network* and *bearer network*, respectively. More detailed definitions of reliability levels, including the circuit packs involved, are given in the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207.

Table 1: Reliability levels (*per system*) for Linux-based systems

	Single Server	Duplicated Server	High	Critical
S8500-Series Server (pre-3.0 releases)	• one server • single control • single bearer	NA	NA	NA
S8700-Series Server fiber-PNC (all releases)	NA	• two servers • single control • single bearer	• two servers • duplicated control • single bearer	• two servers • duplicated control • duplicated bearer
S8700-Series Server IP-PNC (pre-3.1 releases)	NA	• two servers • single control • single bearer	• two servers • duplicated control • single bearer	NA

Table 2: Reliability levels (*per PN*) for Release 3.1 Linux-based systems

	Duplicated Server	High	Critical
S8700-Series Server IP-PNC (Release 3.1 and later)	• two servers • single control • single bearer	• two servers • duplicated control • single bearer	• two servers • duplicated control • duplicated bearer

For more information on conversions, see *Converting Avaya Servers and Media Gateways*, (03-602884).

Resources

To help with the procedures in this book, you might need to refer to the following books. These documents are also included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

✓	Document	Description
	Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers (03-602885).	Procedures to upgrade a newer release of software on a server or a newer version of firmware on a hardware component. Components include media gateways, media modules, Ethernet switches, and programmable circuit packs.
	Converting Avaya Servers and Media Gateways (03-602884).	Procedures on change in function or mode, reliability, or connectivity of various hardware components. Components include servers and media gateways. A conversion may be preceded by a migration and may include an upgrade.
	Installing and Upgrading the Avaya S8300 Server (555-234-100)	Procedures to install, upgrade, or migrate an Avaya S8300 Server.
	Installing and Upgrading the Avaya G700 Media Gateway, 03-603333.	Procedure describes the various ways of connecting to and logging into the Avaya G700 Media Gateway.
	Avaya IA 770 INTUITY AUDIX Messaging Application Release 3.1 Administering the S8300 and S8400 Media Servers to Work with IA 770, (07-600788).	Procedures to administer the Communication Manager Messaging Application (Previously termed as *IA770 INTUITY AUDIX Messaging Application*).
	Quick Start for Hardware Installation: Avaya S8400 Server in an Avaya G650 Media Gateway (03-300705).	Procedure to install the server and connect components.
	Quick Start for Hardware Migration: Avaya S8400 Server in an Avaya CMC1 or G600 Media Gateway (03-300706).	Procedure to install the server and connect components.

1 of 3

✓	Document	Description
	Installing and Configuring the Avaya S8400 Server (03-300678).	Procedures to install Communication Manager and configure the server and the TN8412AP System Internet Protocol Interface circuit pack.
	Quick Start for Hardware Installation: Avaya S8500-Series Server (555-245-701).	Procedures to install the server in a rack and connect components.
	*Installing and Configuring the Avaya S8500-Series Serve*r (03-300143)	Procedures to install Communication Manager and configure the server and the TN2312BP IP Server Interface circuit packs
	Installing the Avaya S8510 Server Family and Its Components (03-602918).	The Avaya S8510 Server Family and its Components use the Linux operating system and supports several Avaya software applications. It is generally used in simplex mode, but for some products it is duplicated.
	Quick Start for Hardware Installation: Avaya S8700-Series Server (555-245-703)	Procedures to install the server in a rack and connect components
	Installing and Configuring an Avaya S8700-Series Server (03-300145)	Procedures to install Communication Manager and configure the server and TN2312BP IP Server Interface (IPSI) circuit packs
	Installing the Avaya G650 Media Gateway (03-300685)	Procedures to install a G650 Media Gateway, backplane, and endpoints
	Avaya Aura™ Communication Manager Hardware Description and Reference (555-245-207)	Descriptions of all products, components, and connectivity
	Using the Avaya Enterprise Survivable Servers (ESS) (03-300428)	Information on installing and configuring ESSs and migrating a main server to an ESS.
	Administering Avaya Aura™ Communication Manager (03-300509)	End-user information on administering trunks and telephones.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Information on implementing converged data and voice communications networks.
		2 of 3

✓	Document	Description
	Avaya Application Solutions: IP Telephony Deployment Guide (555-245-600)	Guidelines for planning converged data and voice communications networks.
	Job Aid: Approved Grounds (555-245-772)	Description of all approved grounds.
	Job Aid: Connector and Cable Diagrams (Pinout Charts) (555-245-773)	Diagrams for various components.
	Job Aid: Option Switch Settings (555-245-774)	Settings for various components.
	Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300431)	How to use command interfaces, command syntax, and output from maintenance-related commands.
	Maintenance Alarms for Avaya Aura™ Communication Manager (03-300430)	How to use alarms, error codes, and tests to diagnose and repair problems.
	Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300432)	How to troubleshoot and replace various components.
		3 of 3

How this book is designed and organized

To use this book, you can print:

- A chapter that includes all the modules contained in that chapter
- A module, which is designed to stand alone

Many modules have tasks that you must complete before you go on site. These prerequisite steps are listed in the chapter that precedes the module or in the module itself. Some modules might have tasks that you need to do after you complete the tasks in that module. These postrequisites might point to another module or other documentation.

The following table provides links to the sections, the chapters, and the modules that this book contains:

Section, chapter, or module	Description
Introduction on page 31	
Chapter 2: Migrating to an Avaya S8400 Server on page 53	Introduces the modules associated with migrating to the S8400 Server.
Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Linear flash) on page 57	Presents the tasks required to migrate a DEFINITY Server CSI in a CMC1 Media Gateway or G600 Media Gateway with a linear flash to an S8400 Server that uses a card reader.
Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (ATA flash card) on page 125	Presents the tasks required to migrate a DEFINITY Server CSI in a CMC1 Media Gateway or G600 Media Gateway with an ATA flash to an S8400 Server.
Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Xmodem) on page 157	Presents the tasks required to migrate a DEFINITY Server CSI in a CMC1 Media Gateway to an S8400 Server that uses Xmodem.
Migrating from an IP600 or S8100 to an S8400 Server on page 91	Presents the tasks required to migrate an S8100 to an S8400 Server using ftp.
Chapter 3: Migrating to an Avaya S8500C and S8510 Server on page 153	Introduces the modules associated with migrating to the S8510 Server.
Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8500-Series Server on page 189	Presents the tasks required to migrate a DEFINITY Server CSI to an S8510 Server.
Migrating a DEFINITY ONE/S8100 to an S8500-Series Server on page 217	Presents the tasks required to migrate a DEFINITY ONE/S8100 in a CMC1 Media Gateway to an S8500-Series Server.
Migrating an Avaya IP600/S8100 to an S8500-Series Server on page 247	Presents the tasks required to migrate an IP600/S8100 in a G600 to an S8500-Series Server.
	1 of 2

Section, chapter, or module	Description
Migrating an Avaya S8500A or S8500B Server to an S8500C or S8510 Server on page 281	Procedures to migrate an existing S8500 Server running Release 2.x, 3.x, 4.x, 5.0 or 5.1 of Communication Manager to an S8510 Server running Release 5.2 or later.
Migrating an Avaya S8400 Server to an S8500-Series Server on page 309	Presents the tasks required to migrate from an existing Avaya S8400 Server to the Avaya S8500-Series Server.
Chapter 4: Migrating to an Avaya S8730 Server on page 339	Introduces the modules associated with migrating to the S8700-Series Server.
Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8730 Server with IP-PNC on page 343	Presents the tasks required to migrate a DEFINITY Server CSI in a CMC1 Media Gateway to an S8700-Series Server in an IP-PNC configuration.
Migrating a DEFINITY ONE/S8100 to an S8730 Server with IP-PNC on page 377	Presents the tasks required to migrate a DEFINITY ONE/S8100 in a CMC1 Media Gateway to an S8700-Series Server in an IP-PNC configuration.
Migrating an Avaya IP600/S8100 to an S8730 Server with IP-PNC on page 409	Presents the tasks required to migrate an IP600/S8100 in a G600 to an S8700-Series Server in an IP-PNC configuration.
Migrating an Avaya S8400 Server to an S8730 Server on page 443	Presents the tasks required to migrate from an existing Avaya S8400 Server to the Avaya S8700-Series Server.
Migrating an S8500-Series Server to an S8730 Server on page 471	Presents the tasks required to migrate an existing S8500-Series Server to an S8730 Server configuration.
Migrating from an S8700, S8710 or S8720 to an S8730 Server on page 525	Presents the tasks required to migrate from an S8700, S8710, or an S8720 Server to an S8730 Server.
	2 of 2

Migrating LSPs and ESS servers

The server type that can be used as an LSP or an ESS depends upon on the server type of the Main. Use Table 3 as a reference for compatible server types.

Table 3: LSP or ESS server types for Release 5.2

	LSP or ESS server						
Main Server	**S8300B**	**S8300 C/D**	**S8400 A[1]/B**	**S8510/ S8500 (B,C)**	**S8720**	**S8720 XL**	**S8730**
S8300B	LSP	N/A	N/A	N/A	N/A	N/A	N/A
S8300C/D	N/A	LSP	N/A	N/A	N/A	N/A	N/A
S8400	LSP	LSP	N/A	N/A	N/A	N/A	N/A
S8500(B,C)	LSP	LSP	ESS	LSP or ESS	N/A	N/A	N/A
S8510	LSP	LSP	ESS	LSP or ESS	N/A	N/A	N/A
S8710	LSP	LSP	ESS	LSP or ESS	ESS	N/A	N/A
S8720	LSP	LSP	ESS	LSP or ESS	ESS	N/A	N/A
S8720 XL	N/A	LSP	ESS	LSP or ESS	N/A	ESS	ESS
S8730	N/A	LSP	ESS	LSP or ESS	N/A	ESS	ESS

1. If you are using an S8400A server as an ESS, you must install a Memory Upgrade Kit (Material Code 218452).

S8400 Server

Use these procedures to migrate from existing DEFINITY systems to the Avaya S8400 Server. The cabinets can be reused as a port network (PN). You do not need a G650 Media Gateway.

You can migrate the following existing systems:

- DEFINITY Server CSI in a Compact Modular Cabinet (CMC)
- DEFINITY ONE in a CMC1 Media Gateway
- Avaya IP600/S8100 in a G600

Hardware migrations

The information in this section is based on the assumption that the processor of the Definity system is replaced during the migration.

DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway

When migrating an existing DEFINITY Server CSI or DEFINITY ONE in a CMC1 Media Gateway, you use the TN8400BP S8400 Server circuit pack to control the PN. You replace the processor circuit pack with the TN8400BP Media Server and TN8412AP S8400 Server IP Interface (SIPI) circuit packs in the cabinet in the A position. Install the TN8400BP Media Server circuit pack in slot 1 and the TN8412AP Server IP Interface (SIPI) circuit pack in slot 2.

This migration affects service because you must turn off the CSI or DEFINITY ONE chassis to replace the processor. Before you turn off the chassis, you must perform some premigration administration.

Avaya IP600 in a G600

When migrating an existing Avaya IP600, you use the TN8400BP S8400 Media Server circuit pack to control the PN. You replace the processor circuit pack with the TN8400BP Media Server and TN8412AP Server IP Interface (SIPI) circuit packs in the cabinet in the A position. Install the

TN8400BP Media Server circuit pack in slot 1 and the TN8412AP Server IP Interface (SIPI) circuit pack in slot 2.

This migration affects service because you must turn off the IP600 chassis to replace the processor. Before you turn off the chassis, you must perform some premigration administration.

S8500-Series Server

Use these procedures to migrate from existing DEFINITY systems to the Avaya S8510 Server with limited out-of-service time. The existing systems must be standard reliability and direct connect. You cannot migrate systems that use a center stage switch (CSS) or asynchronous transfer mode (ATM). In all instances, the cabinets can be reused as port networks (PNs). You do not need a G650 Media Gateway. However, you can add a G650 Media Gateway PN if the existing system has only one or two port networks.

You can migrate the following existing systems:

- DEFINITY Server SI in a single carrier cabinet (SCC) or multicarrier cabinet (MCC). You can migrate only the Direct-Connect configurations
- DEFINITY Server CSI in a compact modular cabinet (CMC). You can migrate only the IP-PNC configurations
- DEFINITY ONE in a CMC1 Media Gateway. You can migrate only the IP-PNC configurations
- Avaya IP600/S8100 in a G600. You can migrate only the IP-PNC configurations

Hardware migrations

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

DEFINITY Server SI in an MCC

When you migrate an existing DEFINITY Server SI in a multicarrier cabinet (MCC), you use one TN2312BP IPSI circuit pack to control from one to three port networks (PNs). Avaya recommends that you install the IPSI in the A carrier in the existing processor port network (PPN) instead of in one of the expansion port networks (EPNs). But before you install the IPSI, you must convert the PPN to a PN. This process requires that you:

- Replace the processor control carrier with an expansion control carrier.
- Remove all the control circuit packs.

This migration affects service because you must be turn off the carrier. Before you turn off the cabinet, you must perform some premigration administration.

DEFINITY Server SI in an SCC

When you migrate an existing DEFINITY Server SI in a single carrier cabinet (SCC), you use one TN2312BP IPSI circuit pack to control from one to three PNs. Avaya recommends that you install the IPSI in the cabinet in the A position in the existing PPN instead of in one of the EPNs. But before installing the IPSI, you must convert the PPN to a PN. This process requires that you:

- Replace the processor control cabinet with an expansion control cabinet.
- Remove all the control circuit packs.

This migration affects service because you must turn off the PPN stack to replace the cabinet. Before turning off the cabinets, you must perform some premigration administration.

DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway

When you migrate an existing DEFINITY Server CSI or DEFINITY ONE in a compact modular cabinet (CMC), you use one TN2312BP IPSI circuit pack to control the PN. If a CSI, you replace the TN2182 Tone Clock circuit pack with the IPSI which you install in the A position of the cabinet. You also must remove the processor circuit pack. If a DEFINITY ONE, you replace the processor circuit pack with the IPSI.

This migration affects service because you must turn off the CMC1 Media Gateways to replace the processor and the tone clock circuit packs. Before you turn off the cabinets, you must perform some premigration administration.

Avaya IP600/S8100 in a G600

When you migrate an existing Avaya IP600, you use one TN2312BP IPSI circuit pack to control the PN. You also must replace the processor circuit pack with the IPSI which you can install in the A position of the cabinet.

This migration affects service because you must turn off the IP600 chassis to replace the processor. Before you turn off the chassis, you must perform some premigration administration.

S8700-Series Server

Use these procedures to migrate from existing DEFINITY and Linux platforms to the Avaya S8730 Server configuration with limited out-of-service time. The S8730 Server can be either a fiber-port network connectivity (PNC) configuration or an IP-PNC configuration or both.

Note:

Once you complete the migration to fiber-PNC, you can convert to IP-PNC.

You can migrate the following existing systems to an S8730 Server:

- DEFINITY Server R in a multicarrier cabinet (MCC)
- DEFINITY Server SI in a single carrier cabinet (SCC) or a multicarrier cabinet (MCC)
- Avaya IP600 (S8100) in a G600 Media Gateway
- DEFINITY ONE (S8100) in a compact modular cabinet (CMC)
- DEFINITY Server CSI in a CMC1 Media Gateway

You can migrate the following existing Linux systems to an S8730 Server:

- S8400
- S8500
- S8700
- S8710

- S8720, S8720XL

Hardware migrations

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

DEFINITY Server SI in an MCC

When you migrate an existing DEFINITY Server SI in a multicarrier cabinet (MCC), you use one TN2312BP IPSI circuit pack to control from one to three port networks (PNs). Avaya recommends that you install the IPSI in the A carrier in the existing processor port network (PPN) instead of in one of the expansion port networks (EPNs). But before installing the IPSI, you must convert the PPN to a PN. This process requires that you:

- Replace the processor control carrier with an expansion control carrier.
- Remove all the control circuit packs.

This migration affects service because you must turn off the PPN to replace the carrier. Before you turn off the cabinet, you must perform some premigration administration.

DEFINITY Server SI in an SCC

When you migrate an existing DEFINITY Server SI in an single carrier cabinet (SCC), you use one TN2312BP IPSI circuit pack to control from one to three PNs. Avaya recommends that you install the IPSI in the cabinet in the A position in the existing PPN instead of in one of the EPNs. But before installing the IPSI, you must convert the PPN to a PN. This process requires that you:

- Replace the processor control cabinet with an expansion control cabinet.
- Remove all the control circuit packs.

This migration affects service because you must turn off the PPN stack to replace the cabinet. Before you turn off the cabinets, you must perform some premigration administration.

DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway

You can only migrate a DEFINITY Server CSI or a DEFINITY ONE/S8100 in a compact modular cabinet (CMC) to an Avaya S8700-Series with an IP-PNC configuration.

When you migrate an existing DEFINITY Server CSI or a DEFINITY ONE in a CMC1 Media Gateway, you use one TN2312BP IPSI circuit pack to control the PN. If a CSI, you replace the TN2182 Tone Clock circuit pack with the IPSI which you install in the A position of the cabinet. You also must remove the processor circuit pack. If a DEFINITY ONE, you replace the processor circuit pack with the IPSI.

This migration affects service because, if a CSI, you must turn off the CMC1 Media Gateways to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform some premigration administration.

Avaya IP600/S8100 in a G600

You can only migrate an Avaya IP600 to an Avaya S8730 Server with an IP-PNC configuration.

When you migrate an existing Avaya IP600, you use one TN2312BP IPSI circuit pack to control the PN. You replace the processor circuit pack with the IPSI in the cabinet in the A position.

This migration affects service because you must turn off the IP600 chassis to replace the processor. Before you turn off the chassis, you must perform some premigration administration.

License and Avaya authentication files

Use Remote Feature Activation (RFA) to obtain the Communication Manager license and authentication file. RFA is a Web-based application that is available to Avaya employees and authorized Business Partners. WIth RFA, you can create and deploy license files for all

Communication Manager product platforms. For more information about RFA and how to generate license and Avaya authentication files, see the RFA Information page at http://rfa.avaya.com.

Generating and retrieving license and authentication files

To generate a license file, you need the following information:

- Your personal single sign-on (SSO) for the RFA Web site authentication login
- The SAP order number
- Required customer information
- For a new license, the serial number of the TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that is designated as the reference IPSI
- For an updated license, the RFA system ID (SID) for the existing server
- Internet access to the RFA Web page with Internet Explorer 5.0 or higher

Before you arrive on site, download the license and the authentication file to the Services laptop. You install these files as part of the installation process.

Logins and passwords

Once you install the authentication file, a challenge/response system called Access Security Gateway (ASG) protects Avaya services logins to the server. The ASG challenge/response protocol confirms the validity of each user, and this reduces the opportunity for unauthorized access.

When you finish installing the authentication file, Communication Manager has a password for the craft login. This password is unique to the server of the customer. You can use the password the next time that you log in as craft, if you access the server through the Services port. Every other means of craft access still requires an ASG challenge/response. RFA records the revised password. ASG Interactive Response provides this password at 1-800-248-1234 or 1-720-444-5557.

Caution about platform/PNC license settings for the S8700-series Server

The license settings for port network connectivity (PNC) — IP-PNC or fiber- PNC (previously referred to as "multiconnect" [MC]) — can be complex and can cause problems if not set correctly. When creating a license for an S8700-series Server, use the following summary

(Table 4: Summary for license settings for the S8700-series platform and PNC on page 49) and guidelines:

Table 4: Summary for license settings for the S8700-series platform and PNC

License file attribute		Result in Communication Manager		
Platform Type	**Internet Protocol (IP) PNC (FEAT_IP_PNC) feature**	**Platform Number in Customer Options screen**	**Internet Protocol (IP) PNC feature in Customer Options screen**	**Allowed configuration**
8700 Server MC[1]	OFF[2]	6[1]	no	IP-PNC and fiber-connect PNs simultaneously SCC1 or MCC1 are allowed in configuration using IP-PNC.
8700 Server IP[3]	OFF[2]	8[3]	no	Same as above.

1. Use for all new installations and migrations. Required for upgrades of an S8700-series Server that was a fiber-PNC or MC (platform 6) configuration before the upgrade.
2. This attribute, before release 3.0, restricted the ability to configure a network with both IP-PNC and fiber-PNC port networks and to configure SCC1 and MCC1 PNs using IP-PNC only. For all upgrades, migrations, and installations to release 3.0 and later, these restrictions have been lifted for both platforms. Thus, this field is no longer applicable and should be set as OFF.
3. Required, and used only, for upgrades of an S8700-series Server that was an IPC (platform 8) configuration before the upgrade.

Guidelines

- For a new installation or migration, the licensed platform type should always be 8700 Server MC (platform **6**).
- For an upgrade, the licensed platform type of the server must remain the same. If the platform type is 8700 Server IP (platform 8) before the upgrade, the platform type must be 8700 Server IP (platform 8) after the upgrade. If the platform type is 8700 Server MC (platform 6) before the upgrade, the type must be 8700 Server MC (platform 6) after the upgrade.
- Effective with Communication Manager 3.0, Internet Protocol (IP) PNC (FEAT_IP_PNC in the RFA license file) is always to set to **OFF**. Effective with Communication Manager 4.0, the field **Internet Protocol (IP) PNC** is not displayed on the **system-parameter customer-options** screen.

Note:

The Internet Protocol (IP) PNC (FEAT_IP_PNC license attribute, **before** release 3.0, restricted port network connectivity (PNC) for each of the platforms. The **OFF** setting previously restricted MC (platform 6) platforms from using IP-PNC. The **ON** setting previously restricted IP (platform 8) platforms from using MC-PNC configurations. With release 3.0, both of these restrictions were lifted.

Server Migration Paths

Server Migration Paths for Communication Manager Release 5.2

In the following table, ✔ indicates a migration path is supported with pricing, documentation, and translation tool support. ✘ indicates there is no supported migration path but circuit pack reuse and manual translation may be supported.

The supported migration paths for Release 5.2 of Communication Manager is contained in the following table:

To →	S8300C/D	S8400B	S8500C	S8510	S8730		
From ↓					**Duplex**	**High**	**Critical**
CSI w/CMC (note 1)	✘	✔	✔	✔	✔ (note 2)	✔ (note 2,4)	✘
S8100 w/ CMC (note 1)	✘	✔	✔	✔	✔ (note 2)	✘	✘
S8100 w/ G600 (note 1)	✘	✔	✔	✔	✔ (note 2)	✘	✘
SI Simplex	✘	✘	✔ (note 3,4)	✔ (note 3,4)	✔ (note 4)	✔ (note 4)	✔ (note 4)
SI Duplex	✘	✘	✘	✘	✔ (note 4)	✔ (note 4)	✔ (note 4)
R Simplex/ Duplex	✘	✘	✘	✘	✔	✔	✔
S8300A/B/ C	✔	✘	✘	✘	✘	✘	✘
S8400A	✘	✔	✔	✔	✔ (note 2)	✘	✘
S8500A/B/ C	✘	✘	✔ (note 5)	✔	✔	✔ (note 4)	✔ (note 4)
S8510	✘	✘	✘	✘	✔	✔ (note 4)	✔ (note 4)
S8700 (IPC/MC)	✘	✘	✘	✘	✔	✔	✔
S8710 (IPC/MC)	✘	✘	✘	✘	✔	✔	✔
S8720 (IPC/MC)	✘	✘	✘	✘	✔	✔	✔

1. Media Gateway does not support duplicate TN2312BP IP Server Interface (IPSI)
2. Merges (system becomes a port network in a larger system) only
3. Direct connect only
4. Must use G650 Media Gateway (move packs from other Media Gateway type)
5. Except S8500C

Legend:

✔ - migration path supported, pricing, documentation and translation tool support

✘ - no migration path supported (does not preclude circuit pack reuse and manual translation)

Chapter 2: Migrating to an Avaya S8400 Server

This chapter describes how to migrate from existing DEFINITY systems to the Avaya S8400 Server.

The most common migrations are from non-Linux-based systems to Linux-based servers. Non-Linux-based systems include systems such as the DEFINITY ONE/S8100. Less common migrations include migrations from one Linux-based server to another. Not all non-Linux-based systems can migrate to a Linux-based server. Whether you can migrate a system depends on the supported migration path. A *migration path* refers to the platform and the software release from which you can migrate to the new platform.

Note:

The S8400 platform supports Communication Manager Messaging (CMM) in addition to Communication Manager.

Migration paths for S8400 Servers

An S8400 Server that is running Communication Manager Release 3.1 software can support a configuration that has one or more LSPs. The LSPs must be running Communication Manager Release 3.1. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway with a Linear Flash

To migrate from a DEFINITY Server CSI in a CMC1 Media Gateway with a Linear Flash to an S8400 Server:

1. Copy the translations to the linear flash card in the PCMCIA slot on the TN798B Processor circuit pack.
2. Plug the PCMCIA flash card with the translations into the flash card reader attached to the Services laptop.
3. Copy the translations to the S8400 Server.

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway using Xmodem

To migrate from a DEFINITY Server CSI in a CMC1 Media Gateway to an S8400 Server using Xmodem:

1. Copy the translations to the Compact Flash card in the PCMCIA slot on the TN798B Processor circuit pack.
2. Copy the translations onto the Services laptop.
3. Copy the translations to the S8400 Server.

Migrating from an S8100 using ftp

To migrate from an S8100 to an S8400 Server using ftp:

1. On the SAT, copy the translation files.
2. Move the translations onto the Services laptop.
3. Copy the translations to the S8400 Server.

Migrating all other systems

When you migrate to an S8400, you can use the existing translations. The only supported method to move translations from legacy systems is to:

1. Copy the translations to the Compact Flash.
2. Copy the translation files from the Compact Flash to the S8400 Server.

Migrations from existing DEFINITY and Linux platforms

Use these procedures to migrate from existing DEFINITY systems to the Avaya S8400 Server. The cabinets can be reused as a port network (PN). You do not need a G650 Media Gateway.

You can migrate the following existing systems:

- DEFINITY Server CSI in a Compact Modular Cabinet (CMC)
- DEFINITY ONE in a CMC1 Media Gateway
- Avaya IP600/S8100 in a G600

Hardware migrations

The information in this section is based on the assumption that the processor of the Definity system is replaced during the migration.

DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway

When migrating an existing DEFINITY Server CSI or DEFINITY ONE in a CMC1 Media Gateway, you use the TN8400BP S8400 Server circuit pack to control the PN. You replace the processor circuit pack with the TN8400BP Media Server and TN8412AP S8400 Server IP Interface (SIPI) circuit packs in the cabinet in the A position. Install the TN8400BP Media Server circuit pack in slot 1 and the TN8412AP Server IP Interface (SIPI) circuit pack in slot 2.

This migration affects service because you must turn off the CSI or DEFINITY ONE chassis to replace the processor. Before you turn off the chassis, you must perform some premigration administration.

Migration modules

This chapter describes the following types of migrations:

- Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Linear flash) on page 57
- Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (ATA flash card) on page 125
- Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Xmodem) on page 157
- Migrating from an IP600 or S8100 to an S8400 Server on page 91.

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Linear flash)

Use these procedures to migrate from an existing DEFINITY Server CSI in a Compact Modular Cabinet (CMC) system or G600 Media Gateway with a linear flash to an Avaya S8400 Server that uses a card reader. This procedure supports a migration to Communication Manager Release 5.x.

To migrate an existing DEFINITY Server CSI in a CMC1 Media Gateway, you use one TN8412AP S8400 IP Interface (SIPI) circuit pack to control the one port network. You must replace the TN2182 Tone Clock circuit pack with a TN8412AP Server IP Interface (SIPI) circuit pack that you install in the A position in the cabinet. You also must remove the processor circuit pack.

This migration affects service because you must turn off the CSI chassis to replace the processor and tone-clock circuit packs.

Migration paths

Avaya supports the following migrations of a DEFINITY Server CSI in a CMC1 Media Gateway or a G600 Media Gateway to the S8400 Server configuration:

- DEFINITY Release 6 through Release 8

To migrate, you can use the existing translations. The only supported method to move translations from legacy systems is to:

1. Copy the translations to the PCMCIA slot on the TN798B Processor circuit pack.
2. Plug the PCMCIA card with the translations to the Services laptop.
3. Copy the translations to the S8400 Server.

Installing the linear card reader software

You need to install the software for the linear card reader so that you can copy the translations to the Services laptop. This installation is a one-time installation.

To install the linear card reader:

1. Insert the CD-ROM into the Services laptop.
2. Under Professional Line, click **USB Professional**.
3. In the PC Card Manager area, click **PCM Setup**. Do not select **Setup** at the bottom.
4. Select the setup language, for example, English and click **OK**.
5. Accept the license and follow the prompts.
6. When you finish, click **Finish**.

   Access to PC Card Manager is by either:

   a. The shortcut created on your desktop
   b. Through **Start** > **Programs** > **PCM**.
7. Click **Exit** and remove the CD-ROM.

Checklists

Before you go on site, perform the following tasks

:

✓	Task	Description
	Verify that your Services laptop has the appropriate hardware.	Correct hardware components include: ● 40 MB available disk space ● direct Ethernet cable ● serial cable and adapter ● RS-232 port connector ● Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● CD-ROM drive
	Verify that your Services laptop has the appropriate software.	Correct software components include: ● Windows 2000/XP operating system ● Terminal emulation program: HyperTerminal or other ● TCP/IP networking software: bundled with Windows OS ● Web browser: Internet Explorer 5.0 or later
	Obtain appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media Gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the equipment of the customer.
	Obtain the serial number of the Servers, if necessary.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file.
	Verify that you have the Communication Manager software distribution CD with the current software and firmware.	You use this CD to install the software on the server and upgrade the firmware.
		1 of 2

✓	Task	Description
	Verify that you have the current preupgrade or premigration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware available.	The following firmware are on the software CD: • IPSI or TN8412AP Server IP Interfaces (SIPI) • C-LAN • MedPro • VAL circuit packs For the most current versions, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download license and authentication files to your Services laptop.	New license and authentication files are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557 and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed as well as any changes to the system alarming configuration. ART is available only to Avaya associates. Business Partners can call 800-295-0099.
	Verify that you have copied all necessary files to your computer	These files can include: • service packs • license file • authentication file • firmware for programmable circuit packs

2 of 2

Premigration setup checklist

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

For more information, see Migration paths on page 57.

To migrate from a DEFINITY system, you must complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. Remote or on-site ASG access is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Presite migration checklist

Before you go on site, perform the following tasks in Table 5:

Table 5: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks before you start the migration:

✓	Task	Description
	Verify that you have the correct cables for the TN8412AP S8400 Internet Protocol Interface (SIPI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see *Installing and Configuring the Avaya S8400 Media Server* (03-300678).

When you are migrating from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Documentation checklist for migrations

For a list of documents that are needed to perform the migration, see Resources on page 35.

✓	Document	Description
	Quick Start for Hardware Migration: Avaya S8400 Server in an Avaya CMC1 or G600 Media Gateway (03-300706)	A quick reference guide that provides physical installation and connection information.
	Installing and Configuring the Avaya S8400 Server (03-300678)	Provides installation instructions for the S8400 Server.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.

Performing a migration

CAUTION:

This migration affects service. When the Definity One/S8100 is turned off, the system drops all calls. Service returns when the server takes control of the IPSIs.

Note:

You must install the new Communication Manager license file on the server before you make the change. The TN8412AP Server IP Interface (SIPI) serial number can be used for licensing purposes.

Premigration administration

This migration is a service-affecting event. The CMCs must be turned off to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

Accessing Remote Feature Activation

Use this section for information on how to access Remote Feature Activation (RFA).

You can access the RFA information page for these items (if not already installed on your PC):

Note:

For Release 10 and later, do not use the FET because the license contains the existing switch configuration information. For Releases G3v4 and earlier, do not use the FET because the ASD tool and process captures the existing switch configuration information.

- Feature Extraction Tool (FET) application. Use FET only for G3v4 through Release 9csi releases that upgrade to Communication Manager. Integrated FET also is available within the RFA application.
- License Installation Tool (LIT) application. Use LIT to install a Communication Manager license on any Release 10 or later DEFINITY Server CSI.

Computer requirements

Before you attempt to access RFA, verify that your computer has:

- Internet Explorer 5.0 or later
- 128-bit encryption
- Internal access to the RFA web site at http://rfa.avaya.com
- A supported monitor resolution of 800 x 600

User requirements

An RFA user must meet the following requirements:

- Be either an:
  - An Avaya associate or contractor with a valid Avaya Human Resources Identification (HR ID) number.

- An approved BusinessPartner with a valid BusinessPartner number.
- An Avaya contractor who works with Avaya.

- Be a registered and authenticated RFA user.
  - To be registered in RFA means you have a Single Sign-On (SSO) login and you have registered for each product family in which you want to create a license file. If you do not already have an SSO login, see *Avaya Remote Feature Activation (RFA) User Guide*, 03-300149. If you are an Avaya employee, you do not have to register. You can use your Windows NT login name and password to log on.
  - To be authenticated in RFA means you have successfully registered, and your Avaya coach or Group Authorization Identification (GAI) manager approved your access to RFA.
- For more information, see *Avaya Remote Feature Activation (RFA) User Guide*, 03-300149.

Going to the Remote Feature Activation web site

The RFA web site automates some of the upgrade procedures, including generating a license file.

1. At the Services laptop/PC browser, type http://rfa.avaya.com
2. Using your SSO, log in to the RFA web site.
3. Follow the links to the RFA information page.
4. Complete the information necessary to create a license file.

If you have a direct connection to the switch:

1. Using your RFA Job Aids, run the Features Extraction Tool (FET) from the RFA web site to create a Switch Configuration file.
2. When prompted, type in the transaction ID number.
3. The FET creates and uploads automatically the Switch Configuration file.
4. Do not deliver the license file at this time. You deliver and install the license later in this upgrade procedure.

If you do not have a direct connection to the switch:

1. Run the Features Extraction Tool (FET) from the Services laptop/PC to create a Switch Configuration file.
2. When prompted, type in the transaction ID number.
3. Use the FET instructions to create a new switch connection profile.
4. Create the Switch Configuration file.
5. Upload the Switch Configuration File to the RFA web site.

Deliver the license file to the Services laptop/PC for installation late in this procedure.

Connecting to the processor

To connect to the processor:

1. Connect the computer that you use to access the cabinet.
2. Start a SAT session using Native Configuration Manager or Avaya Site Administration.
3. Log in as **craft**.

Removing netcon data modules

To remove Netcon data module information:

1. Type **`list data module`**. Press **Enter**.
2. Notice if the system contains any Netcon circuit packs.

   If there are Netcon data modules, continue to step 3.

   If there are no Netcon data modules, continue to Saving translations on page 355.
3. Type **`list user ext`** ***x***. Press **Enter** where ***x*** shows who is using the associated Netcon data module.

```
list usage extension 2501
                              LIST USAGE REPORT

    Used By
    Hunt Group           Group Number           99               Member 1



Command successfully completed
```

   For example, the screen in step 3 shows the extension 2501 is being used on Hunt Group 99.
4. Type **`change hunt-group`** ***xx***. Press **Enter** where ***xx*** is the hunt group number.
5. In the **Hunt Group** screen, press the space bar to highlight the information. Press **Return** to remove the information.

6. Repeat for each extension.
7. When you finish, press **Submit**.
8. Repeat for each listing.
9. Type **`remove data-module`** ***`xxxx`***. Press **Submit** where ***`xxxx`*** is the extension to be removed.
10. Repeat for all items listed on the **`list data module`** command.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:
   a. **`list configuration all`**
   b. **`list trunk-group`**
   c. **`list hunt-group`**

   If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:
   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.

2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

This step is important in case you need to back out of the migration.

To save translations from the CSI:

Note:
Save translations to a properly formatted flash card.

1. Plug the Linear Flash card in the PCMCIA slot on the TN798B Processor circuit pack.
2. Type **`save translation`** and press **Enter** to save translations to the PCMCIA.
3. The system displays a **Command successfully completed** message or an error message.

Migration tasks

You can reuse the translations from the current system when you migrate to an S8400 Server.

Note:

You must install the new Communication Manager license file on the server before you make the change. The TN8412AP Server IP Interface (SIPI) serial number can be used for licensing purposes.

Perform these tasks to convert a processor port network to a port network (CMC).

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

The TN8400BP Server circuit pack replaces the TN798 or TN2402 Processor circuit pack. The TN798 and TN2402 circuit packs do not have the Communication Manager Messaging feature. You must return the current processor circuit pack to Avaya.

Turning off power to all cabinets

CAUTION:

Ensure that you have done the premigration administration. For more information, see Premigration administration on page 257.

To turn off power to all cabinets:

- Turn off the power to each cabinet.

Removing circuit packs

To remove circuit packs from the CMC1 Media Gateway:

1. Remove the TN798B or TN2402 Processor circuit pack from slot A01.
2. Remove the TN2182 Tone Clock circuit pack from slot A02.
3. Remove the TN767 DS1 Interface circuit pack, if installed.
4. Remove the TN2207 DS1 Interface circuit pack, if installed.

5. Remove the TN2313 DS1 Interface circuit pack, if installed.

Inserting circuit packs

To install circuit packs into the CMC1 Media Gateway:

1. Install the TN8412AP S8400 IP Interface (SIPI) circuit pack into slot A02.
2. Install the TN8400BP Media Server circuit pack into slot A01.
3. If the system had a TN767, TN2207, or TN2313 DS1 Interface circuit pack, install the TN464HP DSD1 Interface circuit pack in any open slot.

Connecting cables

To connect cables:

1. On the rear of the carrier, connect the server cable adapter into port 1 on the rear of the TN8400BP Media Server circuit pack.
2. Connect the amphenol connector into slot A02 on the rear of the TN8412AP SIPI circuit pack.
3. Connect the customer LAN cable into the port labeled ETH-B on the adapter in slot A01.
4. Connect the IPSI cable into the port labeled ETH-A on the adapter in slot A01.
5. Connect the other end of the IPSI cable to the amphenol connector in slot A02.
6. Connect the power plug on the DVD drive to a wall outlet.
7. Connect the USB DVD drive to the USB port on the faceplate of the TN8400BP Media Server circuit pack.
8. On the DVD drive, ensure that the on/off/ext switch is in the **EXT** position.
9. Insert the Communication Manager CD into the USB DVD drive.
10. Connect the Services laptop to the Services port on the front of the TN8400BP Media Server circuit pack.
11. Turn on the power to all cabinets.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test

You can install a TN771 Maintenance/Test circuit pack in any slot other than slots A01 and A02. Avaya recommends one TN771 Maintenance/Test circuit pack per location for the following conditions:

- There are three or more G650, G600, or CMC1 Media Gateways in the S8400 system. Do not include G150 and H.248 Media Gateways in this count, and
- There are IP endpoints or ISDN endpoints. These endpoints consist of:
  - BRI trunks
  - PRI trunks
  - BRI stations

The TN8412AP S8400 IP Interface (SIPI) circuit pack provides all maintenance functions that were present on the TN798 or TN2402 Processor circuit pack. This carrier does not have a TN775 Maintenance (EPN) dedicated slot.

Translation migrations

This section describes how to migrate the translation files from the current system to the S8400 Server.

Installing the software load

For more information on installing software loads, see *Installing and Configuring the Avaya S8400 Media Server*, 03-300678.

To install the software load:

1. Power down the server.
2. Connect the USB CD/DVD drive to the S8400 Server.
3. Connect the laptop to the Services port on the faceplate of the server using a crossover cable.
4. Power up the server.
5. From the Services laptop, click **Start** > **Run** to open the **Run** window.
6. Type **`ping -t 192.11.13.6`**. Press **Enter** to indicate when the Services port is responding.
7. From the laptop Start menu, click **Start** > **Run**.
8. In the **Run** dialog box, type **`telnet 192.11.13.6`**. Press **Enter** to view the first screen.

Note:

To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

9. Select **Install**, ensure that OK is highlighted and press **Enter**.

10. On the **Select Release Version** window, ensure that the Build line and <OK> are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

    Once the drive is properly configured, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

    These processes can take up to 20 minutes. When the system finishes the software installation, the server reboots and the CD/DVD-ROM drive opens. You must remove the CD from the drive at this time.

    The reboot can take up to 3 minutes. The telnet session drops automatically.

11. Open a Web browser.
12. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
13. Log in as **craft** or **dadmin**.

Configuring the server

For more information on configuring the server and the use of the Avaya Installation Wizard, see *Installing and Configuring the Avaya S8400 Media Server*, 03-300678.

To configure the server:

1. Open a Web browser.
2. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.
4. Access **System Management Interface (SMI)** click **Administration** > **Server (Maintenance)**
5. Under Server, click **Server Date/Time**.
6. In the **Server Date/Time** window, verify the data and time are correct. If the date and time are incorrect:
   a. Enter the date
   b. Enter the time
   c. Select the time zone
   d. Click **Submit**:

   Important:
   It is necessary to reboot the server to initialize server settings that are restored but not yet activated. See Reboot the server on page 301.

   CAUTION:
   Not rebooting the server will lead to erroneous behavior surrounding the time of day at daylight-saving-time transition.
7. Under Server Configuration, click **Configure Server**.

   The system starts the Configure Server Wizard.
8. In the **Review Notices** window, click **Continue**.
9. In the **Back Up Data** window, click **Continue**.
10. Select **Configure all services using the wizard** and click **Continue**.

    Note:
    You can set up servers to various configurations. The following steps provide a general outline of required steps to complete the configuration.
11. In the **Server Role** window, as shown in Figure 1, choose between Main, ESS or LSP depending on the platform on which the wizard is running.
12. In the **Set Identities** window, perform the following steps:
    - In the **Host Name** field, enter a unique name for the server.
    - In the **ID** field, enter as required or accept the default.
    - In the **CNA** field, enter as required or accept the default.

- In the **Enterprise LAN** field, enter as required or accept the default.
- In the **Assign the Processor Ethernet to an Interface** area, select one as required.

13. Click **Continue**.
14. In the **Configure Ethernet Interfaces** window, set up as required. Click **Continue**.
15. In the **Ethernet Adjuncts** window, set up as required. Click **Continue**.
16. In the **External DNS Server Configuration** window, set up as required. Click **Continue**.
17. In the **Static Network Routes (Optional)** window, set up as required. Click **Continue**.
18. In the **Configure Time Server** window, set up as required. Click **Continue**.
19. In the **Set Modem Interface** window, set up as required. Click **Continue**.
20. In the **Configure Maintenance Processor Complex (MPC)** window, set up as required and click **Continue** to configure the server.

Figure 1: Configure Server - Server Role

Installing the license and authentication file

To install the Communication Manager license file and the Avaya authentication file:

1. Open a Web browser.
2. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.

4. Under Miscellaneous, click **Download Files**.
5. Click **Browse** and select the file saved on the Services laptop.
6. Click **Download** to place the file on the server.
7. Under Security, click **License File**.

   The system displays the **License File** screen.
8. Select **Install the license file I previously downloaded** and click **Submit**.

   The system tells you the license file is installed successfully.
9. Under Security, click **Authentication File**.

   The system displays the **Authentication File** screen.
10. Select **Install the Authentication file I previously downloaded** and click **Install**.

    The system tells you the authentication is installed successfully.

Copying translation files to the server

To copy translation files to the server:

1. Plug the PCMCIA flash card with the translations into the Flash Card Reader attached to the Services laptop.
2. On the desktop, double-click the **PC Card Manager** icon > **Actions** > **Copy** > **Card to File(s)**.

   When the system finishes, the system opens the **Copy: Card to File** window.
3. Highlight any old job and click **Delete** to remove them.
4. In the **Copy Jobs** area, click **New**.

   When the system finishes, system opens the **Define Copy Job** window.
5. In the **Size** field, type the flash card size, for example, **128 MByte**.
6. Enter a file name to copy the translation file to and click **OK**.

   An example of a file name might be **Csixln**.

   When the system finishes, the system returns to the **Copy: Card to File** window.
7. Highlight the desired file. Click **Copy**.

   When the system finishes, the file is placed in the C:\Program Files\PCM directory.

   Click **Cancel** to exit.
8. Open a Web browser to the S8400 Server.

9. Access **System Management Interface (SMI)**.
10. Under Miscellaneous, click **Download Files**.
11. Select **Files to download from the machine I'm using to connect to the server**.
12. Click **Browse** and select the translation file saved on the Services laptop and click **Download**. A translation file example might be C:\Program Files\PCM\Csixln.

    The file is placed in the /var/home/ftp/pub directory of the S8400 Server.
13. Use PuTTY to access the S8400 Server.
14. Log in as **craft** or **dadmin**.
15. From the /var/home/ftp/pub directory, run a bash program.
16. Type **`read_csi_file -f`** ***`filename`***. Press **Enter** where ***`filename`*** in this example is CsiXln.

    The system renames the translation files as xln1 and xln2.
17. Type **`cd /etc/opt/defty`**. Press **Enter**.
18. Type **`ls -ltr`**. Press **Enter**.

    Verify that the xln1 and xln2 files are not zero length.
19. Open a SAT session.
20. Type **`reset system 4`**. Press **Enter** to load the restored translations into memory.

If the read_csi_file process fails, you get an error message with the reason for the failure. If that happens, the translation file is not restored. Resolve the reason for the failure and restart the process.

Post-migration administration

This section describes the post-migration administration to complete the migration to the S8400 Server.

Important:

When you format the compact flash card for use in the S8400 Server, all data is erased from the compact flash card.

Note:

Do not use the compact flash card (Comcode 700381841) in an S8100 Windows system. The operating system does not recognize the compact flash card.

After the migration, you can format the compact flash card (Comcode 700381841) for the S8400 Server and use the compact flash card as the backup compact flash card.

Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs

When you use static IP addressing, you must assign IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs.

Using static addressing

You can administer static IP addresses for the TN8412AP Server IP Interface (SIPI) circuit packs. You administer the addresses directly through the Ethernet port connection on the TN8412AP Server IP Interface (SIPI) faceplate (top port). For more information, see Figure 2: Connecting directly to the SIPI on page 81.

Figure 2: Connecting directly to the SIPI

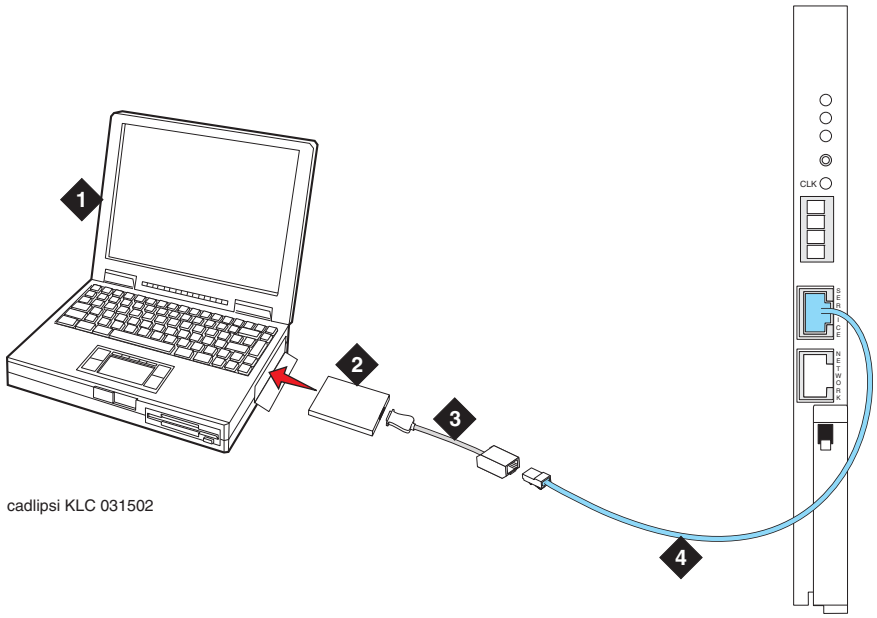


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 crossover cable to SIPI**

Note:

Ensure that you have the password before proceeding.

Logging in to the TN8412AP Server IP Interface (SIPI)

To log in to the TN8412AP Server IP Interface (SIPI):

1. Type **`telnet 192.11.13.6`**. Press **Enter** to open the Telnet window and connect to the TN8412AP Server IP Interface (SIPI)

   Prompt = [IPSI]:

Note:

While connected to the TN8412AP Server IP Interface (SIPI), type **`help`** or **`?`** to obtain online help. Most commands have two or three letter abbreviations.

2. Type **`ipsilogin`**. Press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login used on the TN8412AP Server IP Interface (SIPI) has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`**. Press **Enter**.
2. Type **`show port 1`**. Press **Enter** to see the current settings.
3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnet mask. Press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) session.

5. Telnet to **192.11.13.6** and login.
6. Enter **`show control interface`**.
   The system displays the IP address, subnet mask, and default gateway information. Verify that the proper information was entered.
7. If a default gateway is used, enter the gateway IP address with **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway.
8. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) or IPSI session.
9. Telnet to **192.11.13.6** and login.
10. Use **`show control interface`** to verify the administration.
11. Type **`exit`**. Press **Enter** to see the changes.

Resetting the TN8412AP Server IP Interface (SIPI)

To reset the TN8412AP Server IP Interface (SIPI):

1. Type **`reset`**. Press **Enter**
   Answer **`Y`** to the warning.

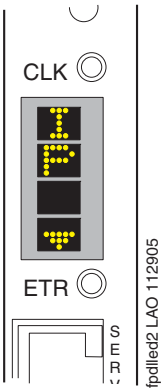
   Note:

   Resetting the TN8412AP Server IP Interface (SIPI) terminates the administration session. If further administration is required, start a new telnet session to the TN8412AP Server IP Interface (SIPI).

   Note:

   Control network settings become effective when you exit the IPADMIN session. Control settings include the IP address, the subnet mask, and the gateway.
2. Disconnect the Services laptop from the faceplate.
3. Check the LCD. Verify that it has an I P with a filled-in V that shows at the bottom. For more information, see Figure 3.

Figure 3: LED display that shows that the SIPI has a static IP address



Note:

Clear the ARP cache on the laptop before connecting to another TN8412AP Server IP Interface (SIPI). If the cache is not cleared, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

4. Close the window.

Enabling control of the TN8412AP Server IP Interface (SIPI)

To enable control of the TN8412AP Server IP Interface (SIPI):

Note:

Ensure that the TN8412P SIPI has the current firmware.

CAUTION:

This procedure allows the server to take control of the TN8412AP Server IP Interface (SIPI)-controlled port network. Failure to complete the procedure correctly can result in no connection to the network.

1. Type **`add cabinet 1`**. Press **Enter**.
2. Administer the appropriate cabinet type and carriers.
3. Type **`add ipserver-interface 1`** where **1** means port network. Press **Enter**.
4. In the **Host** field, type in the IP address that was programmed into the TN8412AP Server IP Interface (SIPI). Press **Enter**.
5. Type **`save translation`**. Press **Enter**.

6. Type **`change system ipserver-interface`**. Press **Enter**.
7. In the **IPSI Control of Port Networks** field, type **`enabled`**. Press **Enter**.
8. Type **`save translation`**. Press **Enter**.
9. Verify the translation migration was successful.

   Place test calls, verify trunk status (if applicable), and so forth.

   The server now controls all the port networks.

Verifying TN8412AP Server IP Interface (SIPI) translations

To verify TN8412AP Server IP Interface (SIPI) translations:

1. Type **`list ipserver-interface`**. Press **Enter**.
2. Verify that the TN8412AP Server IP Interface (SIPI) circuit pack(s) is translated.

Verifying TN8412AP Server IP Interface (SIPI) connectivity

To verify TN8412AP Server IP Interface (SIPI) connectivity:

1. Start a Web browser.
2. Under Diagnostics, click **Ping**.
3. Under Endpoints to Ping, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Type the correct cabinet and carrier numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway

- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.

2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each TN8412AP S8400 IP Interface (SIPI) circuit pack must be on the most current and same firmware load. You might need to upgrade the firmware on the TN8412AP Server IP Interface (SIPI). The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page at (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the TN8412AP Server IP Interface (SIPI) circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN8412AP SIPI circuit pack.

If necessary, upgrade the firmware on the just installed TN8412AP Server IP Interface (SIPI) circuit pack that you just installed. For more information, see Upgrading firmware on page 187.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)

- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see Upgrading firmware on page 187.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating from an IP600 or S8100 to an S8400 Server

Use these procedures to migrate from an existing IP600 system in a Compact Modular Cabinet (CMC) or an S8100 switch in a Compact Modular Cabinet (CMC) to an Avaya S8400 Server using file transfer protocol (ftp). The existing systems supported for migrations must be standard reliability and direct connect. In all instances, the cabinets can be reused as port networks (PNs). However you can add a G650 Media Gateway PN if the existing system has one PN. This procedure supports a migration to Communication Manager Release 5.x.

When migrating an existing S8100 in a CMC1 Media Gateway, you use one TN8412AP S8400 IP Interface (SIPI) circuit pack to control the PN. You also must replace the processor circuit pack.

This migration affects service because you must turn off the S8100 chassis to replace the processor and tone-clock circuit packs.

Migration paths

The IP600 or S8100 and their releases that can be migrated to S8400 Server configuration include:

- Communication Manager Release 9 and later

To migrate, you can use the existing translations. The only supported method to move translations from legacy systems is to use ftp.

When you migrate from an IP600 or an S8100 to an S8400 Server using ftp:

1. On the SAT, copy the translation files.
2. Move the translations onto the Services laptop.
3. Copy the translations to the S8400 Server.

Replacement of INTUITY AUDIX Messaging with Communication Manager Messaging

The S8100 Server offers an embedded version of the INTUITY AUDIX Messaging application. This application is *not* supported on the S8400 Server. Instead, the customer may choose to install the embedded Communication Manager Messaging application.

Installation of Communication Manager Messaging software

If you install the Communication Manager Messaging application as a part of this migration, you install the software as part of the Communication Manager software. If you install an external version of Communication Manager Messaging or Modular Messaging, all installation is done on the external messaging server.

INTUITY AUDIX data that can be reused in Communication Manager Messaging and data that must be reinput

Though you restore the S8100 switch translations in the S8400 Communication Manager as a part of this migration, you *cannot* use Communication Manager Web pages to restore INTUITY AUDIX administration data to the installed Communication Manager Messaging application. This restriction includes all administration data previously defined in the INTUITY AUDIX itself through the INTUITY AUDIX windows or the AUDIX command line interface. This restriction also includes messages, greetings, and names.

Note:

The customer administrator should advise subscribers well in advance that their messages, greetings, and names will be deleted during the upgrade and will not be restored. Additionally, the administrator should advise subscribers to use Message Manager to save critical messages on their P.C.s. These messages will remain available only on the P.C. to which the messages were saved. The messages cannot be reimported into Communication Manager Messaging.

To save some time, you can export INTUITY AUDIX mailbox data prior to the upgrade and import the mailbox data after the upgrade using Avaya Site Administration, ProVision, or another tool. However, you must manually reinput all other administration data using the Communication Manager Messaging interface, Avaya Site Administration, or ProVision.

However, some key switch translations within Communication Manager that support INTUITY AUDIX Messaging are restored as part of the switch translation restore and can be reused. These translations include:

- The AUDIX coverage path

- The assignment of the AUDIX coverage path for each telephone extension

However, the following switch translations must be modified for the Communication Manager Messaging application:

- The node name for AUDIX
- The AUDIX hunt group

Note:

The Communication Manager Messaging hunt group does not require assigned AUDIX ports. Note the extensions of the ports previously assigned to the hunt group, and remove them from the hunt group.

Additional switch elements like a signaling group and trunk group must also be administered to support Communication Manager Messaging. For information on how to administer these and all switch integration elements, see *Avaya IA770 INTUITY AUDIX Messaging Application Release 3.1 Administering the S8300 and S8400 Media Servers to Work with IA770*, 07-600788.

Removing unused INTUITY AUDIX ports or hunt groups

The previously administered INTUITY AUDIX analog ports from the S8100 translations are part of the overall station usage of the switch and count against the maximum station capacity available on the S8400 Server. The hunt group for the Communication Manager Messaging applications does not use analog ports. Therefore, after you modify the AUDIX hunt group for Communication Manager Messaging, the hunt groups's previously assigned AUDIX ports are available for use by telephones or other devices. Use the **`remove station`** command to remove these ports from the switch so that they can be added later for future use.

If you do *not* replace the S8100 embedded INTUITY AUDIX application as part of the migration to the S8400 Server, you should remove the hunt group from switch administration, and then remove the analog ports. In this case, you also must modify the administration of each subscriber telephone to remove the AUDIX coverage path.

For information on how to administer these elements, see *Avaya IA770 INTUITY AUDIX Messaging Application Release 3.1 Administering the S8300 and S8400 Media Servers to Work with IA770*, 07-600788.

Checklists

Before you go on site, perform the following tasks

:

✓	Task	Description
	Verify that your Services laptop has the appropriate hardware.	Correct hardware components include: ● 40 MB available disk space ● direct Ethernet cable ● serial cable and adapter ● RS-232 port connector ● Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● CD-ROM drive
	Verify that your Services laptop has the appropriate software.	Correct software components include: ● Windows 2000/XP operating system ● Terminal emulation program: HyperTerminal or other ● TCP/IP networking software: bundled with Windows OS ● Web browser: Internet Explorer 5.0 or later
	Obtain appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media Gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the equipment of the customer.
	Obtain the serial number of the Servers, if necessary.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD with the current software and firmware.	You use this CD to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware available.	The following firmware are on the software CD: • IPSI or TN8412AP Server IP Interfaces (SIPI) • C-LAN • MedPro • VAL circuit packs For the most current versions, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download license and authentication files to your Services laptop.	New license and authentication files are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557 and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed as well as any changes to the system alarming configuration. ART is available only to Avaya associates. Business Partners can call 800-295-0099.
	Verify that you have copied all necessary files to your computer	These files can include: • service packs • license file • authentication file • firmware for programmable circuit packs
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

For more information, see Migration paths on page 91.

To migrate from a DEFINITY system, you must complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. Remote or on-site ASG access is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Presite migration checklist

Before you go on site, perform the following tasks in Table 6:

Table 6: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks before you start the migration:

✓	Task	Description
	Verify that you have the correct cables for the TN8412AP S8400 Internet Protocol Interface (SIPI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see *Installing and Configuring the Avaya S8400 Media Server* (03-300678).

When you are migrating from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Performing a migration

CAUTION:

This migration affects service. When the Definity One/S8100 is turned off, the system drops all calls. Service returns when the server takes control of the IPSIs.

The general migration procedures are as follows:

- Turn off the processor gracefully - pre-conversion administration
- Replace the processor circuit pack or tone clock circuit pack with a TN8412AP S8400 IP Interface (SIPI) circuit pack
- Connect the TN8412AP Server IP Interface (SIPI) circuit pack to the Ethernet switch on the customer network
- Assign an IP address to the TN8412AP Server IP Interface (SIPI) circuit pack

You can reuse the translations from the existing system when you migrate to an S8400 Server.

Note:

You must install the new Communication Manager license file on the server before you make the change. The TN8412AP Server IP Interface (SIPI) serial number can be used for licensing purposes.

Premigration administration

This migration is a service-affecting event. You must turn off the S8100 chassis to replace the processor and tone-clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

Connecting to the processor

To connect to the processor:

1. Connect the computer that you use to access the cabinet.
2. Start a SAT session using Native Configuration Manager or Avaya Site Administration.
3. Log in as **craft**.

Saving translations

This step is important in case you need to back out of the migration. These translations are not used in the migration.

To save translations:

Note:

Save translations to a flash card.

1. Plug the PCMCIA/Compact Flash adapter in the PCMCIA slot on the TN2314 Processor circuit pack.
2. In DEFINITY, type **`save translation`** and press **Enter** to save the translations.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:
   a. **`list configuration all`**
   b. **`list trunk-group`**

c. **`list hunt-group`**

If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.

2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Migration tasks

You can reuse the translations from the current system when you migrate to an S8400 Server.

Note:

You must install the new Communication Manager license file on the server before you make the change. The TN8412AP Server IP Interface (SIPI) serial number can be used for licensing purposes.

Perform these tasks to change a processor port network to a port network (CMC).

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

The TN8400BP Server circuit pack replaces the TN795 or TN2314 Processor circuit pack. The TN798 and TN2314 circuit packs do not have the Communication Manager Messaging feature. The current processor circuit pack must be returned to Avaya.

Opening a SAT session

To open a SAT session:

1. Use a crossover cable and connect the Services laptop to the Services port on the TN2314 or TN795 Processor circuit pack.
2. Access the server command line interface using an SSH client like PuTTY and an IP address of **`192.11.13.6`**.
3. Log in as **`lucent3`**.
4. At the LAC prompt, type **`definity`** or **`multivantage`** and press **Enter**.
5. For the terminal type, select **NTT**.

Copying translation files

To copy translation files:

1. On the SAT, type **`save translations`** and press **Enter**.
2. Type **`logoff`** and press **Enter**.
3. At the LAC prompt, type **`bash`** and press **Enter**.
4. Type **`ftpserv`**. Press **Enter**.
5. At the prompt, type **`cd d:/LucentData/Definity`** and press **Enter**.
6. Type **`cp xltn1_data.xln d:/LucentPub/ftproot/`** and press **Enter**.
7. Type **`cp xltn2_data.xln d:/LucentPub/ftproot/`** and press **Enter**.
8. Type **`ftpserv`** to turn on the ftp services and press **Enter**.

Opening an ftp session

To open an ftp session on the Services laptop:

1. On the Services laptop, click **Start** > **Run** to open the **Run** window.
2. Create a customer directory or create a directory at \temp for this migration.
3. Type **`cmd`** and press **Enter**.
4. Type **`cd \temp`** or the directory location and press **Enter**.
5. Type **`ftp 192.11.13.6`** and press **Enter**.
6. Log in as **`anonymous`** and press **Enter**.
7. For the password, press **Enter**.
8. At the ftp prompt, type **`bin`** and press **Enter**.
9. Type **`get xltn1_data.xln`** and press **Enter**.
10. Type **`get xltn2_data.xln`** and press **Enter**.
11. Type **`bye`** and press **Enter** to close the ftp session.

Moving the translation files

To move the translation files on the Services laptop

- Move the xln files to the c:/temp directory.

Turning off power to all cabinets

CAUTION:
Ensure that you have done the premigration administration. For more information, see Premigration administration on page 166.

To turn off power to all cabinets:

1. From the bash prompt on the Services laptop, type **`shutdown system`** and press **Enter** to perform a graceful shutdown.
2. Wait until the Shutdown Complete LED on the lower portion of the faceplate of the processor is solid green
3. Turn off the power to all cabinets.

Removing circuit packs

To remove circuit packs from the CMC1 Media Gateway:

1. Remove the TN795 or TN2314 Processor circuit pack from slot A01.
2. Remove the TN744 Call Classifier-Detector circuit pack.
3. Remove the TN767 DS1 Interface circuit pack, if installed.
4. Remove the TN2207 DS1 Interface circuit pack, if installed.
5. Remove the TN2313 DS1 Interface circuit pack, if installed.

Inserting circuit packs

To install circuit packs into the CMC1 Media Gateway:

1. Install the TN8412AP S8400 IP Interface (SIPI) circuit pack into slot A02.
2. Install the TN8400BP Media Server circuit pack into slot A01.
3. If the system had a TN767, TN2207, or TN2313 DS1 Interface circuit pack, install the TN464HP DSD1 Interface circuit pack in any open slot.

Connecting cables

To connect cables:

1. On the rear of the carrier, connect the server cable adapter into port 1 on the rear of the TN8400BP Media Server circuit pack.
2. Connect the amphenol connector into slot A02 on the rear of the TN8412AP SIPI circuit pack.
3. Connect the customer LAN cable into the port labeled ETH-B on the adapter in slot A01.
4. Connect the IPSI cable into the port labeled ETH-A on the adapter in slot A01.
5. Connect the other end of the IPSI cable to the amphenol connector in slot A02.
6. Connect the power plug on the DVD drive to a wall outlet.
7. Connect the USB DVD drive to the USB port on the faceplate of the TN8400BP Media Server circuit pack.
8. On the DVD drive, ensure that the on/off/ext switch is in the **EXT** position.
9. Insert the Communication Manager CD into the USB DVD drive.
10. Connect the Services laptop to the Services port on the front of the TN8400BP Media Server circuit pack.
11. Turn on the power to all cabinets.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test

You can install a TN771 Maintenance/Test circuit pack in any slot other than slots A01 and A02. Avaya recommends one TN771 Maintenance/Test circuit pack per location for the following conditions:

- There are three or more G650, G600, or CMC1 Media Gateways in the S8400 system. Do not include G150 and H.248 Media Gateways in this count, and
- There are IP endpoints or ISDN endpoints. These endpoints consist of:
  - BRI trunks
  - PRI trunks
  - BRI stations

The TN8412AP S8400 IP Interface (SIPI) circuit pack provides all maintenance functions that were present on the TN798 or TN2402 Processor circuit pack. This carrier does not have a TN775 Maintenance (EPN) dedicated slot.

Translation migration

This section provides information to migrate translation files from the current server to the S8400 Server.

Setting telnet parameters

The Microsoft telnet application can be set to send a carriage return (CR) and line feed (LF) whenever you press **Enter**. The installation program interprets this as two key presses. You need to correct this before you telnet to the server.

Note that this procedure is done entirely on your laptop, not on the S8400 Server.

To set the telnet parameters:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. Type **`telnet`**. Press **Enter** to open a Microsoft Telnet session.
3. Type **`unset crlf`**. Press **Enter**.
4. Type **`display`**. Press **Enter** to confirm that `Sending only CR` is set.
5. Close the window by clicking the **X** in the upper-right corner.

   This procedure resets your Microsoft telnet defaults and does not need to be done each time you use Telnet.

Installing the software load

For more information on installing software loads, see *Installing and Configuring the Avaya S8400 Media Server*, 03-300678.

To install the software load:

1. Power down the server.
2. Connect the USB CD/DVD drive to the S8400 Server.
3. Connect the laptop to the Services port on the faceplate of the server using a crossover cable.
4. Power up the server.
5. From the Services laptop, click **Start** > **Run** to open the **Run** window.
6. Type **`ping -t 192.11.13.6`**. Press **Enter** to indicate when the Services port is responding.
7. From the laptop Start menu, click **Start** > **Run**.

8. In the **Run** dialog box, type **`telnet 192.11.13.6`**. Press **Enter** to view the first screen.

Note:

To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

9. Select **Install**, ensure that OK is highlighted and press **Enter**.

10. On the **Select Release Version** window, ensure that the Build line and <OK> are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

    Once the drive is properly configured, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

    These processes can take up to 20 minutes. When the system finishes the software installation, the server reboots and the CD/DVD-ROM drive opens. You must remove the CD from the drive at this time.

    The reboot can take up to 3 minutes. The telnet session drops automatically.

11. Open a Web browser.
12. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
13. Log in as **craft** or **dadmin**.

Configuring the server

To configure the server:

1. From the Services laptop, open a Web browser.

2. In the **Address** field, type **`http://192.11.13.6`** and press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.
4. Under Server, click **Server Date/Time**.
5. On the **Server Date/Time** window, set the date, time, and time zone for the server.
6. Click **Submit** to put the changes into effect.

   Important:
   It is necessary to reboot the server to initialize server settings that are restored but not yet activated. See Reboot the server on page 301.

   CAUTION:
   Not rebooting the server will lead to erroneous behavior surrounding the time of day at daylight-saving-time transition.
7. Under **System Management Interface (SMI)** click **Installation > Configure Server**.
8. In the **Review Notices** window, click **Continue**.
9. In the **Back Up Data** window, click **Continue**.
10. In the **Specify how you want to use this wizard page**, select **Configure all services using the wizard**. Click **Continue**.

    Note:
    You can set up servers to various configurations. The following steps provide a general outline of required steps to complete the configuration.
11. In the **Set Server Identifies** window:
    - In the **Host Name** field, enter a unique name for the server.
    - In the **ID** field, enter as required or accept the default.
    - In the **CNA** field, enter as required or accept the default.
    - In the **Enterprise LAN** field, enter as required or accept the default.
    - In the **Assign the Processor Ethernet to an Interface** area, select one as required.
12. Click **Continue**.
13. In the **Configure Interfaces** window, set up as required. Click **Continue**.

    If you are installing the Communication Manager Messaging application, in the Integrated Messaging area, enter the IP address in the **IP address server1** field. Click **Continue**.
14. In the **Ethernet Adjuncts** window, set up as required. Click **Continue**.
15. In the **External DNS Server Configuration** window, set up as required. Click **Continue**.
16. In the **Static Network Routes (Optional)** window, set up as required. Click **Continue**.
17. In the **Network Time Server** window, set up as required. Click **Continue**.

18. In the **Set Modem Interface** window, set up as required. Click **Continue**.
19. In the **Configure Maintenance Processor Complex (MPC)** window, set up as required. Click **Continue** to configure the server.
20. When completed, under Miscellaneous, click **Messaging Software**.
21. Verify the messaging software is enabled. If messaging software is disabled, click **Enable**.

Installing the license and authentication file

To install the Communication Manager license file and the Avaya authentication file:

1. Open a Web browser.
2. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.
4. Under Miscellaneous, click **Download Files**.
5. Click **Browse** and select the file saved on the Services laptop.
6. Click **Download** to place the file on the server.
7. Under Security, click **License File**.

   The system displays the **License File** screen.
8. Select **Install the license file I previously downloaded** and click **Submit**.

   The system tells you the license file is installed successfully.
9. Under Security, click **Authentication File**.

   The system displays the **Authentication File** screen.
10. Select **Install the Authentication file I previously downloaded** and click **Install**.

    The system tells you the authentication is installed successfully.

Copying translation files to the server

To copy translation files to the server:

1. From the Services laptop, open a Web browser.
2. On **System Management Interface (SMI)** click **Administration > Server (Maintenance)**

3. Under Miscellaneous, click **Download Files**.
4. Select **Files to download from the machine I'm using to connect to the server**.
5. Click **Browse** and select the translation file saved on the Services laptop and click **Download**. A translation file example might be C:\Program Files\PCM\xltn1_data.xln and xl.tn2_data.xln

   The file is placed in the /var/home/ftp/pub directory of the S8400 Server.
6. Access the server command line interface using an SSH client like PuTTY and an IP address of **`192.11.13.6`** to the Services port on the TN8400BP S8400 circuit pack.
7. Log in as **craft** or **dadmin**.
8. Type **`cd /var/home/ftp/pub directory`**. Press **Enter**.
9. From the /var/home/ftp/pub directory, type **`read_s8100_file`** and press **Enter**.

   The system renames the translation files as xln1 and xln2.

   If the restore process fails, you get an error message with the reason for the failure. If that happens, the translation file is not restored. Resolve the reason for the failure and restart the process.
10. Type **`cd /etc/opt/defty`** and press **Enter**.
11. Type **`ls -ltr`** and press **Enter**.

    Verify that the xln1 and xln2 files are not zero length.
12. Open a SAT session.
13. Type **`reset system 4`** and press **Enter** to load the restored translations into memory.

Post-migration administration

This section describes the post-migration administration to complete the migration to the S8400 Server.

Important:
When you format the compact flash card for use in the S8400 Server, all data is erased from the compact flash card.

Note:
Do not use the compact flash card (Comcode 700381841) in an S8100 Windows system. The operating system does not recognize the compact flash card.

After the migration, you can format the compact flash card with Comcode 700381841 for the S8400 Server and use the compact flash card as the backup compact flash card.

Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs

When you use static IP addressing, you must assign IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs.

Using static addressing

You can administer static IP addresses for the TN8412AP Server IP Interface (SIPI) circuit packs. You administer the addresses directly through the Ethernet port connection on the TN8412AP Server IP Interface (SIPI) faceplate (top port). For more information, see Figure 4: Connecting directly to the SIPI on page 115.

Figure 4: Connecting directly to the SIPI

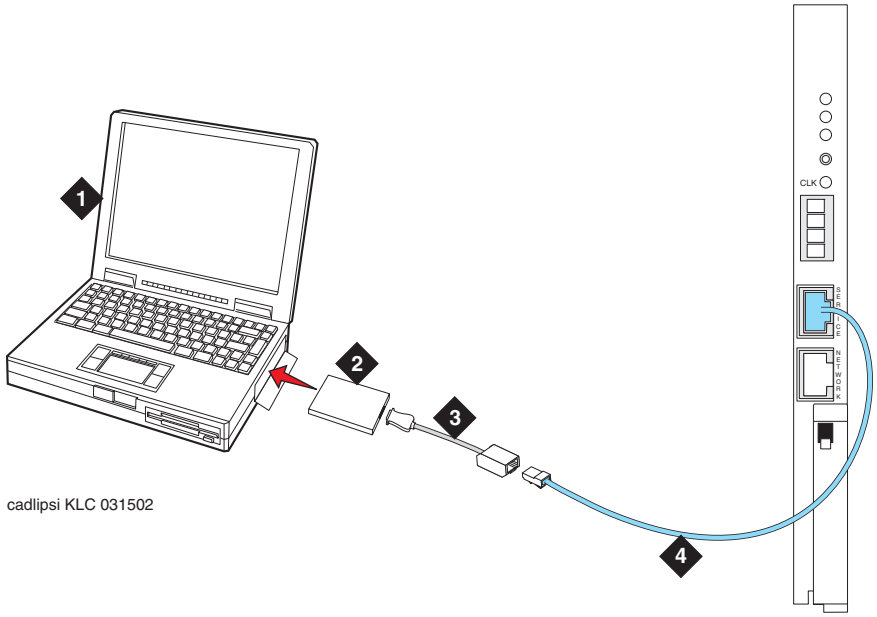


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 crossover cable to SIPI**

Note:

Ensure that you have the password before proceeding.

Logging in to the TN8412AP Server IP Interface (SIPI)

To log in to the TN8412AP Server IP Interface (SIPI):

1. Type **`telnet 192.11.13.6`**. Press **Enter** to open the Telnet window and connect to the TN8412AP Server IP Interface (SIPI)

   Prompt = [IPSI]:

   Note:

   While connected to the TN8412AP Server IP Interface (SIPI), type **`help`** or **`?`** to obtain online help. Most commands have two or three letter abbreviations.

2. Type **`ipsilogin`**. Press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login used on the TN8412AP Server IP Interface (SIPI) has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`**. Press **Enter**.
2. Type **`show port 1`**. Press **Enter** to see the current settings.

3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnet mask. Press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) session.
5. Telnet to **192.11.13.6** and login.
6. Enter **`show control interface`**.
   The system displays the IP address, subnet mask, and default gateway information. Verify that the proper information was entered.
7. If a default gateway is used, enter the gateway IP address with **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway.
8. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) or IPSI session.
9. Telnet to **192.11.13.6** and login.
10. Use **`show control interface`** to verify the administration.
11. Type **`exit`**. Press **Enter** to see the changes.

Resetting the TN8412AP Server IP Interface (SIPI)

To reset the TN8412AP Server IP Interface (SIPI):

1. Type **`reset`**. Press **Enter**
   Answer **Y** to the warning.

   Note:

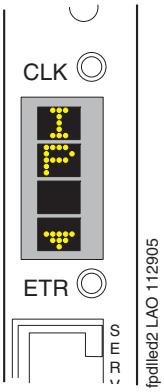
   Resetting the TN8412AP Server IP Interface (SIPI) terminates the administration session. If further administration is required, start a new telnet session to the TN8412AP Server IP Interface (SIPI).

   Note:

   Control network settings become effective when you exit the IPADMIN session. Control settings include the IP address, the subnet mask, and the gateway.

2. Disconnect the Services laptop from the faceplate.
3. Check the LCD. Verify that it has an I P with a filled-in V that shows at the bottom. For more information, see Figure 5.

Figure 5: LED display that shows that the SIPI has a static IP address



   Note:

   Clear the ARP cache on the laptop before connecting to another TN8412AP Server IP Interface (SIPI). If the cache is not cleared, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

4. Close the window.

Enabling control of the TN8412AP Server IP Interface (SIPI)

To enable control of the TN8412AP Server IP Interface (SIPI):

Note:

Ensure that the TN8412P SIPI has the current firmware.

CAUTION:

This procedure allows the server to take control of the TN8412AP Server IP Interface (SIPI)-controlled port network. Failure to complete the procedure correctly can result in no connection to the network.

1. Type **`add cabinet 1`**. Press **Enter**.
2. Administer the appropriate cabinet type and carriers.
3. Type **`add ipserver-interface 1`** where **`1`** means port network. Press **Enter**.
4. In the **Host** field, type in the IP address that was programmed into the TN8412AP Server IP Interface (SIPI). Press **Enter**.
5. Type **`save translation`**. Press **Enter**.
6. Type **`change system ipserver-interface`**. Press **Enter**.
7. In the **IPSI Control of Port Networks** field, type **`enabled`**. Press **Enter**.
8. Type **`save translation`**. Press **Enter**.
9. Verify the translation migration was successful.

   Place test calls, verify trunk status (if applicable), and so forth.

   The server now controls all the port networks.

Verifying TN8412AP Server IP Interface (SIPI) translations

To verify TN8412AP Server IP Interface (SIPI) translations:

1. Type **`list ipserver-interface`**. Press **Enter**.
2. Verify that the TN8412AP Server IP Interface (SIPI) circuit pack(s) is translated.

Verifying TN8412AP Server IP Interface (SIPI) connectivity

To verify TN8412AP Server IP Interface (SIPI) connectivity:

1. Start a Web browser.
2. Under Diagnostics, click **Ping**.
3. Under Endpoints to Ping, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Type the correct cabinet and carrier numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each TN8412AP S8400 IP Interface (SIPI) circuit pack must be on the most current and same firmware load. You might need to upgrade the firmware on the TN8412AP Server IP Interface (SIPI). The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page at (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the TN8412AP Server IP Interface (SIPI) circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN8412AP SIPI circuit pack.

If necessary, upgrade the firmware on the just installed TN8412AP Server IP Interface (SIPI) circuit pack that you just installed. For more information, see Upgrading firmware on page 187.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see Upgrading firmware on page 187.

Administering Communication Manager Messaging

Administer the Communication Manager Messaging (previously known as IA770 INTUITY AUDIX Messaging) as required. For more information, see *Avaya IA 770 INTUITY AUDIX Messaging Application, Administering the S8300 and S8400 Media Servers to work with IA 770*.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*,

03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (ATA flash card)

Use these procedures to migrate from an existing DEFINITY Server CSI in a Compact Modular Cabinet (CMC) or G600 Media Gateway to an Avaya S8400 Server. Use the ATA flash card on the TN2402 ProLogix Processor circuit pack for whichever loads that circuit pack supports. This procedure supports a migration to Communication Manager Release 5.x.

To migrate an existing DEFINITY Server CSI in a CMC1 Media Gateway, you use one TN8412AP S8400 IP Interface (SIPI) circuit pack to control the one port network. You must replace the TN2182 Tone Clock circuit pack with a TN8412AP Server IP Interface (SIPI) circuit pack that you install in the A position in the cabinet. You also must remove the processor circuit pack.

This migration affects service because you must turn off the CSI chassis to replace the processor and tone-clock circuit packs.

Migration paths

Avaya supports the following migrations of a DEFINITY Server CSI in a CMC1 Media Gateway or a G600 Media Gateway to the S8400 Server configuration:

- DEFINITY Release 9 and later

To migrate, you can use the existing translations. The only supported method to move translations from legacy systems is to:

1. Copy the translations to the compact flash.
2. Plug the Compact Flash card from the PCMCIA/Compact Flash adapter into the Compact Flash slot on the TN8400BP Server circuit pack.
3. Copy the translation files from the compact flash to the S8400 Server.

Checklists

Before you go on site, perform the following tasks

:

✓	Task	Description
	Verify that your Services laptop has the appropriate hardware.	Correct hardware components include: ● 40 MB available disk space ● direct Ethernet cable ● serial cable and adapter ● RS-232 port connector ● Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● CD-ROM drive
	Verify that your Services laptop has the appropriate software.	Correct software components include: ● Windows 2000/XP operating system ● Terminal emulation program: HyperTerminal or other ● TCP/IP networking software: bundled with Windows OS ● Web browser: Internet Explorer 5.0 or later
	Obtain appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media Gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the equipment of the customer.
	Obtain the serial number of the Servers, if necessary.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file.
	Verify that you have the Communication Manager software distribution CD with the current software and firmware.	You use this CD to install the software on the server and upgrade the firmware.
		1 of 2

✓	Task	Description
	Verify that you have the current preupgrade or premigration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware available.	The following firmware are on the software CD: • IPSI or TN8412AP Server IP Interfaces (SIPI) • C-LAN • MedPro • VAL circuit packs For the most current versions, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download license and authentication files to your Services laptop.	New license and authentication files are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557 and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed as well as any changes to the system alarming configuration. ART is available only to Avaya associates. Business Partners can call 800-295-0099.
	Verify that you have copied all necessary files to your computer	These files can include: • service packs • license file • authentication file • firmware for programmable circuit packs

2 of 2

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

For more information, see Migration paths on page 125.

To migrate from a DEFINITY system, you must complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Presite migration checklist

Before you go on site, complete the following tasks:

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Matrix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace any TN799B/C circuit pack with the TN799DP circuit pack.
	Replace the 259A adapter and CAT3 cable.	Replace the 259A adapter with the cable extender adapter (Comcode 848525887) and the CAT3 cable with a CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570 EI circuit packs with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks before you start the migration:

✓	Task	Description
	Verify that you have the correct cables for the TN8412AP S8400 Internet Protocol Interface (SIPI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see *Installing and Configuring the Avaya S8400 Server* (03-300678).

When you are migrating from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Documentation checklist for migrations

For a list of documents that are needed to perform the migration, see Resources on page 35.

✓	Document	Description
	Quick Start for Hardware Migration: Avaya S8400 Server in an Avaya CMC1 or G600 Media Gateway (03-300706)	A quick reference guide that provides physical installation and connection information.
	Installing and Configuring the Avaya S8400 Server (03-300678)	Provides installation instructions for the S8400 Server.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.

Performing a migration

CAUTION:

This migration affects service because when you turn off the processor port network (PPN), the system drops all calls. Service returns when the server takes control of the IPSIs.

You can reuse the translations from the existing system when you migrate to an S8400 Server.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Premigration administration

This migration affects service. You must turn off the CMCs to replace the processor and tone-clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

Connecting to the processor

To connect to the processor:

1. Connect the computer that you use to access the cabinet.
2. Start a SAT session using Native Configuration Manager or Avaya Site Administration.
3. Log in as **craft**.

Removing netcon data modules

To remove Netcon data module information:

1. Type **`list data module`**. Press **Enter**.
2. Notice if the system contains any Netcon circuit packs.

   If there are Netcon data modules, continue to step 3.

   If there are no Netcon data modules, continue to Saving translations on page 355.

3. Type **`list user ext x`**. Press **Enter** where ***x*** shows who is using the associated Netcon data module.

```
list usage extension 2501
                              LIST USAGE REPORT

    Used By
    Hunt Group           Group Number           99               Member 1



Command successfully completed
```

   For example, the screen in step 3 shows the extension 2501 is being used on Hunt Group 99.

4. Type **`change hunt-group xx`**. Press **Enter** where ***xx*** is the hunt group number.
5. In the **Hunt Group** screen, press the space bar to highlight the information. Press **Return** to remove the information.
6. Repeat for each extension.
7. When you finish, press **Submit**.
8. Repeat for each listing.
9. Type **`remove data-module xxxx`**. Press **Submit** where ***xxxx*** is the extension to be removed.
10. Repeat for all items listed on the **`list data module`** command.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:
   a. **`list configuration all`**
   b. **`list trunk-group`**

c. **`list hunt-group`**

If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.

2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

This step is important in case you need to back out of the migration.

To save translations:

Note:

Save translations to a flash card.

1. Plug the PCMCIA/Compact Flash adapter in the PCMCIA slot on the TN2402 ProLogix Processor circuit pack.
2. Type **`save translation`**. Press **Enter** to save translations to the system disk.
3. The system displays a **Command successfully completed** message or an error message.

Migration tasks

You can reuse the translations from the current system when you migrate to an S8400 Server.

Note:

You must install the new Communication Manager license file on the server before you make the change. The TN8412AP Server IP Interface (SIPI) serial number can be used for licensing purposes.

Perform these tasks to convert a processor port network to a port network (CMC).

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

The TN8400BP Server circuit pack replaces the TN798 or TN2402 Processor circuit pack. The TN798 and TN2402 circuit packs do not have the Communication Manager Messaging feature. You must return the current processor circuit pack to Avaya.

Turning off the power to the control cabinet

CAUTION:
Ensure that you have completed the premigration administration. If you do not perform the premigration administration, the system will not function. For more information, see Premigration administration on page 226.

To turn off power to the control cabinet:

1. On the faceplate of the processor, press and hold the shutdown button until the shutdown process starts.

   When you see the green light the system is shut down.

   DANGER:
   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the cabinet, pull the AC power cord from the back of the cabinet.

2. Unplug the power cord from the back of the cabinet to turn off the cabinet.

Removing circuit packs

To remove circuit packs from the CMC1 Media Gateway:

1. Remove the TN798B or TN2402 Processor circuit pack from slot A01.
2. Remove the TN2182 Tone Clock circuit pack from slot A02.
3. Remove the TN767 DS1 Interface circuit pack, if installed.
4. Remove the TN2207 DS1 Interface circuit pack, if installed.
5. Remove the TN2313 DS1 Interface circuit pack, if installed.

Inserting circuit packs

To install circuit packs into the CMC1 Media Gateway:

1. Install the TN8412AP S8400 IP Interface (SIPI) circuit pack into slot A02.
2. Install the TN8400BP Media Server circuit pack into slot A01.

3. If the system had a TN767, TN2207, or TN2313 DS1 Interface circuit pack, install the TN464HP DSD1 Interface circuit pack in any open slot.

Connecting cables

To connect cables:

1. On the rear of the carrier, connect the server cable adapter into port 1 on the rear of the TN8400BP Media Server circuit pack.
2. Connect the amphenol connector into slot A02 on the rear of the TN8412AP SIPI circuit pack.
3. Connect the customer LAN cable into the port labeled ETH-B on the adapter in slot A01.
4. Connect the IPSI cable into the port labeled ETH-A on the adapter in slot A01.
5. Connect the other end of the IPSI cable to the amphenol connector in slot A02.
6. Connect the power plug on the DVD drive to a wall outlet.
7. Connect the USB DVD drive to the USB port on the faceplate of the TN8400BP Media Server circuit pack.
8. On the DVD drive, ensure that the on/off/ext switch is in the **EXT** position.
9. Insert the Communication Manager CD into the USB DVD drive.
10. Connect the Services laptop to the Services port on the front of the TN8400BP Media Server circuit pack.
11. Turn on the power to all cabinets.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.

5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test

You can install a TN771 Maintenance/Test circuit pack in any slot other than slots A01 and A02. Avaya recommends one TN771 Maintenance/Test circuit pack per location for the following conditions:

- There are three or more G650, G600, or CMC1 Media Gateways in the S8400 system. Do not include G150 and H.248 Media Gateways in this count, and
- There are IP endpoints or ISDN endpoints. These endpoints consist of:
  - BRI trunks
  - PRI trunks
  - BRI stations

The TN8412AP S8400 IP Interface (SIPI) circuit pack provides all maintenance functions that were present on the TN798 or TN2402 Processor circuit pack. This carrier does not have a TN775 Maintenance (EPN) dedicated slot.

Translation migrations

This section describes how to migrate the translation files from the current system to the S8400 Server.

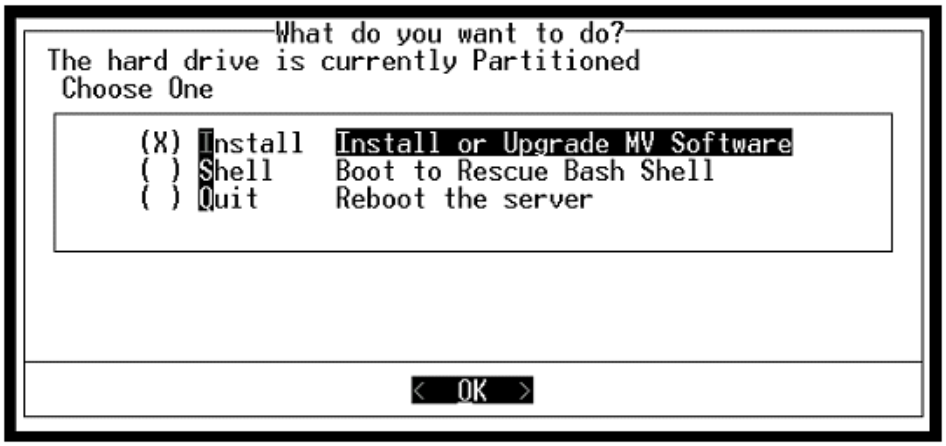
Installing the software load

For more information on installing software loads, see *Installing and Configuring the Avaya S8400 Media Server*, 03-300678.

To install the software load:

1. Power down the server.
2. Connect the USB CD/DVD drive to the S8400 Server.

3. Connect the laptop to the Services port on the faceplate of the server using a crossover cable.
4. Power up the server.
5. From the Services laptop, click **Start** > **Run** to open the **Run** window.
6. Type **`ping -t 192.11.13.6`**. Press **Enter** to indicate when the Services port is responding.
7. From the laptop Start menu, click **Start** > **Run**.
8. In the **Run** dialog box, type **`telnet 192.11.13.6`**. Press **Enter** to view the first screen.



Note:

To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

9. Select **Install**, ensure that OK is highlighted and press **Enter**.

10. On the **Select Release Version** window, ensure that the Build line and <OK> are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

    Once the drive is properly configured, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

    These processes can take up to 20 minutes. When the system finishes the software installation, the server reboots and the CD/DVD-ROM drive opens. You must remove the CD from the drive at this time.

    The reboot can take up to 3 minutes. The telnet session drops automatically.

11. Open a Web browser.
12. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
13. Log in as **craft** or **dadmin**.

Configuring the server

For more information on configuring the server and the use of the Avaya Installation Wizard, see *Installing and Configuring the Avaya S8400 Media Server*, 03-300678.

To configure the server:

1. Open a Web browser.
2. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.
4. Access **System Management Interface (SMI)** click **Administration** > **Server (Maintenance)**
5. Under Server, click **Server Date/Time**.
6. In the **Server Date/Time** window, verify the data and time are correct. If the date and time are incorrect:
   a. Enter the date
   b. Enter the time
   c. Select the time zone
   d. Click **Submit**:

   Important:
   It is necessary to reboot the server to initialize server settings that are restored but not yet activated. See Reboot the server on page 301.

   CAUTION:
   Not rebooting the server will lead to erroneous behavior surrounding the time of day at daylight-saving-time transition.
7. Under Server Configuration, click **Configure Server**.

   The system starts the Configure Server Wizard.
8. In the **Review Notices** window, click **Continue**.
9. In the **Back Up Data** window, click **Continue**.
10. Select **Configure all services using the wizard** and click **Continue**.

    Note:
    You can set up servers to various configurations. The following steps provide a general outline of required steps to complete the configuration.
11. In the **Server Role** window, as shown in Figure 6, choose between Main, ESS or LSP depending on the platform on which the wizard is running.
12. In the **Set Identities** window, perform the following steps:
    - In the **Host Name** field, enter a unique name for the server.
    - In the **ID** field, enter as required or accept the default.
    - In the **CNA** field, enter as required or accept the default.

- In the **Enterprise LAN** field, enter as required or accept the default.
- In the **Assign the Processor Ethernet to an Interface** area, select one as required.

13. Click **Continue**.
14. In the **Configure Ethernet Interfaces** window, set up as required. Click **Continue**.
15. In the **Ethernet Adjuncts** window, set up as required. Click **Continue**.
16. In the **External DNS Server Configuration** window, set up as required. Click **Continue**.
17. In the **Static Network Routes (Optional)** window, set up as required. Click **Continue**.
18. In the **Configure Time Server** window, set up as required. Click **Continue**.
19. In the **Set Modem Interface** window, set up as required. Click **Continue**.
20. In the **Configure Maintenance Processor Complex (MPC)** window, set up as required and click **Continue** to configure the server.

Figure 6: Configure Server - Server Role

Installing the license and authentication file

To install the Communication Manager license file and the Avaya authentication file:

1. Open a Web browser.
2. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.

4. Under Miscellaneous, click **Download Files**.
5. Click **Browse** and select the file saved on the Services laptop.
6. Click **Download** to place the file on the server.
7. Under Security, click **License File**.

   The system displays the **License File** screen.
8. Select **Install the license file I previously downloaded** and click **Submit**.

   The system tells you the license file is installed successfully.
9. Under Security, click **Authentication File**.

   The system displays the **Authentication File** screen.
10. Select **Install the Authentication file I previously downloaded** and click **Install**.

    The system tells you the authentication is installed successfully.

Copying translation files to the server

To copy translation files to the server:

1. Plug the Compact Flash card with the translations from the PCMCIA/Compact Flash adapter into the Compact Flash slot on the TN8400BP Server circuit pack.
2. From the Services laptop, open a bash session.
3. Type **`read_csi_xln`** and press **Enter** to bring the CSI translations from the Compact Flash to the /etc/opt/defty directory.

   The system renames the translation files as xln1 and xln2.

   Note:

   Based on the server types use the command syntax as shown here:

   For S8400A Server, type: **`read_csi_xln -f /dev/sda`**

   For S8400B Server, type: **`read_csi_xln -f /dev/sdb`**
4. Type **`cd /etc/opt/defty`** and press **Enter**.
5. Type **`ls -ltr`** and press **Enter**.

   Verify that the xln1 and xln2 files are not zero length.
6. Open a SAT session.
7. Type **`reset system 4`** and press **Enter** to load the restored translations into memory.

If the restore process fails, you get an error message with the reason for the failure. If that happens, the translation file is not restored. Resolve the reason for the failure and restart the process.

Post-migration administration

This section describes the post-migration administration to complete the migration to the S8400 Server.

Important:
When you format the compact flash card for use in the S8400 Server, all data is erased from the compact flash card.

Note:
Do not use the compact flash card (Comcode 700381841) in an S8400 Windows system. The operation system does not recognize the compact flash card.

After the migration, you can format the compact flash card (Comcode 700381841) for the S8400 Server and use the compact flash card as the backup compact flash card.

Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs

When you use static IP addressing, you must assign IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs.

Using static addressing

You can administer static IP addresses for the TN8412AP Server IP Interface (SIPI) circuit packs. You administer the addresses directly through the Ethernet port connection on the TN8412AP Server IP Interface (SIPI) faceplate (top port). For more information, see Figure 7: Connecting directly to the SIPI on page 145.

Figure 7: Connecting directly to the SIPI

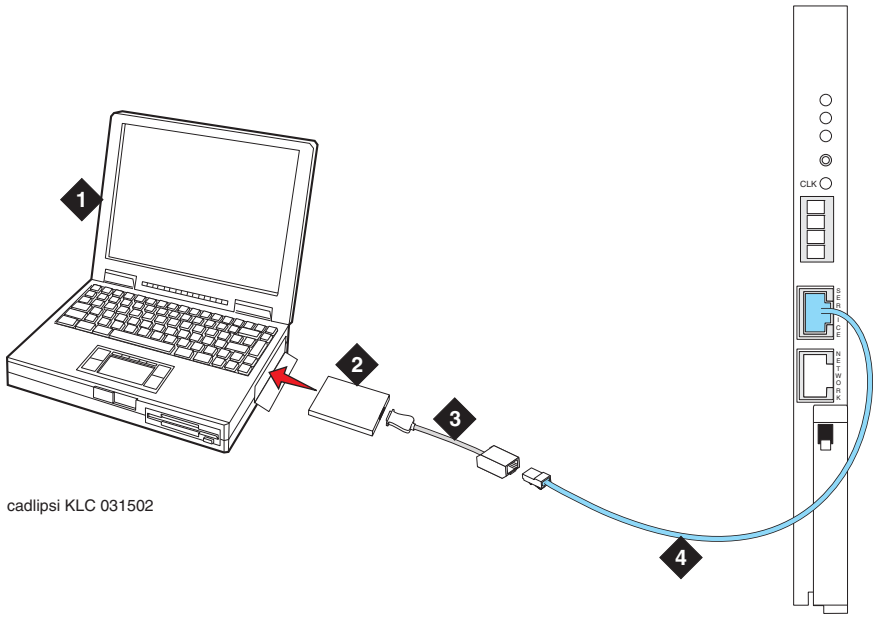


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 crossover cable to SIPI**

Note:

Ensure that you have the password before proceeding.

Logging in to the TN8412AP Server IP Interface (SIPI)

To log in to the TN8412AP Server IP Interface (SIPI):

1. Type **`telnet 192.11.13.6`**. Press **Enter** to open the Telnet window and connect to the TN8412AP Server IP Interface (SIPI)

   Prompt = [IPSI]:

Note:

While connected to the TN8412AP Server IP Interface (SIPI), type **`help`** or **`?`** to obtain online help. Most commands have two or three letter abbreviations.

2. Type **`ipsilogin`**. Press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login used on the TN8412AP Server IP Interface (SIPI) has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`**. Press **Enter**.
2. Type **`show port 1`**. Press **Enter** to see the current settings.
3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnet mask. Press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) session.

5. Telnet to **192.11.13.6** and login.
6. Enter **`show control interface`**.
   The system displays the IP address, subnet mask, and default gateway information. Verify that the proper information was entered.
7. If a default gateway is used, enter the gateway IP address with **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway.
8. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) or IPSI session.
9. Telnet to **192.11.13.6** and login.
10. Use **`show control interface`** to verify the administration.
11. Type **`exit`**. Press **Enter** to see the changes.

Resetting the TN8412AP Server IP Interface (SIPI)

To reset the TN8412AP Server IP Interface (SIPI):

1. Type **`reset`**. Press **Enter**
   Answer **`Y`** to the warning.

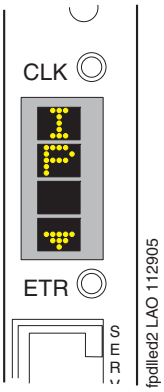
   Note:

   Resetting the TN8412AP Server IP Interface (SIPI) terminates the administration session. If further administration is required, start a new telnet session to the TN8412AP Server IP Interface (SIPI).

   Note:

   Control network settings become effective when you exit the IPADMIN session. Control settings include the IP address, the subnet mask, and the gateway.
2. Disconnect the Services laptop from the faceplate.
3. Check the LCD. Verify that it has an I P with a filled-in V that shows at the bottom. For more information, see Figure 8.

Figure 8: LED display that shows that the SIPI has a static IP address



Note:

Clear the ARP cache on the laptop before connecting to another TN8412AP Server IP Interface (SIPI). If the cache is not cleared, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

4. Close the window.

Enabling control of the TN8412AP Server IP Interface (SIPI)

To enable control of the TN8412AP Server IP Interface (SIPI):

Note:

Ensure that the TN8412P SIPI has the current firmware.

CAUTION:

This procedure allows the server to take control of the TN8412AP Server IP Interface (SIPI)-controlled port network. Failure to complete the procedure correctly can result in no connection to the network.

1. Type **`add cabinet 1`**. Press **Enter**.
2. Administer the appropriate cabinet type and carriers.
3. Type **`add ipserver-interface 1`** where **1** means port network. Press **Enter**.
4. In the **Host** field, type in the IP address that was programmed into the TN8412AP Server IP Interface (SIPI). Press **Enter**.
5. Type **`save translation`**. Press **Enter**.

6. Type **`change system ipserver-interface`**. Press **Enter**.
7. In the **IPSI Control of Port Networks** field, type **`enabled`**. Press **Enter**.
8. Type **`save translation`**. Press **Enter**.
9. Verify the translation migration was successful.

   Place test calls, verify trunk status (if applicable), and so forth.

   The server now controls all the port networks.

Verifying TN8412AP Server IP Interface (SIPI) translations

To verify TN8412AP Server IP Interface (SIPI) translations:

1. Type **`list ipserver-interface`**. Press **Enter**.
2. Verify that the TN8412AP Server IP Interface (SIPI) circuit pack(s) is translated.

Verifying TN8412AP Server IP Interface (SIPI) connectivity

To verify TN8412AP Server IP Interface (SIPI) connectivity:

1. Start a Web browser.
2. Under Diagnostics, click **Ping**.
3. Under Endpoints to Ping, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Type the correct cabinet and carrier numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway

- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.

2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each TN8412AP S8400 IP Interface (SIPI) circuit pack must be on the most current and same firmware load. You might need to upgrade the firmware on the TN8412AP Server IP Interface (SIPI). The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page at (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the TN8412AP Server IP Interface (SIPI) circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN8412AP SIPI circuit pack.

If necessary, upgrade the firmware on the just installed TN8412AP Server IP Interface (SIPI) circuit pack that you just installed. For more information, see Upgrading firmware on page 187.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)

- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see Upgrading firmware on page 187.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Chapter 3: Migrating to an Avaya S8500C and S8510 Server

This chapter describes how to migrate from existing DEFINITY systems to the Avaya S8500C and S8510 Server.

The most common migrations are from non-Linux-based systems to Linux-based servers. Non-Linux-based systems include systems such as the DEFINITY ONE/S8100. Less common migrations include migrations from one Linux-based server to another. Not all non-Linux-based systems can migrate to a Linux-based server. Whether you can migrate a system depends on the supported migration path. A *migration path* refers to the platform and the software release from which you can migrate to the new platform.

Important:
S8500A Servers are not supported on Communication Manager 5.x and later releases. Refer to the table of Server Migration Paths on page 50 for possible migrations that include Communication Manager Release 5.2.

Migrations from existing DEFINITY and Linux platforms

Use these procedures to migrate from existing DEFINITY systems to the Avaya S8510 Server with limited out-of-service time. The existing systems must be standard reliability and direct connect. You cannot migrate systems that use a center stage switch (CSS) or asynchronous transfer mode (ATM). In all instances, the cabinets can be reused as port networks (PNs). You do not need a G650 Media Gateway. However, you can add a G650 Media Gateway PN if the existing system has only one or two port networks.

You can migrate the following existing systems:

- DEFINITY Server SI in a single carrier cabinet (SCC) or multicarrier cabinet (MCC). You can migrate only the Direct-Connect configurations
- DEFINITY Server CSI in a compact modular cabinet (CMC). You can migrate only the IP-PNC configurations
- DEFINITY ONE in a CMC1 Media Gateway. You can migrate only the IP-PNC configurations
- Avaya IP600/S8100 in a G600. You can migrate only the IP-PNC configurations

Hardware migrations

This information in this section is based on the assumption that the server complex is installed, configured, and operational.

DEFINITY Server SI in an MCC

When you migrate an existing DEFINITY Server SI in a multicarrier cabinet (MCC), you use one TN2312BP IPSI circuit pack to control from one to three port networks (PNs). Avaya recommends that you install the IPSI in the A carrier in the existing processor port network (PPN) instead of in one of the expansion port networks (EPNs). But before you install the IPSI, you must convert the PPN to a PN. This process requires that you:

- Replace the processor control carrier with an expansion control carrier.
- Remove all the control circuit packs.

This migration affects service because you must be turn off the carrier. Before you turn off the cabinet, you must perform some premigration administration.

DEFINITY Server SI in an SCC

When you migrate an existing DEFINITY Server SI in a single carrier cabinet (SCC), you use one TN2312BP IPSI circuit pack to control from one to three PNs. Avaya recommends that you install the IPSI in the cabinet in the A position in the existing PPN instead of in one of the EPNs. But before installing the IPSI, you must convert the PPN to a PN. This process requires that you:

- Replace the processor control cabinet with an expansion control cabinet.
- Remove all the control circuit packs.

This migration affects service because you must turn off the PPN stack to replace the cabinet. Before turning off the cabinets, you must perform some premigration administration.

DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway

When you migrate an existing DEFINITY Server CSI or DEFINITY ONE in a compact modular cabinet (CMC), you use one TN2312BP IPSI circuit pack to control the PN. If a CSI, you replace the TN2182 Tone Clock circuit pack with the IPSI which you install in the A position of the cabinet. You also must remove the processor circuit pack. If a DEFINITY ONE, you replace the processor circuit pack with the IPSI.

This migration affects service because you must turn off the CMC1 Media Gateways to replace the processor and the tone clock circuit packs. Before you turn off the cabinets, you must perform some premigration administration.

Avaya IP600/S8100 in a G600

When you migrate an existing Avaya IP600, you use one TN2312BP IPSI circuit pack to control the PN. You also must replace the processor circuit pack with the IPSI which you can install in the A position of the cabinet.

This migration affects service because you must turn off the IP600 chassis to replace the processor. Before you turn off the chassis, you must perform some premigration administration.

Migration modules

This chapter describes the following types of migrations:

- Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8500-Series Server on page 189
- Migrating a DEFINITY ONE/S8100 to an S8500-Series Server on page 217
- Migrating an Avaya IP600/S8100 to an S8500-Series Server on page 247
- Migrating an Avaya S8500A or S8500B Server to an S8500C or S8510 Server on page 281

Migrating from a DEFINITY Server CSI in a CMC1 Media Gateway (Xmodem)

Use these procedures to migrate from an existing DEFINITY Server CSI in a Compact Modular Cabinet (CMC) with a linear flash to an Avaya S8400 Server that uses Xmodem. This procedure supports a migration to Communication Manager Release 5.x.

When you migrate an existing DEFINITY Server CSI in a CMC1 Media Gateway, you use one TN8412AP S8400 IP Interface (SIPI) circuit pack to control the one port network (PN). You must replace the TN2182 Tone Clock circuit pack with the TN8412AP Server IP Interface (SIPI) circuit pack. You also must replace the TN798B Processor circuit pack.

This migration affects service because you must turn off the CSI chassis to replace the processor and tone-clock circuit packs.

Migration paths

Avaya supports the following migrations of a DEFINITY Server CSI in a CMC1 Media Gateway to the S8400 Server configuration:

- DEFINITY Release 8 and later

To migrate, you can use the existing translations. One supported method to move translations from legacy systems is to:

1. Copy the translations using Xmodem.
2. Copy the translation files to the S8400 Server.

Checklists

Before you go on site, perform the following tasks

:

✓	Task	Description
	Verify that your Services laptop has the appropriate hardware.	Correct hardware components include: ● 40 MB available disk space ● direct Ethernet cable ● serial cable and adapter ● RS-232 port connector ● Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● CD-ROM drive
	Verify that your Services laptop has the appropriate software.	Correct software components include: ● Windows 2000/XP operating system ● Terminal emulation program: HyperTerminal or other ● TCP/IP networking software: bundled with Windows OS ● Web browser: Internet Explorer 5.0 or later
	Obtain appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media Gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the equipment of the customer.
	Obtain the serial number of the Servers, if necessary.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD with the current software and firmware.	You use this CD to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware available.	The following firmware are on the software CD: • IPSI or TN8412AP Server IP Interfaces (SIPI) • C-LAN • MedPro • VAL circuit packs For the most current versions, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download license and authentication files to your Services laptop.	New license and authentication files are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557 and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed as well as any changes to the system alarming configuration. ART is available only to Avaya associates. Business Partners can call 800-295-0099.
	Verify that you have copied all necessary files to your computer	These files can include: ● service packs ● license file ● authentication file ● firmware for programmable circuit packs
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

For more information, see Migration paths on page 157.

To migrate from a DEFINITY system, you must complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. Remote or on-site ASG access is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Presite migration checklist

Before you go on site, perform the following tasks in Table 7:

Table 7: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks before you start the migration:

✓	Task	Description
	Verify that you have the correct cables for the TN8412AP S8400 Internet Protocol Interface (SIPI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see *Installing and Configuring the Avaya S8400 Media Server* (03-300678).

When you are migrating from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.

Documentation checklist for migrations

For a list of documents that are needed to perform the migration, see Resources on page 35.

✓	Document	Description
	Quick Start for Hardware Migration: Avaya S8400 Media Server in an Avaya CMC1 or G600 Media Gateway (03-300706)	A quick reference guide that provides physical installation and connection information.
	Installing and Configuring the Avaya S8400 Media Server (03-300678)	Provides installation instructions for the S8400 Server.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.

Performing a migration

CAUTION:

This migration affects service because you must turn off the CMC1 Media Gateway to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

Note:

You must install the new Communication Manager license file on the server before you make the change. The TN8412AP Server IP Interface (SIPI) serial number can be used for licensing purposes.

Premigration administration

This migration is a service-affecting event. The CMCs must be turned off to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

Connecting to the processor

To connect to the processor:

1. Connect the computer that you use to access the cabinet.
2. Start a SAT session using Native Configuration Manager or Avaya Site Administration.
3. Log in as **craft**.

Removing netcon data modules

To remove Netcon data module information:

1. Type **`list data module`**. Press **Enter**.
2. Notice if the system contains any Netcon circuit packs.

   If there are Netcon data modules, continue to step 3.

   If there are no Netcon data modules, continue to Saving translations on page 355.
3. Type **`list user ext`** ***`x`***. Press **Enter** where ***`x`*** shows who is using the associated Netcon data module.

```
list usage extension 2501
                              LIST USAGE REPORT

    Used By
    Hunt Group           Group Number           99               Member 1



Command successfully completed
```

   For example, the screen in step 3 shows the extension 2501 is being used on Hunt Group 99.
4. Type **`change hunt-group`** ***`xx`***. Press **Enter** where ***`xx`*** is the hunt group number.
5. In the **Hunt Group** screen, press the space bar to highlight the information. Press **Return** to remove the information.
6. Repeat for each extension.
7. When you finish, press **Submit**.
8. Repeat for each listing.
9. Type **`remove data-module`** ***`xxxx`***. Press **Submit** where ***`xxxx`*** is the extension to be removed.
10. Repeat for all items listed on the **`list data module`** command.

Saving translations

This step is important in case you need to back out of the migration.

To save translations:

Note:

Save translations to a flash card.

1. Plug the PCMCIA/Compact Flash adapter in the PCMCIA slot on the TN798B or TN2402 Processor circuit pack.
2. Type **`save translation`**. Press **Enter** to save the translations to the PCMCIA.

   The system displays a **Command successfully completed** message or an error message.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:

   a. **`list configuration all`**

   b. **`list trunk-group`**

   c. **`list hunt-group`**

   If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.

2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Migration tasks

You can reuse the translations from the current system when you migrate to an S8400 Server.

Note:

You must install the new Communication Manager license file on the server before you make the change. The TN8412AP Server IP Interface (SIPI) serial number can be used for licensing purposes.

Perform these tasks to convert a processor port network to a port network (CMC).

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

The TN8400BP Server circuit pack replaces the TN798 or TN2402 Processor circuit pack. The TN798 and TN2402 circuit packs do not have the Communication Manager Messaging feature. You must return the current processor circuit pack to Avaya.

Connecting to the SAT

To do connect to the System Administration Terminal (SAT):

1. Connect the Services laptop modem to an analog line.
2. On the Services laptop, click **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal**.
3. In the **Connect To** window, fill in the appropriate data and click **OK**.
4. In the **Connect** window, verify the information and click **Dial**.
5. At the login prompt, type **`craft`** and the password and press **Enter**.
6. For the Terminal Type, type **`VT220`** and press **Enter**.

   You now are logged in to the SAT.

Copying translation files

To do copy the translation files:

1. On the SAT, type **`upload trans`** and press **Enter**.
2. Click **Transfer** > **Receive File**.
3. In the **Place received file in the following folder** field, enter the location where the translation files are to be placed.
4. In the **Use receiving protocol** field, select **Xmodem** and click **Receive**.
5. In the **Receive Filename** window, in the file name field, type in a file name and click **OK**.
6. In **Xmodem file to receive** window, in the **Error checking** field, CRC is shown and attempts to upload the files three times and fails.

   CRC then changes to Checksum and Xmodem starts the upload.

   When the system finishes, the file is located in the directory designated in step 3.

Turning off power to all cabinets

CAUTION:
Ensure that you have done the premigration administration. For more information, see Premigration administration on page 257.

To turn off power to all cabinets:

- Turn off the power to each cabinet.

Removing circuit packs

To remove circuit packs from the CMC1 Media Gateway:

1. Remove the TN798B or TN2402 Processor circuit pack from slot A01.
2. Remove the TN2182 Tone Clock circuit pack from slot A02.
3. Remove the TN767 DS1 Interface circuit pack, if installed.
4. Remove the TN2207 DS1 Interface circuit pack, if installed.
5. Remove the TN2313 DS1 Interface circuit pack, if installed.

Inserting circuit packs

To install circuit packs into the CMC1 Media Gateway:

1. Install the TN8412AP S8400 IP Interface (SIPI) circuit pack into slot A02.
2. Install the TN8400BP Media Server circuit pack into slot A01.
3. If the system had a TN767, TN2207, or TN2313 DS1 Interface circuit pack, install the TN464HP DSD1 Interface circuit pack in any open slot.

Connecting cables

To connect cables:

1. On the rear of the carrier, connect the server cable adapter into port 1 on the rear of the TN8400BP Media Server circuit pack.
2. Connect the amphenol connector into slot A02 on the rear of the TN8412AP SIPI circuit pack.
3. Connect the customer LAN cable into the port labeled ETH-B on the adapter in slot A01.
4. Connect the IPSI cable into the port labeled ETH-A on the adapter in slot A01.
5. Connect the other end of the IPSI cable to the amphenol connector in slot A02.
6. Connect the power plug on the DVD drive to a wall outlet.
7. Connect the USB DVD drive to the USB port on the faceplate of the TN8400BP Media Server circuit pack.
8. On the DVD drive, ensure that the on/off/ext switch is in the **EXT** position.
9. Insert the Communication Manager CD into the USB DVD drive.
10. Connect the Services laptop to the Services port on the front of the TN8400BP Media Server circuit pack.
11. Turn on the power to all cabinets.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test

You can install a TN771 Maintenance/Test circuit pack in any slot other than slots A01 and A02. Avaya recommends one TN771 Maintenance/Test circuit pack per location for the following conditions:

- There are three or more G650, G600, or CMC1 Media Gateways in the S8400 system. Do not include G150 and H.248 Media Gateways in this count, and
- There are IP endpoints or ISDN endpoints. These endpoints consist of:
  - BRI trunks
  - PRI trunks
  - BRI stations

The TN8412AP S8400 IP Interface (SIPI) circuit pack provides all maintenance functions that were present on the TN798 or TN2402 Processor circuit pack. This carrier does not have a TN775 Maintenance (EPN) dedicated slot.

Translation migrations

This section describes how to migrate the translation files from the current system to the S8400 Server.

Installing the software load

For more information on installing software loads, see *Installing and Configuring the Avaya S8400 Media Server*, 03-300678.

To install the software load:

1. Power down the server.
2. Connect the USB CD/DVD drive to the S8400 Server.
3. Connect the laptop to the Services port on the faceplate of the server using a crossover cable.
4. Power up the server.
5. From the Services laptop, click **Start** > **Run** to open the **Run** window.

6. Type **`ping -t 192.11.13.6`**. Press **Enter** to indicate when the Services port is responding.
7. From the laptop Start menu, click **Start** > **Run**.
8. In the **Run** dialog box, type **`telnet 192.11.13.6`**. Press **Enter** to view the first screen.

Note:

To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

9. Select **Install**, ensure that OK is highlighted and press **Enter**.

10. On the **Select Release Version** window, ensure that the Build line and <OK> are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

    Once the drive is properly configured, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

    These processes can take up to 20 minutes. When the system finishes the software installation, the server reboots and the CD/DVD-ROM drive opens. You must remove the CD from the drive at this time.

    The reboot can take up to 3 minutes. The telnet session drops automatically.

11. Open a Web browser.
12. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
13. Log in as **craft** or **dadmin**.

Configuring the server

For more information on configuring the server and the use of the Avaya Installation Wizard, see *Installing and Configuring the Avaya S8400 Media Server*, 03-300678.

To configure the server:

1. Open a Web browser.
2. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.
4. Access **System Management Interface (SMI)** click **Administration** > **Server (Maintenance)**
5. Under Server, click **Server Date/Time**.
6. In the **Server Date/Time** window, verify the data and time are correct. If the date and time are incorrect:
   a. Enter the date
   b. Enter the time
   c. Select the time zone
   d. Click **Submit**:

   Important:
   It is necessary to reboot the server to initialize server settings that are restored but not yet activated. See Reboot the server on page 301.

   CAUTION:
   Not rebooting the server will lead to erroneous behavior surrounding the time of day at daylight-saving-time transition.
7. Under Server Configuration, click **Configure Server**.

   The system starts the Configure Server Wizard.
8. In the **Review Notices** window, click **Continue**.
9. In the **Back Up Data** window, click **Continue**.
10. Select **Configure all services using the wizard** and click **Continue**.

    Note:
    You can set up servers to various configurations. The following steps provide a general outline of required steps to complete the configuration.
11. In the **Server Role** window, as shown in Figure 9, choose between Main, ESS or LSP depending on the platform on which the wizard is running.
12. In the **Set Identities** window, perform the following steps:
    - In the **Host Name** field, enter a unique name for the server.
    - In the **ID** field, enter as required or accept the default.
    - In the **CNA** field, enter as required or accept the default.

- In the **Enterprise LAN** field, enter as required or accept the default.
- In the **Assign the Processor Ethernet to an Interface** area, select one as required.

13. Click **Continue**.
14. In the **Configure Ethernet Interfaces** window, set up as required. Click **Continue**.
15. In the **Ethernet Adjuncts** window, set up as required. Click **Continue**.
16. In the **External DNS Server Configuration** window, set up as required. Click **Continue**.
17. In the **Static Network Routes (Optional)** window, set up as required. Click **Continue**.
18. In the **Configure Time Server** window, set up as required. Click **Continue**.
19. In the **Set Modem Interface** window, set up as required. Click **Continue**.
20. In the **Configure Maintenance Processor Complex (MPC)** window, set up as required and click **Continue** to configure the server.

Figure 9: Configure Server - Server Role

Installing the license and authentication file

To install the Communication Manager license file and the Avaya authentication file:

1. Open a Web browser.
2. In the **Address** field, type **`http://192.11.13.6`**. Press **Enter** to access the login Web page.
3. Log in as **craft** or **dadmin**.

4. Under Miscellaneous, click **Download Files**.
5. Click **Browse** and select the file saved on the Services laptop.
6. Click **Download** to place the file on the server.
7. Under Security, click **License File**.

   The system displays the **License File** screen.
8. Select **Install the license file I previously downloaded** and click **Submit**.

   The system tells you the license file is installed successfully.
9. Under Security, click **Authentication File**.

   The system displays the **Authentication File** screen.
10. Select **Install the Authentication file I previously downloaded** and click **Install**.

    The system tells you the authentication is installed successfully.

Copying translation files to the server

To copy translation files to the S8400 Server:

1. Open a Web browser.
2. Use **System Management Interface (SMI)**.
3. Under Miscellaneous, click **Download Files**.
4. Select **Files to download from the machine I'm using to connect to the server**.
5. Click **Browse** and select the translation file saved on the Services laptop and click **Download**. A translation file example might be C:\Program Files\PCCsixln.

   The file is placed in the /var/home/ftp/pub directory of the S8400 Server.
6. Click **Start** > **Run** to open the **Run** window.
7. Type **`telnet 192.11.13.6`**. Click **OK** to telnet in to the Services port on the TN8412AP SIPI circuit pack.
8. Log in as **craft** or **dadmin**.
9. From the /var/home/ftp/pub directory, type **`read_csi_xmod -f`** ***`filename`***. Press **Enter** where ***`filename`*** in this example is CsiXln.

   The system renames the translation files as xln1 and xln2.

   If the read_csi_xln process fails, you get an error message with the reason for the failure. If that happens, the translation file is not restored. Resolve the reason for the failure and restart the process.

10. Type **`cd /etc/opt/defty`**. Press **Enter**.
11. Type **`ls -ltr`**. Press **Enter**.

    Verify that the xln1 and xln2 files are not zero length.
12. Open a SAT session.
13. Type **`reset system 4`**. Press **Enter** to load the restored translations into memory.

Closing all sessions

To close all sessions:

1. From the HyperTerminal window, when the upload finishes

   The system displays a **Command successfully completed** message or an error message.
2. Type **`logoff`** and press **Enter**.

Post-migration administration

This section describes the post-migration administration to complete the migration to the S8400 Server.

Important:

When you format the compact flash card for use in the S8400 Server, all data is erased from the compact flash card.

Note:

Do not use the compact flash card (Comcode 700381841) in an S8100 Windows system. The operation system does not recognize the compact flash card.

After the migration, you can format the compact flash card (Comcode 700381841) for the S8400 Server and use the compact flash card as the backup compact flash card.

Assigning IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs

When you use static IP addressing, you must assign IP addresses to the TN8412AP Server IP Interface (SIPI) circuit packs.

Using static addressing

You can administer static IP addresses for the TN8412AP Server IP Interface (SIPI) circuit packs. You administer the addresses directly through the Ethernet port connection on the TN8412AP Server IP Interface (SIPI) faceplate (top port). For more information, see Figure 10: Connecting directly to the SIPI on page 180.

Figure 10: Connecting directly to the SIPI

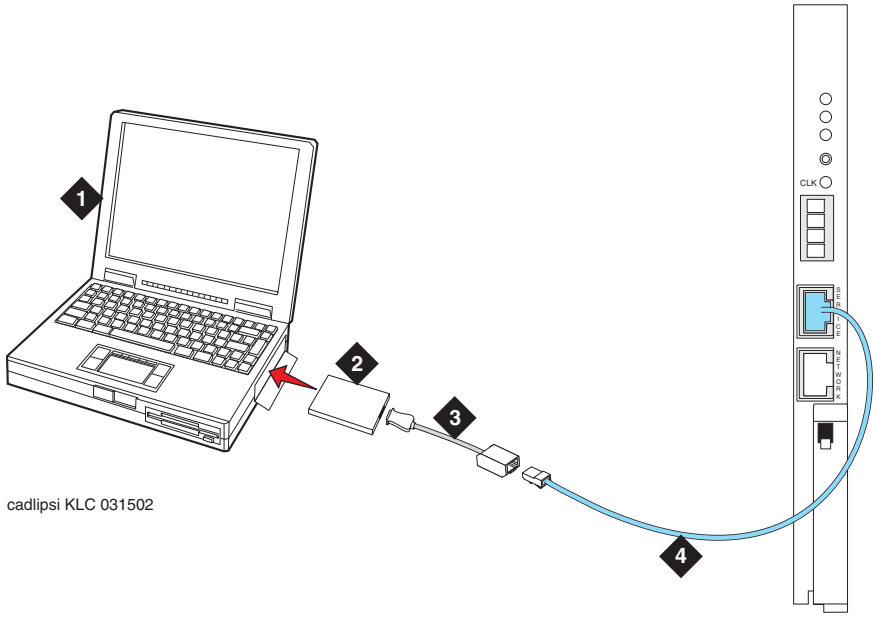


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 crossover cable to SIPI**

Note:

Ensure that you have the password before proceeding.

Logging in to the TN8412AP Server IP Interface (SIPI)

To log in to the TN8412AP Server IP Interface (SIPI):

1. Type **`telnet 192.11.13.6`**. Press **Enter** to open the Telnet window and connect to the TN8412AP Server IP Interface (SIPI)

   Prompt = [IPSI]:

   Note:

   While connected to the TN8412AP Server IP Interface (SIPI), type **`help`** or **`?`** to obtain online help. Most commands have two or three letter abbreviations.

2. Type **`ipsilogin`**. Press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login used on the TN8412AP Server IP Interface (SIPI) has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`**. Press **Enter**.
2. Type **`show port 1`**. Press **Enter** to see the current settings.

3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnet mask. Press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) session.
5. Telnet to **192.11.13.6** and login.
6. Enter **`show control interface`**.
   The system displays the IP address, subnet mask, and default gateway information. Verify that the proper information was entered.
7. If a default gateway is used, enter the gateway IP address with **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway.
8. Enter **`quit`** to save the changes and exit the TN8412AP Server IP Interface (SIPI) or IPSI session.
9. Telnet to **192.11.13.6** and login.
10. Use **`show control interface`** to verify the administration.
11. Type **`exit`**. Press **Enter** to see the changes.

Resetting the TN8412AP Server IP Interface (SIPI)

To reset the TN8412AP Server IP Interface (SIPI):

1. Type **`reset`**. Press **Enter**
   Answer **Y** to the warning.

   Note:

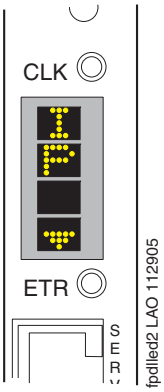
   Resetting the TN8412AP Server IP Interface (SIPI) terminates the administration session. If further administration is required, start a new telnet session to the TN8412AP Server IP Interface (SIPI).

   Note:

   Control network settings become effective when you exit the IPADMIN session. Control settings include the IP address, the subnet mask, and the gateway.

2. Disconnect the Services laptop from the faceplate.
3. Check the LCD. Verify that it has an I P with a filled-in V that shows at the bottom. For more information, see Figure 11.

Figure 11: LED display that shows that the SIPI has a static IP address



Note:

Clear the ARP cache on the laptop before connecting to another TN8412AP Server IP Interface (SIPI). If the cache is not cleared, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

4. Close the window.

Enabling control of the TN8412AP Server IP Interface (SIPI)

To enable control of the TN8412AP Server IP Interface (SIPI):

Note:

Ensure that the TN8412P SIPI has the current firmware.

CAUTION:

This procedure allows the server to take control of the TN8412AP Server IP Interface (SIPI)-controlled port network. Failure to complete the procedure correctly can result in no connection to the network.

1. Type **`add cabinet 1`**. Press **Enter**.
2. Administer the appropriate cabinet type and carriers.
3. Type **`add ipserver-interface 1`** where **`1`** means port network. Press **Enter**.
4. In the **Host** field, type in the IP address that was programmed into the TN8412AP Server IP Interface (SIPI). Press **Enter**.
5. Type **`save translation`**. Press **Enter**.
6. Type **`change system ipserver-interface`**. Press **Enter**.
7. In the **IPSI Control of Port Networks** field, type **`enabled`**. Press **Enter**.
8. Type **`save translation`**. Press **Enter**.
9. Verify the translation migration was successful.

   Place test calls, verify trunk status (if applicable), and so forth.

   The server now controls all the port networks.

Verifying TN8412AP Server IP Interface (SIPI) translations

To verify TN8412AP Server IP Interface (SIPI) translations:

1. Type **`list ipserver-interface`**. Press **Enter**.
2. Verify that the TN8412AP Server IP Interface (SIPI) circuit pack(s) is translated.

Verifying TN8412AP Server IP Interface (SIPI) connectivity

To verify TN8412AP Server IP Interface (SIPI) connectivity:

1. Start a Web browser.
2. Under Diagnostics, click **Ping**.
3. Under Endpoints to Ping, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Type the correct cabinet and carrier numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each TN8412AP S8400 IP Interface (SIPI) circuit pack must be on the most current and same firmware load. You might need to upgrade the firmware on the TN8412AP Server IP Interface (SIPI). The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page at (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the TN8412AP Server IP Interface (SIPI) circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN8412AP SIPI circuit pack.

If necessary, upgrade the firmware on the just installed TN8412AP Server IP Interface (SIPI) circuit pack that you just installed. For more information, see Upgrading firmware on page 187.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see Upgrading firmware on page 187.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8500-Series Server

Use these procedures to migrate from an existing DEFINITY Server CSI in a compact modular cabinet (CMC) system to the Avaya S8500-Series Server with an IP-port network connectivity (PNC) configuration. The existing systems must be standard reliability. In all instances, the cabinets can be reused as port networks. However, you can add a G650 Media Gateway port network if the existing system has a port network. This procedure supports a migration to Communication Manager Release 5.x.

To migrate an existing DEFINITY Server CSI in a CMC1 Media Gateway, you use one TN2312BP IPSI circuit pack to control the one port network (PN). You must remove the TN2182 Tone Clock circuit pack and install an IPSI circuit pack in the A position. You also must remove the processor circuit pack.

This migration affects service because you must turn off the CMCs to replace the processor and tone-clock circuit packs.

Important:
S8500A Servers are not supported on Communication Manager 5.0 and later releases. Refer to the table of Server Migration Paths on page 50 for possible migrations that include Communication Manager release 5.2.

Migration paths

Avaya supports the following migrations of a DEFINITY Server CSI in a CMC1 Media Gateway to the S8510 Server IP-PNC configuration:

- DEFINITY Release 5 through Release 10
- MultiVantage Release 11 and 1.x
- Communication Manager Release 2.0 through Release 3.1.2

Checklists

Before you go on site, perform the following tasks:

:

✓	Task	Description
	Verify that the correct hardware is installed on your Services laptop.	Correct hardware components include: ● 40 MB available disk space ● A direct Ethernet cable ● A serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● A CD-ROM drive
	Verify that the correct software is installed on your Services laptop.	Correct software includes: ● Windows 2000 or Windows 2000/XP operating system ● HyperTerminal or another terminal emulation program ● TCP/IP networking software that is bundled with the Windows OS ● Internet Explorer 5.0 or later
	Obtain the appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the logins and the passwords that you might need for the equipment of the customer.
	Obtain the serial number.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file and authentication file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	Use this CD-ROM to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware.	The following firmware is on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs **Important:** Firmware is upgraded often. To ensure that you have the latest version, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop.	New license file and authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	For DEFINITY systems only: Verify that you have the required, customer-provided network information. Obtain a completed *Electronic Preinstallation Worksheet (EPW)*.	The EPW is an Excel spreadsheet that provides the information about the network. You need this information to configure the control network components with the Avaya Installation Wizard. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard Web site.
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

For more information, see Migration paths on page 189.

When you are migrating from a DEFINITY system, complete the following additional tasks before starting the migration:

✓	Task	Description
	About 2 weeks before the migration, freeze the translations. Use a spare flash card to collect the translations locally.	For more information on where and how to send the translations, contact the STS scheduling desk at 720-444-9418. STS updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For forms and more information, contact the STS scheduling desk at 720-444-9418.
	About 2 business days before the migration, create a trouble ticket to contact the STARS team.	Whenever an S8x00 server is upgraded from 1.x.x to 2.x.x and a new authentication file is requested, ASG access (remote and on-site) is impacted. You need assistance from the Service Tools and Application Remote Support (STARS) team to ensure successful ASG access before and after the upgrade. To contact the STARS team, use http://stars.avaya.com/ticket/requests/request.asp
	Mark the ticket status as CRITICAL.	Indicate text in the ticket to notify the STARS team that you are upgrading an S8x00 server. Include the date of the upgrade and the FL and product or alarm ID of the system. The STARS team contacts you on how to access your product before and after the upgrade. A temporary ASG product ID is created for you and your team to use for access during the time of the upgrade.
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.

✓	Task	Description
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.
	Copy the translation file from STS to a directory on the Services laptop.	File size is usually in the range of 1-4 megabytes.

2 of 2

Presite migration checklist

Before you go on site, perform the following tasks in Table 8:

Table 8: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site for a migration from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	The customer supplies an open EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack. Verify that this rack is installed correctly.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on how to install the rail, see the documentation that comes with the rail kit.
	Verify that you have the license file that the file includes the licensed features.	Use the License File link on the System Management Interface (SMI) to verify.
	Verify that you have the Avaya Authentication File (if not installed with AIW) on page 300.	Use the Authentication File link on the System Management Interface (SMI) to verify.

Documentation checklist for migrations

For a list of documents that Avaya recommends you have on hand for the migration, see Resources on page 35.

You also need the following additional documentation:

✓	Task	Description
	Quick Start for Hardware Installation: Avaya S8500 Server (555-245-701)	A quick reference guide that provides physical installation and connection information.
	Installing and Configuring the Avaya S8500-Series Server (03-300143)	Provides installation instructions for the S8500 Server.
	Installing the Avaya S8510 Server Family and Its Components, 03-602918.	Provides installation instructions for the S8510 Server Family and Its Components
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.

Performing a migration

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

CAUTION:

This migration affects service. When the Definity One/S8100 is turned off, the system drops all calls. Service returns when the server takes control of the IPSIs.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Premigration administration

This migration is a service-affecting event. The CMCs must be turned off to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

Connecting to the processor

To connect to the processor:

1. Connect the computer that you use to access the cabinet.
2. Start a SAT session using Native Configuration Manager or Avaya Site Administration.
3. Log in as **craft**.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:
   a. **`list configuration all`**
   b. **`list trunk-group`**
   c. **`list hunt-group`**

   If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.
2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

Although the migrated translations are already copied to the server, you must save the translations in case you need to back out of the migration.

Note:

Save translations to a flash card.

To save translations:

1. To save translations to the system disk, type **`save translation`**. Press **Enter**.

   Either a **Command successfully completed** The message displays or all error messages are logged.

Translation migration

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Copying translation files to server

To copy translation files to the server:

1. Under Miscellaneous, click **Download Files**.
2. Click **Files(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** and select the file saved on the services laptop.
4. Click **Download** to place the file on the server.

Restoring translation files

To restore translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Local Directory** and click **View**. The field automatically shows the default directory.
3. Select the translation file.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.
5. Click **Restore** to restore the translation files.
6. Click **Restore Status**.
7. Select the first file and then scroll down and click **Review Status** to see the results of the restore.

   When the restore process completes, the screen displays **Restore is finished**.
8. Use Native Configuration Manager or Avaya Site Administration to start a SAT session.
9. Type **`reset system 4`**. Press **Enter** to load the restored translations.

If the restore process fails, the system displays an error message that states the reason for the failure. The translation file is not restored. You must resolve the reason for the failure and restart the process.

Administering the IPSIs

To administer the IPSIs:

1. Type **`change system-parameters ipserver-interface`**. Press **Enter**
2. Verify that the **Primary Control Subnet Address** field is correct.

   The subnet address must match the most significant three octets (the first three groups of digits in the subnet address) of the server IP address that is listed on the control network entry from the completed Electronic Preinstallation Worksheet (EPW).

   An asterisk (*****) to the right of the **Subnet Address** field means that although a subnet address displays, this address is incorrect. Communication Manager does not have the subnet information. After you verify the information shown on the screen, submit this form with or without changes to update the Communication Manager with the correct subnet information.

CAUTION:

If the information in the **Primary Control Subnet Address** field is incorrect, you must change the information on the server. Use the System Management Interface (SMI) and access **Installation > Configure Server** to change the server configuration. Then continue with step 3 of this procedure.

3. Verify that the **Switch Identifier** field is set correctly for this installation. You must enter the correct switch identifier here before you administer the TN2312 IPSI circuit packs.
4. Verify that the **IPSI Control of Port Networks** field is set to **disabled**.
5. Press **Enter**.

Adding IPSI translations to Communication Manager

To add IPSI translations to Communication Manager:

1. Type **`add ipserver-interface 1`**. Press **Enter** to add the IPSI circuit pack information.
2. If you use static addressing, in the **Host** field, type the IP address for the IPSI that is in the port network listed in the **Location** field.
3. Verify that the **IP Control** field is set to **y**.
4. Verify that all the other fields are populated.
5. Press **Enter** to put the changes into effect.
6. Repeat Steps 1 through 5 for each IPSI.

Setting the alarm activation level

To set the alarm activation level:

1. Type **`change system-parameters maintenance`** and press **Enter**.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that the customer wants. The default is **none**.

Backing up translations

To back up translations:

1. Under Data Backup/Restore, click **Backup Now**.
2. Select the data sets and the backup method.

   If you select **Save ACP translations prior to backup**, the server automatically saves the translations to the hard drive before the server saves the translations to the backup media.
3. Click **Start Backup** to begin the backup process.

Migration tasks

You can reuse the translations from the existing system when you migrate to an S8500-Series Server.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

The TN798 circuit pack or the TN2402 Processor circuit pack that contains the Audix feature is replaced with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that does not have the Audix feature. You must return the existing processor circuit pack to Avaya.

Note:

Customers also must add an ED-1E568-70G1 DEFINITY Audix Slim board and a TN2501AP Voice Announcement over LAN (VAL) circuit pack for announcements.

Changing the control cabinet to a port network

To change the control cabinet to a port network (PN):

1. Remove the TN798 or the TN2402 Processor circuit pack.
2. Replace the TN2182 Tone Clock circuit pack with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack.
3. Connect a CAT5 straight-through cable from the IPSI to the server through the customer network.

   Note:

   If you replace a TN795 Processor circuit pack, you might not need the TN744D/E Call Classifier-Detector circuit pack. The TN2312BP IPSI circuit pack has call classifier functionality. However, increased voice and data traffic can require the TN744D/E Call Classifier-Detector circuit pack.

   Note:

   If you have a TN799C or earlier C-LAN circuit pack, you must replace the circuit pack with a TN799DP C-LAN circuit pack.

Turning off the power to the control cabinet

CAUTION:

Ensure that you have completed the premigration administration. If you do not perform the premigration administration, the system will not function. For more information, see Premigration administration on page 226.

To turn off power to the control cabinet:

1. On the faceplate of the processor, press and hold the shutdown button until the shutdown process starts.

   When you see the green light the system is shut down.

DANGER:

The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the cabinet, pull the AC power cord from the back of the cabinet.

2. Unplug the power cord from the back of the cabinet to turn off the cabinet.

Replacing the processor circuit pack

To replace the processor circuit pack:

1. Remove the entire processor circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Remove the TN2182 Tone Clock circuit pack.
4. Remove the octopus cable from the connector that is associated with slot 2 on the connector panel.
5. Install the IPSI adapter to the connector that is associated with slot 2 on the connector panel.
6. Install the maintenance cable onto the 9-pin D-sub connector on the adapter. This cable is for emergency transfer and "auxsig" signal.

   Note:

   The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack takes only one slot.

7. Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit pack into slot 2.
8. Attach the new label above the circuit pack slots.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.

3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test circuit pack

You must replace the TN795 or the TN2412 circuit pack with a TN771 Maintenance/Test circuit pack. Each location must have one TN771 Maintenance/Test circuit pack.

To install the TN771 Maintenance/Test circuit pack:

- Install the TN771 circuit pack in slot 1.

  This carrier does not have a dedicated slot for the TN775 Maintenance (EPN) circuit pack.

Connecting the IPSI to the network

After connecting to the server, power up the CMC1 cabinets:

1. Connect one end of the green CAT5 straight-through cable to the Ethernet switch on the customer network.
2. Connect the other end of the cable to the IPSI adapter on the back of the media gateway.

Postmigration administration

Perform the following tasks to complete postmigration administration.

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 12: Connecting directly to the IPSI on page 207).

Figure 12: Connecting directly to the IPSI

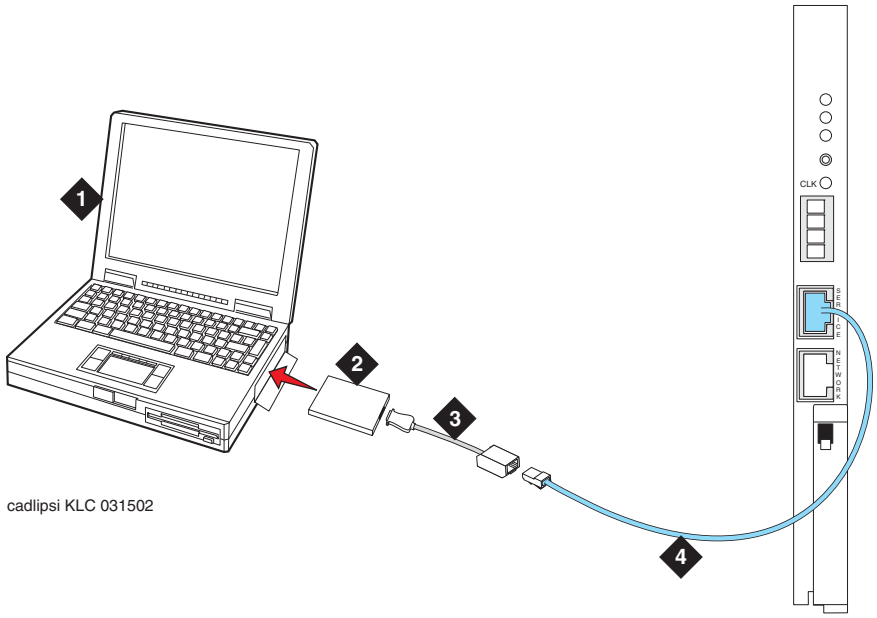


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application on the service laptop to access the server (192.11.13.6 port 22).

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.

2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`** and press **Enter**.
2. To see the current settings, type **`show port 1`** and press **Enter**.

3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Verify that the correct information was entered.
5. If a default gateway is used, enter the gateway IP address.
   Type **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway and press **Enter**.
6. To save the changes and exit the IPSI session, type **`quit`** and press **Enter**.
7. SSH to **192.11.13.6** and log in.
8. To verify the administration, type **`show control interface`** and press **Enter**.
9. To see the changes, type **`exit`** and press **Enter**.

Setting the VLAN and diffserv parameters

To set the VLAN parameters and the diffserver parameters:

1. Log back in as **`craft`**.
2. To display the quality of service values, type **`show qos`** and press **Enter**.
3. If necessary, use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

Note:

Use **Help** to obtain syntax guidelines for these commands.

- Type **`set vlan priority 6`**
- Type **`set diffserv 46`**
- Type **`set vlan tag on`**
- Type **`set port negotiation 1 disable`**
- Type **`set port duplex 1 full`**
- Type **`set port speed 1 100`**

4. To check the administered values, type **`show qos`** and press **Enter**.
5. To exit, type **`quit`**. Press **Enter**.

Important:

Ensure that the port settings on the Ethernet switches are set to the same values as shown in the **`set port`** commands in step 3.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

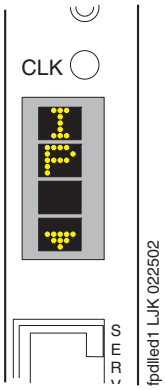
   Note:

   Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

   Note:

   The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.
2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 13).

Figure 13: LED display that shows that the IPSI has a static IP address



4. Repeat steps 1 through 3 for each IPSI circuit pack.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "1" shows in any position, you must troubleshoot the problem.

   Tip:

   The pattern `0.1.1.0` usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.

2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct cabinet and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Enabling control of the IPSI

To enable control of the IPSI:

Note:
Ensure that the IPSI has the same, current firmware.

CAUTION:
This procedure allows the server to take control of the IPSI-controlled port network(s). Failure to complete the steps correctly can result in no connection to the network.

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Set the **IPSI Control of Port Networks:** field to **enabled**
3. Press **Enter** to effect the change.
4. Type **`save translation`** and press **Enter**.

   The server now controls all the port networks.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating a DEFINITY ONE/S8100 to an S8500-Series Server

Important:
The S8500A Server is not supported on Communication Manager 5.0 and later releases. Refer to the table of Server Migration Paths on page 50 for possible migrations that include Communication Manager release 5.2.

Use these procedures to migrate from an existing DEFINITY ONE/S8100 in a compact modular cabinet (CMC) system to the Avaya S8510 Server with a IP-port network connectivity (PNC) configuration. In all instances, the cabinets can be reused as port networks (PNs). However, you can add a G650 Media Gateway PN if the existing system has one PN. This procedure supports a migration to Communication Manager Release 5.x.

When you migrate an existing DEFINITY ONE/S8100 in a CMC1 Media Gateway, you use one TN2312BP IPSI circuit pack to control the PN. You also replace the processor circuit pack with the IPSI.

This migration affects service because you must turn off the CMCs to replace the processor and tone-clock circuit packs.

Migration paths

DEFINITY ONE/S8100 and their releases that can be migrated to the S8510 Server IP-PNC configuration include:

- DEFINITY Release 6 through Release 10
- MultiVantage Release 11 and Release 1.x
- Communication Manager Release 1.0 through Release 2.0.1

Checklists

Before you go on site, perform the following tasks:

:

✓	Task	Description
	Verify that the correct hardware is installed on your Services laptop.	Correct hardware components include: ● 40 MB available disk space ● A direct Ethernet cable ● A serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● A CD-ROM drive
	Verify that the correct software is installed on your Services laptop.	Correct software includes: ● Windows 2000 or Windows 2000/XP operating system ● HyperTerminal or another terminal emulation program ● TCP/IP networking software that is bundled with the Windows OS ● Internet Explorer 5.0 or later
	Obtain the appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the logins and the passwords that you might need for the equipment of the customer.
	Obtain the serial number.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file and authentication file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	Use this CD-ROM to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware.	The following firmware is on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs **Important:** Firmware is upgraded often. To ensure that you have the latest version, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop.	New license file and authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	For DEFINITY systems only: Verify that you have the required, customer-provided network information. Obtain a completed *Electronic Preinstallation Worksheet (EPW)*.	The EPW is an Excel spreadsheet that provides the information about the network. You need this information to configure the control network components with the Avaya Installation Wizard. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard Web site.
		3 of 3

Premigration setup checklist

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

For more information, see Migration paths *on page 217*.

When you are migrating from a DEFINITY system, complete the following additional tasks before starting the migration:

✓	Task	Description
	About 2 weeks before the migration, freeze the translations. Use a spare flash card to collect the translations locally.	For more information on where and how to send the translations, contact the STS scheduling desk at 720-444-9418. STS updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For forms and more information, contact the STS scheduling desk at 720-444-9418.
	About 2 business days before the migration, create a trouble ticket to contact the STARS team.	Whenever an S8x00 server is upgraded from 1.x.x to 2.x.x and a new authentication file is requested, ASG access (remote and on-site) is impacted. You need assistance from the Service Tools and Application Remote Support (STARS) team to ensure successful ASG access before and after the upgrade. To contact the STARS team, use http://stars.avaya.com/ticket/requests/request.asp
	Mark the ticket status as CRITICAL.	Indicate text in the ticket to notify the STARS team that you are upgrading an S8x00 server. Include the date of the upgrade and the FL and product or alarm ID of the system. The STARS team contacts you on how to access your product before and after the upgrade. A temporary ASG product ID is created for you and your team to use for access during the time of the upgrade.
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.
		1 of 2

✓	Task	Description
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.
	Copy the translation file from STS to a directory on the Services laptop.	File size is usually in the range of 1-4 megabytes.
		2 of 2

Presite migration checklist

Before you go on site, perform the following tasks in Table 9:

Table 9: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks in Table 10 before you start the migration:

Table 10: On site migration checklist

✓	Task	Description
	Verify that the EIA 310D 19-inch (48-cm) open equipment rack is grounded.	See the job aid titled *Approved Grounds* (555-245-772).
	For S8510, S8710, S8720, and S8730: Verify that the open, customer-supplied, EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack is properly installed and solidly secured.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on installing the rail, see the rail kit documentation.
	Verify that you have the correct cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see: • *Installing and Configuring the Avaya S8500 Media Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Media Server* (03-300145)

Documentation checklist for migrations

For a list of documents that Avaya recommends you have on hand for the migration, see Resources on page 35.

You also need the following additional documentation:

✓	Task	Description
	Quick Start for Hardware Installation: Avaya S8500 Server (555-245-701)	A quick reference guide that provides physical installation and connection information.
	Installing and Configuring the Avaya S8500-Series Server (03-300143)	Provides installation instructions for the S8500 Server.
	Installing the Avaya S8510 Server Family and Its Components, 03-602918.	Provides installation instructions for the S8510 Server Family and Its Components
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.

Performing a migration

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

CAUTION:
This migration affects service. When the Definity One/S8100 is turned off, the system drops all calls. Service returns when the server takes control of the IPSIs.

You can reuse the translations from the existing system when you migrate to an S8510 Server, see Premigration setup on page 220.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Premigration administration

This migration is a service-affecting event. The CMCs must be turned off to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

Connecting to the processor

To connect to the processor:

Note:

You need a cross-over cable to connect your Services laptop directly to the processor.

1. Perform one of the following actions to connect the Services laptop directly into the Avaya IP600 processor circuit pack:
   - If the processor circuit pack is a TN795, place the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector directly into the RJ45 jack on the faceplate.
2. Start a terminal emulation application or Avaya Site Administration.
3. Log in as **lucent3**.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.

2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

Although the migrated translations are already copied to the server, you must save the translations in case you need to back out of the migration.

Note:

Save translations to a flash card.

To save translations:

1. To save translations to the system disk, type **`save translation`**. Press **Enter**.

   Either a **Command successfully completed** The message displays or all error messages are logged.

Recording IP settings

You must view and record the IP settings that are assigned to the processor, and use these same settings for the Avaya S8500-Series Server. You can verify the IP settings against the filled-out *Electronic Preinstallation Worksheet*.

To view these settings, perform the following administration on the Services laptop that is connected to the processor circuit pack by way of telnet. To record the IP settings:

1. Select **Start** > **Run** to open the **Run** dialog box.
2. Type **`telnet 192.11.13.6`**. Press **Enter** to access the server.
3. Log in as **lucent3** to get to the LAC prompt.
4. Type **`bash`**. Press **Enter** to start a BASH session.
5. Type **`setip`**. Press **Enter** to display the current list of IP settings. You will see the following information:
   - cust: *IPaddress, subnet mask, gateway*
   - dns: *server name, domain name, 2 DNS server IP addresses*
   - wins: *two WINS server IP addresses*
   - ras: *one remote access server IP address*
6. Record this information *exactly* as displayed.

Important:
Include any periods, commas, or other punctuation marks. Record this information in lowercase or uppercase as the information appears.

Translation migration

This section describes how to migrate translation files from the existing system to the S8510 Server.

Note:
The information in this section is based on the assumption that the S8510 is installed, configured, and operational.

Accessing the server command line interface with ssh protocol

Note:
Using the ssh protocol to access the server is applicable to Communication Manager Release 3.0 and later.

To use this procedure with a laptop cable connection to the services port, you must configure your laptop for the network connection. In addition, a third-party ssh client must already be installed on your computer.

For more information on Network Configuration, see *Converting Avaya Servers and Media Gateways*, 03-602884.

PuTTY is one such client available for download from http://www.putty.nl/download.html. The following procedure describes, as an example of ssh access, how to log into the server command line with PuTTY.

Note:

A version of PuTTY that is defaulted for ssh server access is available for Avaya services personnel only. In this version, some values below have already been pre-selected.

CAUTION:

While a variety of Avaya products support access using ssh, Avaya does not provide support for third-party clients used for ssh access. Any problems with an ssh client, including PuTTY, are the responsibility of the user or the ssh client vendor.

To access the command line interface using PuTTY with ssh:

1. On your computer, click on the **PuTTY** desktop link or select **Start** > **Programs** > **PuTTY** > **PuTTY**.
2. In the **Host Name (or IP address)** field, type **`192.11.13.6`** if connecting to the services port. Otherwise, for access over the LAN/WAN, type the IP address or the host name of the server.
3. In the **Port** field, type **22** (the SAT is **5022**).
4. Under Protocol, select **SSH**.
5. In the PuTTY menu on the left, click **Connection** > **SSH**.

   The Options controlling SSH connections dialog box opens.
6. In the **Preferred SSH protocol version** field, select **2**.
7. In the **Encryption options** window, use the up and down arrows to set **AES (SSH-2)** as the top option and **3DES** as the second option.

   Note:

   You can save the PuTTY settings and customize the PuTTY tool with other settings, such as for color. For documentation on PuTTY, see http://www.putty.nl/docs.html.
8. In the PuTTY menu on the left, click **Terminal** > **Keyboard**.

   The **Options controlling the effects of keys** dialog box opens.
9. In the **Backspace key** area, select **Control-H**.

   This activates the backspace key while you are using the SAT.
10. Click **Open**.

Note:

If you have not connected to this particular server before, ssh prompts you to accept the server host key. If you save this key when prompted, you will not be prompted if you connect again later. If you do not save the key, PuTTY prompts you the next time you connect to this server.

When connecting through the Services laptop interface on the server, if you save the host key, the host will be identified as 192.11.13.6. If you later connect to a different server through its laptop interface, this new host also appears as 192.11.13.6, but it will have a different key. You get a prompt in this case because it appears that the host key has changed.

11. If necessary, click **Yes** to accept the server's host key.
12. Log in to the server.

Clearing the ARP cache on the laptop computer

You might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. This need depends on the operating system on your laptop computer. If you enter an IP address and your computer cannot connect, you might need to clear the cache.

To clear the ARP cache on the laptop:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. To open an MS-DOS command line window, type **`command`** and press **Enter**.
3. Type **`arp -d 192.11.13.6`** and press **Enter**. This command produces one of the following responses:
   - The command line prompt displays when the cache is cleared.
   - The message **The specified entry was not found** appears when the specified IP address does not currently appear in the ARP cache.

Type **exit** to close the MS-DOS window.

Clearing the Web browser cache on the laptop

Due to underlying changes on Communication Manager Web pages, you might experience problems with accessing some of the pages. For example, you might see some strange behavior when using the same laptop/PC to switch in-between Communication Manager loads or releases, especially when accessing the Communication Manager server(s) through the Services port (http://192.11.13.6). This is due to how your web browser is caching information and it does not always know what is new and what is old.

For example, for Communication Manager Release 3.1 and earlier, you log into https://192.11.13.6 and it takes you to https://192.11.13.6/log-in.

But if you are in Communication Manager Release 5.x and you log into https://192.11.13.6, it takes you to https://192.11.13.6/log-in/web-page (or something similar).

The problem is that the laptop gets confused after it has been at Release 5.x and then you want to go to another site in pre Release 5.x. The system cannot find the old login page.

This happens only if you are switching between releases and/or loads - especially if you go backwards in releases (for example, from Release 5.x on Server 1 to Release 3.0 on Server 2). There does not seem to be a problem going forward in releases.

If you are experiencing problems logging in to Web pages:

1. On the Internet Explorer page, select **Tools** > **Internet Options**.
2. In the Temporary Internet files section, click **Delete Cookies**.
3. Click **OK**.
4. In the Temporary Internet files section, click **Delete files**.
5. Click **OK**.
6. In the History section, click **History**.
7. Click **OK**.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Copying translation files to server

To copy translation files to the server:

1. Under Miscellaneous, click **Download Files**.
2. Click **Files(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** and select the file that you saved on the Services laptop.
4. Click **Download** to place a copy of the file on the server.

Restoring translation files

To restore translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Local Directory** and click **View**. The field automatically shows the default directory.
3. Select the translation file.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.
5. Click **Restore** to restore the translation files.
6. Click **Restore Status**.
7. Select the first file and then scroll down and click **Review Status** to see the results of the restore.

   When the restore process completes, the screen displays **Restore is finished**.
8. Use Native Configuration Manager or Avaya Site Administration to start a SAT session.
9. Type **`reset system 4`**. Press **Enter** to load the restored translations.

If the restore process fails, the system displays an error message that states the reason for the failure. The translation file is not restored. You must resolve the reason for the failure and restart the process.

Administering the IPSIs

To administer the IPSIs:

1. Type **`change system-parameters ipserver-interface`**. Press **Enter**
2. Verify that the **Primary Control Subnet Address** field is correct.

   The subnet address must match the most significant three octets (the first three groups of digits in the subnet address) of the server IP address that is listed on the control network entry from the completed Electronic Preinstallation Worksheet (EPW).

   An asterisk (*****) to the right of the **Subnet Address** field means that although a subnet address displays, this address is incorrect. Communication Manager does not have the subnet information. After you verify the information shown on the screen, submit this form with or without changes to update the Communication Manager with the correct subnet information.

   CAUTION:

   If the information in the **Primary Control Subnet Address** field is incorrect, you must change the information on the server. Use the System Management Interface (SMI) and access **Installation > Configure Server** to change the server configuration. Then continue with step 3 of this procedure.
3. Verify that the **Switch Identifier** field is set correctly for this installation. You must enter the correct switch identifier here before you administer the TN2312 IPSI circuit packs.
4. Verify that the **IPSI Control of Port Networks** field is set to **disabled**.
5. Press **Enter**.

Adding IPSI translations to Communication Manager

To add IPSI translations to Communication Manager:

1. Type **`add ipserver-interface 1`**. Press **Enter** to add the IPSI circuit pack information.
2. If you use static addressing, in the **Host** field, type the IP address for the IPSI that is in the port network listed in the **Location** field.
3. Verify that the **IP Control** field is set to **y**.
4. Verify that all the other fields are populated.
5. Press **Enter** to put the changes into effect.

6. Repeat Steps 1 through 5 for each IPSI.

Setting the alarm activation level

To set the alarm activation level:

1. Type **`change system-parameters maintenance`** and press **Enter**.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that the customer wants. The default is **none**.

Backing up translations

To back up translations:

1. Under Data Backup/Restore, click **Backup Now**.
2. Select the data sets and the backup method.

   If you select **Save ACP translations prior to backup**, the server automatically saves the translations to the hard drive before the server saves the translations to the backup media.
3. Click **Start Backup** to begin the backup process.

Migration tasks

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Perform the following tasks to convert a processor port network to a port network (CMC).

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

Customers who currently use the Audix feature on the S8100 must purchase a separate Audix system. The TN795 or the TN2314 Processor circuit pack that contains the Audix feature is replaced with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that does not contain the Audix feature. You must return the existing processor circuit pack to Avaya.

Note:

Customers also must add an ED-1E568-70G1 DEFINITY Audix Slim board and a TN2501AP Voice Announcement over LAN (VAL) circuit pack for announcements.

Changing the control cabinet to a port network

To change the control cabinet to a port network, you must:

- Replace the TN795 or TN2314 Processor circuit pack with a TN2312BP Internal Protocol Server Interface (IPSI) circuit pack.
- Connect a CAT5 straight-through cable from the IPSI to the server through the network of the customer.

Note:

If you replace a TN795 Processor circuit pack, you might not need the TN744D/E Call Classifier-Detector circuit pack. The TN2312BP IPSI circuit pack has call classifier functionality. However, increased voice and data traffic can require the TN744D/E Call Classifier-Detector circuit pack.

Note:

If you have a TN799C or earlier C-LAN circuit pack, you must replace the TN799 circuit pack with a TN799DP C-LAN circuit pack.

Turning off the power to the control cabinet

CAUTION:

Ensure that you have completed the premigration administration. If you do not perform the premigration administration, the system will not function. For more information, see Premigration administration on page 226.

To turn off power to the control cabinet:

1. On the faceplate of the processor, press and hold the shutdown button until the shutdown process starts.

   When you see the green light the system is shut down.

   DANGER:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the cabinet, pull the AC power cord from the back of the cabinet.

2. Unplug the power cord from the back of the cabinet to turn off the cabinet.

Replacing the processor circuit pack

To replace the processor circuit pack:

1. Remove the entire processor circuit pack and place it in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
2. Remove the octopus cable from the connector that is associated with slot 2 on the connector panel.
3. Install the IPSI adapter to the connector that is associated with slot 2 on the connector panel.
4. Install the maintenance cable onto the 9-pin D-sub connector on the adapter. This cable is for emergency transfer and "auxsig" signal.

Note:

The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack takes only one slot.

5. Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit pack into slot 2.
6. Attach the new label above the circuit pack slots.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test circuit pack

You must replace the TN795 or the TN2412 circuit pack with a TN771 Maintenance/Test circuit pack. Each location must have one TN771 Maintenance/Test circuit pack.

To install the TN771 Maintenance/Test circuit pack:

- Install the TN771 circuit pack in slot 1.

  This carrier does not have a dedicated slot for the TN775 Maintenance (EPN) circuit pack.

Connecting the IPSI to the network

After connecting to the server, power up the CMC1 cabinets:

1. Connect one end of the green CAT5 straight-through cable to the Ethernet switch on the customer network.
2. Connect the other end of the cable to the IPSI adapter on the back of the media gateway.

Post-migration administration

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 14: Connecting directly to the IPSI on page 239).

Figure 14: Connecting directly to the IPSI

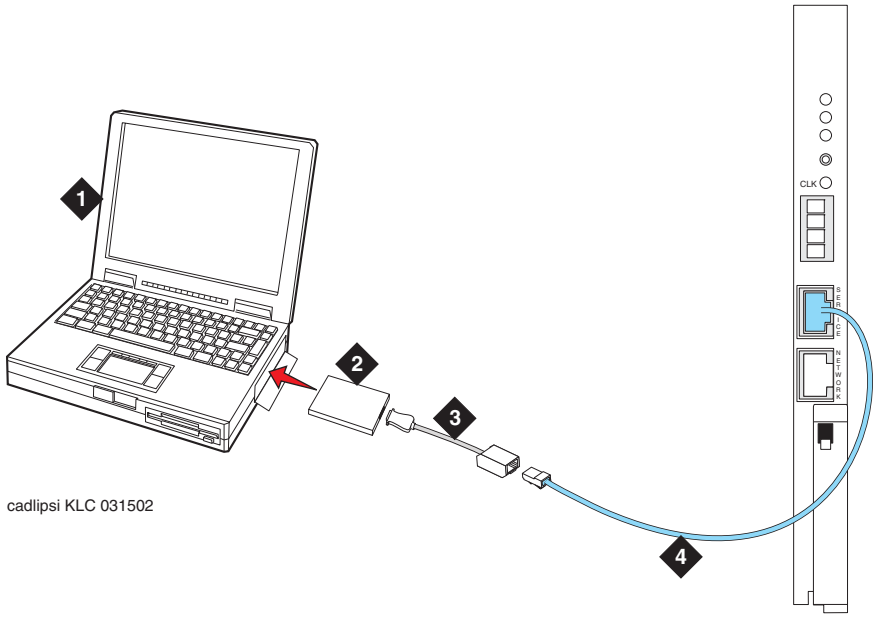


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application on the service laptop to access the server (192.11.13.6 port 22).

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.

2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

Note:

The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`** and press **Enter**.
2. To see the current settings, type **`show port 1`** and press **Enter**.
3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Verify that the correct information was entered.
5. If a default gateway is used, enter the gateway IP address.
   Type **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway and press **Enter**.
6. To save the changes and exit the IPSI session, type **`quit`** and press **Enter**.
7. SSH to **192.11.13.6** and log in.

8. To verify the administration, type **`show control interface`** and press **Enter**.
9. To see the changes, type **`exit`** and press **Enter**.

Setting the VLAN and diffserv parameters

To set the VLAN parameters and the diffserver parameters:

1. Log back in as **`craft`**.
2. To display the quality of service values, type **`show qos`** and press **Enter**.
3. If necessary, use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

   Note:
   Use **Help** to obtain syntax guidelines for these commands.

   - Type **`set vlan priority 6`**
   - Type **`set diffserv 46`**
   - Type **`set vlan tag on`**
   - Type **`set port negotiation 1 disable`**
   - Type **`set port duplex 1 full`**
   - Type **`set port speed 1 100`**
4. To check the administered values, type **`show qos`** and press **Enter**.
5. To exit, type **`quit`**. Press **Enter**.

   Important:
   Ensure that the port settings on the Ethernet switches are set to the same values as shown in the **`set port`** commands in step 3.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

Note:

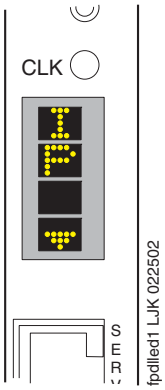
Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

Note:

The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.

2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 15).

Figure 15: LED display that shows that the IPSI has a static IP address



4. Repeat steps 1 through 3 for each IPSI circuit pack.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "1" shows in any position, you must troubleshoot the problem.

Tip:

The pattern `0.1.1.0` usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct cabinet and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying the license file

To verify the Communication Manager license file:

1. Under Security, click **License File**.
2. Verify that the **Communication Mgr License Mode** field is set to **Normal**.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating an Avaya IP600/S8100 to an S8500-Series Server

Important:
The S8500A Server is not supported on Communication Manager 5.0 and later releases. Refer to the table of Server Migration Paths on page 50 for possible migrations that include Communication Manager release 5.2.

Use these procedures to migrate from an existing DEFINITY IP600/S8100 to the Avaya S8510 Server with a IP-port network connectivity (PNC) configuration. In all instances, you can reuse the cabinets as port networks (PNs). However, you can add a G650 Media Gateway port network only if the existing switch has one or two PNs. This procedure supports a migration to Communication Manager Release 5.x.

To migrate an existing Avaya IP600/S8100, you use one TN2312BP IPSI circuit pack to control the PN. You replace the processor circuit pack in the A position in the cabinet with the IPSI.

This migration affects service because you must turn off the IP600 chassis to replace the processor circuit pack.

Migration paths

DEFINITY IP600/S8100 and their releases that can be migrated to the S8510 Server IP-PNC configuration include:

- DEFINITY Release 9 through Release 10
- MultiVantage Release 11 and Release 1.x
- Communication Manager Release 1.0 through Release 2.0.1

Checklists

Before you go on site, perform the following tasks:

:

✓	Task	Description
	Verify that the correct hardware is installed on your Services laptop.	Correct hardware components include: ● 40 MB available disk space ● A direct Ethernet cable ● A serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● A CD-ROM drive
	Verify that the correct software is installed on your Services laptop.	Correct software includes: ● Windows 2000 or Windows 2000/XP operating system ● HyperTerminal or another terminal emulation program ● TCP/IP networking software that is bundled with the Windows OS ● Internet Explorer 5.0 or later
	Obtain the appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the logins and the passwords that you might need for the equipment of the customer.
	Obtain the serial number.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file and authentication file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	Use this CD-ROM to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware.	The following firmware is on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs **Important:** Firmware is upgraded often. To ensure that you have the latest version, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop.	New license file and authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	For DEFINITY systems only: Verify that you have the required, customer-provided network information. Obtain a completed *Electronic Preinstallation Worksheet (EPW)*.	The EPW is an Excel spreadsheet that provides the information about the network. You need this information to configure the control network components with the Avaya Installation Wizard. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard Web site.
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

For additional information, see.Migration paths on page 247.

When you are migrating from a DEFINITY system, complete the following additional tasks before starting the migration:

✓	Task	Description
	About 2 weeks before the migration, freeze the translations. Use a spare flash card to collect the translations locally.	For more information on where and how to send the translations, contact the STS scheduling desk at 720-444-9418. STS updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For forms and more information, contact the STS scheduling desk at 720-444-9418.
	About 2 business days before the migration, create a trouble ticket to contact the STARS team.	Whenever an S8x00 server is upgraded from 1.x.x to 2.x.x and a new authentication file is requested, ASG access (remote and on-site) is impacted. You need assistance from the Service Tools and Application Remote Support (STARS) team to ensure successful ASG access before and after the upgrade. To contact the STARS team, use http://stars.avaya.com/ticket/requests/request.asp
	Mark the ticket status as CRITICAL.	Indicate text in the ticket to notify the STARS team that you are upgrading an S8x00 server. Include the date of the upgrade and the FL and product or alarm ID of the system. The STARS team contacts you on how to access your product before and after the upgrade. A temporary ASG product ID is created for you and your team to use for access during the time of the upgrade.
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This happens at least one day prior to the migration.

✓	Task	Description
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.
	Copy the translation file from STS to a directory on the Services laptop.	File size is usually in the range of 1-4 megabytes.

2 of 2

Presite migration checklist

Before you go on site, perform the following tasks in Table 11:

Table 11: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site for a migration from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	The customer supplies an open EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack. Verify that this rack is installed correctly.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on how to install the rail, see the documentation that comes with the rail kit.
	Verify that you have the license file that the file includes the licensed features.	Use the License File link on the System Management Interface (SMI) to verify.
	Verify that you have the Avaya Authentication File (if not installed with AIW) on page 300.	Use the Authentication File link on the System Management Interface (SMI) to verify.

When you are on site for a migration from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	Verify the customer supplies an EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack. Verify that this rack is installed correctly and solidly secured.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For information on how to install the rail, see the rail kit documentation.
	Verify that you have the license file that the license file includes: • the right to use (RTU) feature • the applicable hardware parts in the existing system • any hardware that is being added as part of the migration	Use the License File link on the System Management Interface (SMI) to verify.
	Verify that you have the Avaya authentication file.	Use the License File link on the System Management Interface (SMI) to verify.
	Replace the TN795 or the TN2314 Processor circuit pack that contains the CMM feature.	Replace with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that does not have the CMM feature. You also must return the existing Processor circuit pack to Avaya.

Documentation checklist for migrations

For a list of documents that Avaya recommends you have on hand for the migration, see Resources on page 35.

You also need the following additional documentation:

✓	Task	Description
	Quick Start for Hardware Installation: Avaya S8500 Server (555-245-701)	A quick reference guide that provides physical installation and connection information.
	Installing and Configuring the Avaya S8500-Series Server (03-300143)	Provides installation instructions for the S8500 Server.
	Installing the Avaya S8510 Server Family and Its Components, 03-602918.	Provides installation instructions for the S8510 Server Family and Its Components
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.

Performing a migration

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

CAUTION:

This migration affects service. When the IP600/S8100 is turned off, the system drops all calls. Service returns when the server takes control of the IPSIs.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Premigration administration

This migration affects service. You must turn off the IP600 chassis to replace the processor circuit pack. Before you turn off the chassis, you must perform the following premigration administration.

Connecting to the processor

To connect to the processor:

Note:

You need a cross-over cable to connect your Services laptop directly to the processor.

1. Perform one of the following actions to connect the Services laptop directly into the Avaya IP600 processor circuit pack:
   - If the processor circuit pack is a TN795, place the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector directly into the RJ45 jack on the faceplate.
2. Start a terminal emulation application or Avaya Site Administration.
3. Log in as **lucent3**.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.
2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.

3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

You must save the translations in case you need to stop out of the migration. You might want to print out the translations for reference.

To save translations:

1. Type **`save translation`** and press **Enter** to save translations to the system disk.

   Either a **Command successfully completed** message displays or all error messages are logged.

Recording IP settings

You must view and record the IP settings that are assigned to the processor, and use these same settings for the Avaya S8500-Series Server. You can verify the IP settings against the filled-out *Electronic Preinstallation Worksheet*.

To view these settings, perform the following administration on the Services laptop that is connected to the processor circuit pack by way of telnet. To record the IP settings:

1. Select **Start** > **Run** to open the **Run** dialog box.
2. Type **`telnet 192.11.13.6`**. Press **Enter** to access the server.
3. Log in as **lucent3** to get to the LAC prompt.
4. Type **`bash`**. Press **Enter** to start a BASH session.
5. Type **`setip`**. Press **Enter** to display the current list of IP settings. You will see the following information:
   - cust: *IPaddress, subnet mask, gateway*
   - dns: *server name, domain name, 2 DNS server IP addresses*
   - wins: *two WINS server IP addresses*
   - ras: *one remote access server IP address*
6. Record this information *exactly* as displayed.

Important:

Include any periods, commas, or other punctuation marks. Record this information in lowercase or uppercase as the information appears.

Translation migration

This section describes how to migrate translation files from the existing switch to the S8510 Server.

Accessing the server command line interface with ssh protocol

Note:

Using the ssh protocol to access the server is applicable to Communication Manager Release 3.0 and later.

To use this procedure with a laptop cable connection to the services port, you must configure your laptop for the network connection. In addition, a third-party ssh client must already be installed on your computer.

For more information on Network Configuration, see *Converting Avaya Servers and Media Gateways*, 03-602884.

PuTTY is one such client available for download from http://www.putty.nl/download.html. The following procedure describes, as an example of ssh access, how to log into the server command line with PuTTY.

Note:

A version of PuTTY that is defaulted for ssh server access is available for Avaya services personnel only. In this version, some values below have already been pre-selected.

CAUTION:

While a variety of Avaya products support access using ssh, Avaya does not provide support for third-party clients used for ssh access. Any problems with an ssh client, including PuTTY, are the responsibility of the user or the ssh client vendor.

To access the command line interface using PuTTY with ssh:

1. On your computer, click on the **PuTTY** desktop link or select **Start** > **Programs** > **PuTTY** > **PuTTY**.
2. In the **Host Name (or IP address)** field, type **`192.11.13.6`** if connecting to the services port. Otherwise, for access over the LAN/WAN, type the IP address or the host name of the server.
3. In the **Port** field, type **22** (the SAT is **5022**).
4. Under Protocol, select **SSH**.
5. In the PuTTY menu on the left, click **Connection** > **SSH**.

   The Options controlling SSH connections dialog box opens.
6. In the **Preferred SSH protocol version** field, select **2**.
7. In the **Encryption options** window, use the up and down arrows to set **AES (SSH-2)** as the top option and **3DES** as the second option.

   Note:

   You can save the PuTTY settings and customize the PuTTY tool with other settings, such as for color. For documentation on PuTTY, see http://www.putty.nl/docs.html.
8. In the PuTTY menu on the left, click **Terminal** > **Keyboard**.

   The **Options controlling the effects of keys** dialog box opens.
9. In the **Backspace key** area, select **Control-H**.

   This activates the backspace key while you are using the SAT.
10. Click **Open**.

    Note:

    If you have not connected to this particular server before, ssh prompts you to accept the server host key. If you save this key when prompted, you will not be prompted if you connect again later. If you do not save the key, PuTTY prompts you the next time you connect to this server.

    When connecting through the Services laptop interface on the server, if you save the host key, the host will be identified as 192.11.13.6. If you later connect to a different server through its laptop interface, this new host also appears as 192.11.13.6, but it will have a different key. You get a prompt in this case because it appears that the host key has changed.
11. If necessary, click **Yes** to accept the server's host key.
12. Log in to the server.

Clearing the ARP cache on the laptop computer

You might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. This need depends on the operating system on your laptop computer. If you enter an IP address and your computer cannot connect, you might need to clear the cache.

To clear the ARP cache on the laptop:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. To open an MS-DOS command line window, type **`command`** and press **Enter**.
3. Type **`arp -d 192.11.13.6`** and press **Enter**. This command produces one of the following responses:
   - The command line prompt displays when the cache is cleared.
   - The message **The specified entry was not found** appears when the specified IP address does not currently appear in the ARP cache.

Type **exit** to close the MS-DOS window.

Clearing the Web browser cache on the laptop

Due to underlying changes on Communication Manager Web pages, you might experience problems with accessing some of the pages. For example, you might see some strange behavior when using the same laptop/PC to switch in-between Communication Manager loads or releases, especially when accessing the Communication Manager server(s) through the Services port (http://192.11.13.6). This is due to how your web browser is caching information and it does not always know what is new and what is old.

For example, for Communication Manager Release 3.1 and earlier, you log into https://192.11.13.6 and it takes you to https://192.11.13.6/log-in.

But if you are in Communication Manager Release 5.x and you log into https://192.11.13.6, it takes you to https://192.11.13.6/log-in/web-page (or something similar).

The problem is that the laptop gets confused after it has been at Release 5.x and then you want to go to another site in pre Release 5.x. The system cannot find the old login page.

This happens only if you are switching between releases and/or loads - especially if you go backwards in releases (for example, from Release 5.x on Server 1 to Release 3.0 on Server 2). There does not seem to be a problem going forward in releases.

If you are experiencing problems logging in to Web pages:

1. On the Internet Explorer page, select **Tools** > **Internet Options**.
2. In the Temporary Internet files section, click **Delete Cookies**.
3. Click **OK**.
4. In the Temporary Internet files section, click **Delete files**.

5. Click **OK**.
6. In the History section, click **History.**
7. Click **OK**.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Copying translation files to server

To copy translation files to the server:

1. Under Miscellaneous, click **Download Files**.
2. Click **Files(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** and select the file that you saved on the Services laptop.
4. Click **Download** to place a copy of the file on the server.

Restoring translation files

To restore translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Local Directory** and click **View**. The field automatically shows the default directory.
3. Select the translation file.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.

5. Click **Restore** to restore the translation files.
6. Click **Restore Status**.
7. Select the first file and then scroll down and click **Review Status** to see the results of the restore.

   When the restore process completes, the screen displays **Restore is finished**.
8. Use Native Configuration Manager or Avaya Site Administration to start a SAT session.
9. Type **`reset system 4`**. Press **Enter** to load the restored translations.

If the restore process fails, the system displays an error message that states the reason for the failure. The translation file is not restored. You must resolve the reason for the failure and restart the process.

Administering the IPSIs

To administer the IPSIs:

1. Type **`change system-parameters ipserver-interface`**. Press **Enter**
2. Verify that the **Primary Control Subnet Address** field is correct.

   The subnet address must match the most significant three octets (the first three groups of digits in the subnet address) of the server IP address that is listed on the control network entry from the completed Electronic Preinstallation Worksheet (EPW).

   An asterisk (*****) to the right of the **Subnet Address** field means that although a subnet address displays, this address is incorrect. Communication Manager does not have the subnet information. After you verify the information shown on the screen, submit this form with or without changes to update the Communication Manager with the correct subnet information.

   CAUTION:

   If the information in the **Primary Control Subnet Address** field is incorrect, you must change the information on the server. Use the System Management Interface (SMI) and access **Installation > Configure Server** to change the server configuration. Then continue with step 3 of this procedure.
3. Verify that the **Switch Identifier** field is set correctly for this installation. You must enter the correct switch identifier here before you administer the TN2312 IPSI circuit packs.
4. Verify that the **IPSI Control of Port Networks** field is set to **disabled**.
5. Press **Enter**.

Adding IPSI translations to Communication Manager

To add IPSI translations to Communication Manager:

1. Type **`add ipserver-interface 1`**. Press **Enter** to add the IPSI circuit pack information.
2. If you use static addressing, in the **Host** field, type the IP address for the IPSI that is in the port network listed in the **Location** field.
3. Verify that the **IP Control** field is set to **y**.
4. Verify that all the other fields are populated.
5. Press **Enter** to put the changes into effect.
6. Repeat Steps 1 through 5 for each IPSI.

Setting the alarm activation level

To set the alarm activation level:

1. Type **`change system-parameters maintenance`** and press **Enter**.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that the customer wants. The default is **none**.

Backing up translations

To back up translations:

1. Under Data Backup/Restore, click **Backup Now**.
2. Select the data sets and the backup method.

   If you select **Save ACP translations prior to backup**, the server automatically saves the translations to the hard drive before the server saves the translations to the backup media.
3. Click **Start Backup** to begin the backup process.

Migration tasks

Perform the following tasks to convert a processor port network to a port network (IP600).

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

Customers who currently use the Audix feature on the S8100 must purchase a separate Audix system. The TN795 or the TN2314 Processor circuit pack that contains the Audix feature is replaced with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that does not contain the Audix feature. You must return the existing processor circuit pack to Avaya.

Note:

Customers also must add an ED-1E568-70G1 DEFINITY Audix Slim board and a TN2501AP Voice Announcement over LAN (VAL) circuit pack for announcements.

Changing the IP600 control chassis to a port network

To change the Avaya IP600 control chassis to a port network, you must:

- Replace the existing straight-wire WP cables, if present, with new twisted pair I/O cables.
- Replace the processor circuit pack with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack.
- Connect a CAT5 straight-through cable from the IPSI to the server through the network of the customer.

Note:

If you replace a TN795 Processor circuit pack, you might not need the TN744D/E Call Classifier-Detector circuit pack. The TN2312BP IPSI circuit pack has call classifier functionality. However, increased voice and data traffic can require the TN744D/E Call Classifier-Detector circuit pack.

Note:

If you have a TN799C or earlier C-LAN circuit pack, you must replace the TN799 circuit pack with a TN799DP C-LAN circuit pack.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Turning off the control chassis

To turn off the control chassis:

CAUTION:

Ensure that you have completed the premigration administration. For more information, see Premigration administration on page 257.

1. Press and hold the shutdown button on the on the faceplate of the processor until the shutdown process starts.

   Ensure that you see the green light. This light indicates that the system is shut down.

   DANGER:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the chassis, pull the AC power cord from the back of the chassis.

2. To turn off the chassis, unplug the power cord from the back of the chassis.

Replacing I/O cables

On older MCC, SCC, and G600 cabinets you must replace the existing I/O cables (WP-90753, LI), which connect the backplane to the rear connector panel, with twisted pair I/O cables.

The existing I/O cables have straight, not twisted, wires. They may be mostly white with two red, or multi-colored. If the cables have multi-colored, tightly twisted wires, no replacement is necessary.

To order the DEFINITY kit with twisted pair I/O cables, use comcode 700234032.

CAUTION:
Turn off power to the carrier or media gateway being serviced. Failure to turn off the power can result in electric shock.

CAUTION:
When adding or replacing any hardware and associated cables and adapters, be sure to ground yourself against electrostatic discharge (ESD) by wearing a grounded wrist strap. Failure to follow ESD procedures can result in system damage or service disruption.

To replace the existing I/O cables:

1. For the G600 Media Gateway, you must remove the fan assembly to access the cables. Loosen the thumb screws on the fan assembly and pull it straight out as shown in Figure 16: G600 Media Gateway fan assembly removal on page 268. Leave the fan assembly off until all the wires are installed.
2. Note the orientation of the existing 10 cables. The existing I/O cables may be white and red or multicolored. They are not twisted.
3. Remove the nontwisted pair of existing I/O cables from the backplane and the connector panel slots.
4. In their place install the 10 tight-twisted pair I/O cables onto the backplane, according to the proper orientation shown in Figure 17: Proper orientation for the twisted pair I/O cables on page 269. Observe the white outline printed on the backplane for the location of each connector.
5. When viewed from the "wiring" side of the twin connectors (that is, while plugging them into the backplane) and with the connectors oriented properly for plug-in, they should look like Figure 17: Proper orientation for the twisted pair I/O cables on page 269.

   The circled pin locations are “No-Connects”; that is, they have no wires in them. At the top there is an orange-black pair on the right and a violet-brown pair on the left.

   The 50-position metal shell D connectors should be installed into the connector panel with the longer side of the D (pins 1–25) toward the right when viewed from the rear of the media gateway.

6. For the G600 Media Gateway, replace the fan unit if no other media gateways are to be installed. If you are adding more media gateways to the rack, leave the fan units off until all of the TDM cables are installed.

Figure 16: G600 Media Gateway fan assembly removal

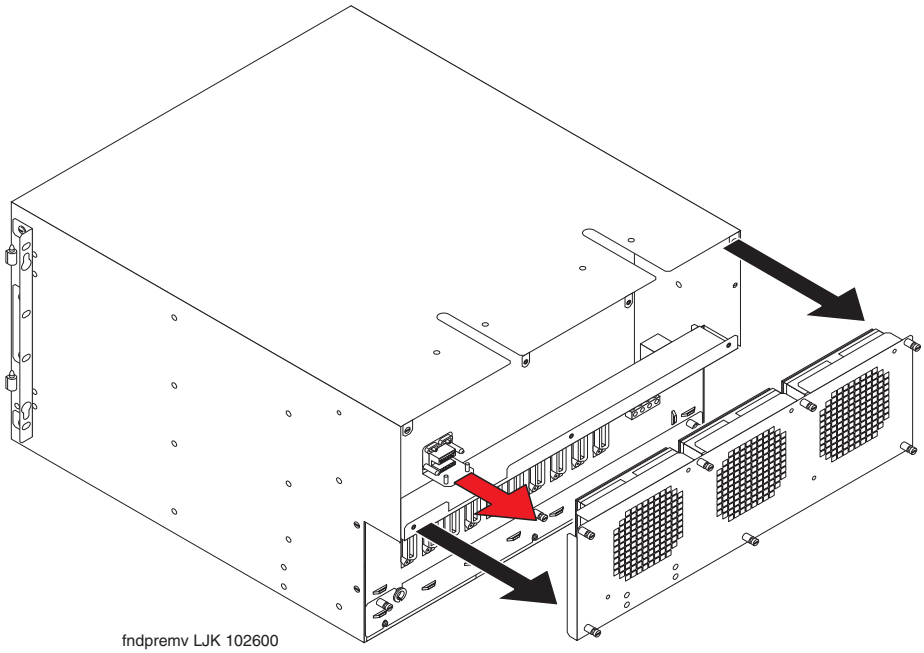


Figure 17: Proper orientation for the twisted pair I/O cables

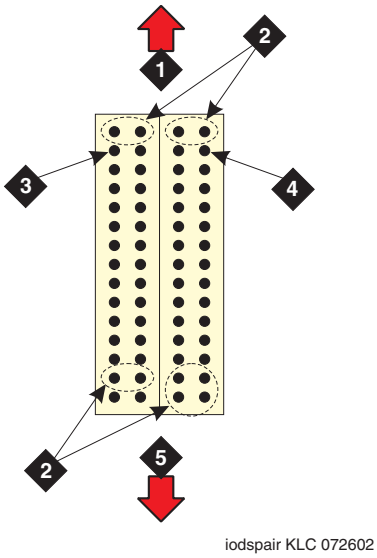


Figure notes:

1. **Top**
2. **No connects; no wires**
3. **Violet-brown**
4. **Orange-black**
5. **Bottom**

Replacing the processor circuit pack

To replace the processor circuit pack:

1. Remove the entire processor circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You want the circuit pack intact if you need to back out of the migration.
3. Remove the octopus cable from the connector that is associated with slot 2 on the backplane.
4. Install the IPSI adapter to the connector that is associated with slot 2 on the backplane.
5. Install the maintenance cable onto the 9-pin D-sub connector on the adapter. This cable is for emergency transfer and "auxsig" signal.

   Note:

   The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack takes only one slot.

6. Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit pack into slot 2.
7. Attach the new label above the circuit pack slots.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test circuit pack

You must replace the TN795 or the TN2412 circuit pack with a TN771 Maintenance/Test circuit pack. Each location must have one TN771 Maintenance/Test circuit pack.

To install the TN771 Maintenance/Test circuit pack:

- Install the TN771 circuit pack in slot 1.

  This carrier does not have a dedicated slot for the TN775 Maintenance (EPN) circuit pack.

Connecting the IPSI to the network

After connecting to the server, power up the CMC1 cabinets:

1. Connect one end of the green CAT5 straight-through cable to the Ethernet switch on the customer network.
2. Connect the other end of the cable to the IPSI adapter on the back of the media gateway.

Post-migration administration

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 18: Connecting directly to the IPSI on page 272).

Figure 18: Connecting directly to the IPSI

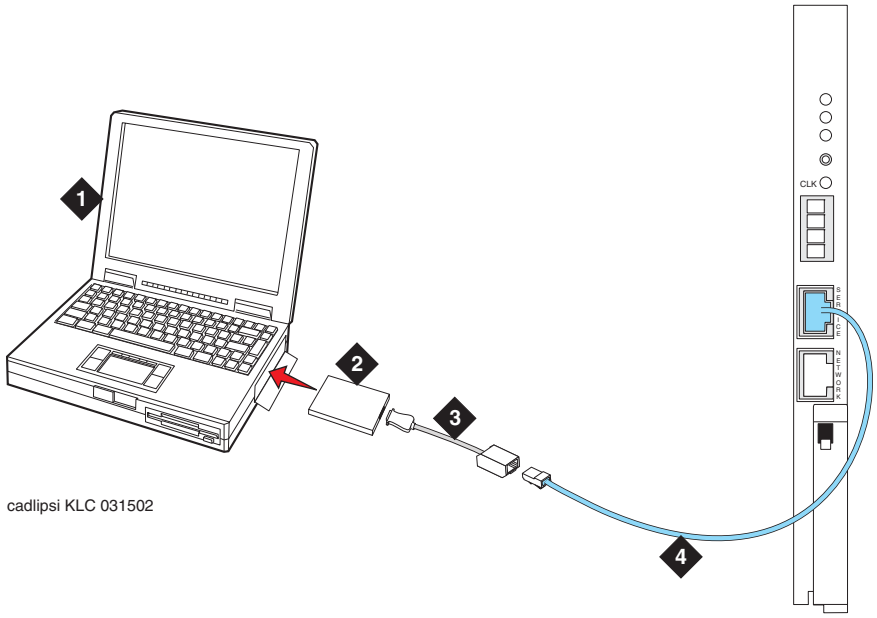


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application on the service laptop to access the server (192.11.13.6 port 22).

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.

2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **craft**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **show control interface** and press **Enter**.
2. To see the current settings, type **show port 1** and press **Enter**.
3. Type **set control interface *ipaddr netmask***, where ***ipaddr*** is the customer-provided IP address and ***netmask*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Verify that the correct information was entered.
5. If a default gateway is used, enter the gateway IP address.
   Type **set control gateway *gatewayaddr***, where ***gatewayaddr*** is the customer-provided IP address for their gateway and press **Enter**.
6. To save the changes and exit the IPSI session, type **quit** and press **Enter**.
7. SSH to **192.11.13.6** and log in.
8. To verify the administration, type **show control interface** and press **Enter**.

9. To see the changes, type **`exit`** and press **Enter**.

Setting the VLAN and diffserv parameters

To set the VLAN parameters and the diffserver parameters:

1. Log back in as **`craft`**.
2. To display the quality of service values, type **`show qos`** and press **Enter**.
3. If necessary, use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

   Note:
   Use **Help** to obtain syntax guidelines for these commands.

   - Type **`set vlan priority 6`**
   - Type **`set diffserv 46`**
   - Type **`set vlan tag on`**
   - Type **`set port negotiation 1 disable`**
   - Type **`set port duplex 1 full`**
   - Type **`set port speed 1 100`**
4. To check the administered values, type **`show qos`** and press **Enter**.
5. To exit, type **`quit`**. Press **Enter**.

   Important:
   Ensure that the port settings on the Ethernet switches are set to the same values as shown in the **`set port`** commands in step 3.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

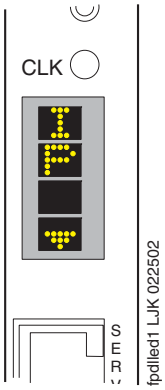
   Note:
   Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

Note:

The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.

2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 19).

Figure 19: LED display that shows that the IPSI has a static IP address



4. Repeat steps 1 through 3 for each IPSI circuit pack.

Note:

Clear the ARP cache on the laptop before you connect to another IPSI. If you do not clear the cache, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "1" shows in any position, you must troubleshoot the problem.

Tip:

The pattern `0.1.1.0` usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct cabinet and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Enabling control of the IPSI

To enable control of the IPSI:

Note:

Ensure that the IPSI has the same, current firmware.

CAUTION:

This procedure allows the server to take control of the IPSI-controlled port network(s). Failure to complete the steps correctly can result in no connection to the network.

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Set the **IPSI Control of Port Networks:** field to **enabled**
3. Press **Enter** to effect the change.
4. Type **`save translation`** and press **Enter**.

   The server now controls all the port networks.

Verifying the license file

To verify the Communication Manager license file:

1. Under Security, click **License File**.
2. Verify that the **Communication Mgr License Mode** field is set to **Normal**.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.

2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the

firmware, you also can go to Avaya Support Web page (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating an Avaya S8500A or S8500B Server to an S8500C or S8510 Server

Use these procedures to migrate an existing S8500 Server running Release 2.x, 3.x, 4.x, 5.0 or 5.1 of Communication Manager to an S8500C or S8510 Server running Release 5.2 or later. This procedure can be used for migration from S8500A, S8500B to S8300C, S8510; or for migration from S8500A, S8500B, and S8500C to S8510. This procedure can be used for a Main Server, Local Survivable Processors (LSP), or an Enterprise Survivable Server (ESS).

Important:
In this module of: Migrating an Avaya S8500A or S8500B Server to an S8500C or S8510 Server to simplify the instructions, the old server will be referred to as the S8500 and the new server will be referred to as the S8510, even though the new server possibly can also be an S8500C. The old server can be any of S8500A, S8500B, or S8500C.

Important:
The S8500A Server is not supported on Communication Manager 5.0 and later releases. Refer to the table of Server Migration Paths on page 50 for possible migrations that include Communication Manager release 5.2.

In this migration, a copy of the translations from the S8500 Server is loaded onto the S8510 Server. The translations are the only thing that is transferred to the S8510 Server. You must record the configuration information for the S8500 Server and input the configuration information into the S8510 Server.

With this migration, you also upgrade to Communication Manager Release 5.2. If the configuration includes LSPs and ESS servers, you must upgrade the LSPs and the ESS servers *before* the S8510 Server takes control.

This migration affects service because you must turn off the S8500 Server before you change over to the S8510 Server.

This migration requires an updated RFA license and authentication file if the S8500 being replaced is on a previous major release (2.x, 3.x, 4.x).

Enterprise Survivable Servers (ESS)

The migration procedures in this chapter can be used for both the main server and an ESS server. If a procedure is used for only one server type it is noted.

For Release 5.x, if the main servers are S8720 Server in an Extra Large (XL) configuration, the ESS must be:

- Upgraded to 5.x *before* the migration of the main server. An ESS must be running the same or a later release than that of the main server.
- An S8510 configured as XL, or an S8720 configured XL, or an S8730.

Note:

All ESS servers must be configured as XL to be compatible with a main server configured as XL. The S8700 ESS servers and the S8710 ESS servers cannot be configured as XL and therefore are not compatible with an S8730 main server or an S8720 main server configured as XL.

Important:

The server type that can be used as an ESS server changes depending on the main server type.

Local Survivable Processor (LSP)

For Release 5.x, if the main servers are an S8720 Server in an Extra Large (XL) configuration, the LSPs must be:

- Upgraded to 5.x *before* the migration of the main server. An LSP must be running the same or later release than that of the main server.
- An S8510 configured as an XL.

Important:

All LSPs must be configured as XL to be compatible with an XL main server.

Prerequisites

Before you start the migration and the server configuration, you must verify that:

- The customer has a local area network (LAN) that is set up and running and a network administrator who is available to assist you on the date of the migration.
- You have the IP addresses and the unique names for the servers.
- You have a new license file and a password file.
- The Services laptop has the correct hardware and software.
  - Windows 2000 or Windows XP operating system
  - 32-MB of RAM
  - 40-MB of available disk space

- An RS-232 port connector
- A network interface card (NIC) with a 10/100BaseT Ethernet interface
- A 10/100 BaseT Ethernet, category 5 (or better), cross-connect cable with an RJ45 connector on each end (MDI to MDI-X)
- A CD-ROM drive

- You have a filled-out Electronic Pre-Installation Worksheet (EPW). For the blank form, see the Avaya Installation Wizard Web site (http://support.avaya.com/avayaiw). The EPW provides:
  - An IP addresses
  - A product ID
  - An Avaya Services telephone number for remote access over modem
  - An Avaya Services IP address for alarms through the network
- You have the current firmware available. Firmware files for the IPSI, the C-LAN, the MedPro, and the VAL and other programmable circuit packs that are available on the Communication Manager distribution CD. For the latest software and firmware, see the Avaya Support Web site http://support.avaya.com. Click **Find Documentation and Downloads by Product Name**.
- You have the login IDs and the passwords to access the S8500 Servers and the server complex components. The password includes the unique service password for that equipment of the customer.

  To obtain the password for a specific server, call ASG Conversant at 9-800-248-1234 or 1-720-444-5557. You must have the IL, FL, or product ID to get the password.

  To log in through the Services port as craft after you install the Avaya authentication file, use this password. This password does not require an ASG challenge or response.

Pre-migration administration

Upgrading media gateways and LSPs

Note:

If the customer does not have media gateways or LSPs, skip these steps and go to Upgrading firmware.

If the configuration is using media gateways and media modules and newer firmware exists for them, you must upgrade the firmware on them first. If the server is the primary controller for a media gateway equipped with an LSP, you must upgrade the software on the LSPs *before* you transfer control to the S8510 Server. The correct order is:

1. Upgrade media gateway firmware to latest version

2. Upgrade media modules firmware to latest version
3. Upgrade the LSP
4. Upgrade the server software to latest version
5. Transfer control to the S8510 Server.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page at http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Select **Query All.**
4. Click **View IPSI Version**.
5. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the TN2313BP IP Server Interface circuit pack that you just installed.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

Upgrading software on the LSP

Although the LSP remains registered with the primary controller, the LSP does not accept translations if it is running an older version of the software than the software that is on the primary controller.

For more information on the software upgrade process, see:

- *Installing and Upgrading the Avaya S8300 Server*, 555-234-100.
- *Installing and Upgrading the Avaya G700 Media Gateway*, 03-603333.

CAUTION:

You may choose to stop call processing on the LSPs during the migration process. If the main server is duplicated server, you can stop call processing on the *active* server. If you do not stop call processing on the LSPs, all calls to the LSPs are dropped.

Performing the migration

The information in this section is based on the assumption that the S8500 Server is installed, configured, and operational and that the S8510 Server is replacing the S8500 Server in the rack.

On the S8500 Server

Clearing the ARP cache on the laptop computer

You might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. This need depends on the operating system on your laptop computer. If you enter an IP address and your computer cannot connect, you might need to clear the cache.

To clear the ARP cache on the laptop:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. To open an MS-DOS command line window, enter **`command`** and press **Enter**.
3. Enter **`arp -d 192.11.13.6`** and press **Enter**. This command produces one of the following responses:
   - The command line prompt displays when the cache is cleared.
   - The message **The specified entry was not found** appears when the specified IP address does not currently appear in the ARP cache.
4. Enter **exit** to close the MS-DOS window.

Clearing the Web browser cache on the laptop

Because of underlying changes on Communication Manager Web pages, you might experience problems with accessing some of the pages. For example, you might see some strange behavior when using the same laptop/PC to switch in-between Communication Manager loads or releases, especially when accessing the Communication Manager server(s) through the Services port (http://192.11.13.6). This is because your web browser is caching information and it does not always know what is new and what is old.

For example, for Communication Manager Release 3.1 and earlier, you log into https://192.11.13.6 and it takes you to https://192.11.13.6/log-in.

But if you are in Communication Manager Release 5.x and you log into https://192.11.13.6, it takes you to https://192.11.13.6/log-in/web-page (or something similar).

The problem is that the laptop gets confused after it has been at Release 5.x and then you want to go to another site in pre-Release 5.x. The system cannot find the old login page.

This happens only if you are switching between releases and/or loads - especially if you go backwards in releases. There does not seem to be a problem going forward in releases.

If you are experiencing problems logging in to Web pages:

1. On the Internet Explorer page, select **Tools** > **Internet Options**.
2. In the Temporary Internet files section, click **Delete Cookies**.
3. Click **OK**.
4. In the Temporary Internet files section, click **Delete files**.
5. Click **OK**.
6. In the History section, click **History**.
7. Click **OK**.

Connecting to the S8500 Server

Use the following steps to connect to the server and access the System Management Interface (SMI):

1. Plug one end of the CAT5 cable into the Services access port on the back of the server.
2. Plug the other end of the CAT5 cable into the NIC on your computer. Use a NIC adapter if necessary.
3. Configure your network connection
   - IP address: 192.11.13.5
   - Subnetwork mask: 255.255.255.252.
4. In the address field of your Web browser, type 192.11.13.6 and hit Enter.

Starting a SAT session (main server only)

Note:

If this is an LSP or an ESS server, go to Copy the configuration information for the S8500.

1. Open a terminal emulation application, such as MS HyperTerminal.

2. Type **192.11.13.6 `5023`** and press **Enter**.
3. Log on as **craft** or **dadmin**.
4. Suppress alarm origination.

Disabling scheduled maintenance

To prevent scheduled daily maintenance from interfering with the migration:

1. Type **`change system-parameters maintenance`**. Press **Enter**.
2. Record the settings for the **Stop Time** and **Start Time** fields.
3. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

   or

   If scheduled maintenance is not in progress, set the **Start Time** field to a time after the migration is completed.

For example, if you start the migration at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to 21:30.

Checking for translation corruption

To check for translation corruption:

1. On the SAT, type **`newterm`** and press **Enter**.
2. If you see the following message:

   Warning: Translation corruption detected . . .

   then follow the normal escalation procedure for translation corruption before continuing the migration.

Saving translations (main only)

The save translation command is release dependent.

Release	Load	Command	Condition
2.0	219.0	save translation lsp	If LSP is present
2.0.1	221.1	save translation lsp	If LSP is present
2.1	411.7	save translation all	If LSP is present
2.1.1	414.1	save translation all	If LSP is present

Release	Load	Command	Condition
2.2	111.4	save translation all	If LSP is present
2.2.1	118.0	save translation all	If LSP is present
3.0 and later	340.3 and later	save translation all	If LSP or ESS is present

To save translations, perform the following step:

Type **`save translation all`** and press **Enter**.

If this operation is unsuccessful, follow the normal escalation procedures before continuing.

Obtaining the product ID on the S8500 Server

To obtain the Product ID:

1. Access the server command line interface.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**. Press **Enter**.
4. Record the product ID and the RMB product ID.

Obtaining the cluster ID

To obtain the cluster ID:

1. At the command line interface, type **`server`** Press **Enter**.
2. Save the output of the command to your laptop using the steps outlined in How to copy the configuration screens

Run almcall

To run almcall:

1. At the command line interface, type **`almcall`** and press **Enter**.
2. Save the output of the command to your laptop using the steps outlined in How to copy the configuration screens

Run almenable

To run almenable:

1. At the command line interface, type **`almenable`** and press **Enter**.

2. Save the output of the command to your laptop using the steps outlined in How to copy the configuration screens

Run modserve

To run modserve:

1. At the command line interface, type **`modsrv -v`** and press **Enter**.
2. Save the output of the command to your laptop using the steps outlined in How to copy the configuration screens

Copy the configuration information for the S8500

Note:

When migrating from an S8500 to an S8510 you cannot use **View/Restore Data** to restore the server and system files, security files, or do a full backup. All configuration data must be obtained from the existing S8500 and recorded for later use.

The configuration information found in the **Communication Manager System Management Interface (SMI)** for the S8500 Server is used to configure the S8510 Server. You cannot complete the migration without this information. You can manually copy the information in each screen (not recommended), copy and save each screen to your computer, or print each screen.

You may also use the EPW to record most of the server configuration data. The AIW with the EPW can be used later to configure the S8510 Server, or the EPW can be used as a reference to configure the S8510 Server when using the Configure Server wizard.

How to copy the configuration screens

Use the following steps to copy each configuration screen. When you choose to copy the screen, each screen can be stored as a separate file on your PC.

1. Create a new folder on your PC to store the configuration files that you copy. Storing the files in a new folder will make them easier to find.
2. You can copy the screens to Word, Wordpad, or Paint. Decide which application you are going to use and open it on your PC.
3. When the configuration screen is displayed on your computer, hit Alt +PrintScrn on your keyboard. The captured screen is copied into the Windows clipboard.
4. Bring up the application you are going to copy the screen into (Word, Wordpad, or Paint):
   a. Left click on your mouse and select **Paste**. The configuration screen should appear in your application window.

b. Click **File** and select **Save As**. Select the folder you created in step 1. In the **File Name** field, change the name of the file to match the configuration screen that you copied. Click **Save**.

Viewing the configuration screens to copy or print

In the **System Management Interface:**

1. Under **Installation** Click **Configure Server**.
2. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.
3. Select the **Configure all services using the wizard** option, then click **Continue**.
4. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Configure ESS/LSP**
   - **Configure Switches**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Set Modem Interface**
   - **Configure RMB**: You will use the RSA or SAMP settings when you configure the RMB on the S8510 Server.
   - **Update System**
5. After copying or printing the Configure Server screens, click **Cancel**. ***Do not*** click **Submit**.
6. Under **Alarms** click on the following links and look for data. If the screens are administered, copy the information or print them.
   - **SNMP Agents**
   - **SNMP Traps**
   - **Filters**

   Note:

   The SNMPV3 authentication password and privacy password does not display on the screen.

Backing up the translation files to the compact flash card

Backing up the translation files to the compact flash card is the preferred method of backup for this migration. Use the **System Management Interface** for this procedure.

1. Connect the cord of the compact flash disk into one of the USB ports on the front of the server.
2. Insert a formatted 128-MB compact flash drive into the drive.
3. On the main menu, under **Data Backup/Restore** click **Backup Now**.
4. Under Data Sets, select **Specify Data Sets** and **Avaya Call Processing (ACP) Translations**. ***Do not*** select any other data sets.
5. Under Backup Method, select **Local CompactFlash Card**.
6. Click **Start Backup** to start the backup process.
7. Under **Data Backup/Restore** click **Backup History** to view the progress of the backup process.
8. When the backup is finished, disconnect the compact flash card reader/writer from the server.

Shutting down the S8500 Server

To shut down the S8500 Server:

CAUTION:
Do not unplug a functioning server unless you first stop all processes. If you unplug a functioning server but do not stop all processes first, you can corrupt the hard disk drive.

1. Under Server, click **Shutdown Server**.
2. Select **Delayed shutdown**
3. Deselect **Restart server after shutdown**.
4. Click **Shutdown**.
5. Wait about 30 seconds.

CAUTION:
Do not press the power button for more than a second. If you hold it down too long, the server reboots.

6. Press and release the power-control button on the front of the server.

The internal fan shuts off.

Disconnecting the cables

Label and disconnect the cables off the back of the S8500 Server. If you are not sure what the cable is, use the **Set Identities** screen that you captured in Copy the configuration information for the S8500 as a reference. For example, if the **Set Identities** screen shows that Control Network A is connected to Eth0, find Eth0 on the S8500 Server, label the cable Control Network A, and then disconnect the cable.

Disconnect the following cables:

1. The laptop from the Services port
2. The power cord from S8500 Server
3. The power cord from the SAMP or RSA
4. The modem from the RS-232 port on the SAMP or RSA card
5. The LAN connection (if used) from the Ethernet port on the SAMP or RSA card
6. The cable(s) from the Ethernet ports

Remove the S8500 from the rack

Use the Quick Start for Hardware Installation: Avaya S8500 Server as a reference.

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

On the S8510 Server

Install the S8510 in the rack

To install the S8510 Server, see *Installing and Configuring the Avaya S8500-Series Server,* (03-300143).

Note:

Do not apply power to the S8510 Server in this step.

Inserting the Communication Manager CD in the CD-ROM drive

Insert the Communication Manager CD/DVD in the optical drive before you apply power to the S8510 server. Use the following steps:

1. Use a paperclip to open the CD-ROM drive on the server. The paperclip is inserted in the Manual Emergency Eject Hole on the CD-ROM drive.

2. Insert the Communication Manager software distribution CD in the drive and close the drive door.

Turning on the S8510 Server

To turn on the server:

1. Connect the AC power cord to the server and to the UPS.
2. If the S8510 does not turn on, push the power button on the front of the server.

Accessing the S8510 Server

To access the server:

1. Clear the ARP cache from the laptop if necessary.
2. Use a cross-connect cable to connect the laptop to the Services port (GB 2).
3. Wait at least 3 minutes after you turn on the server before you start a Telnet session to access the information on the CD-ROM.

Setting up a Telnet session

To set up a Telnet session:

Note:

Use a telnet session to access the information on the CD-ROM.

You can set the Microsoft Telnet application to send a carriage return (CR) and a line feed (LF) whenever you press Enter. The installation program sees this as two key presses. If you are running Windows 2000 or Windows XP, you must correct this before you install Communication Manager to the hard disk.

1. Click **Start** > **Run** to open the **Run** dialog box.
2. Type **`telnet`**. Press **Enter** to open a Microsoft Telnet session.
3. Type **`display`**. Press **Enter** to see the current settings.
4. Perform one of the following actions:

   If the system displays the message **Sending only CR**, or line feed mode which causes the return key to send CR, close the dialog box.

   If the system displays the message **Sending both CR & LF**, or line feed mode causes return key to send CR and LF, continue with step 5.
5. Type **`unset crlf`**. Press **Enter**.

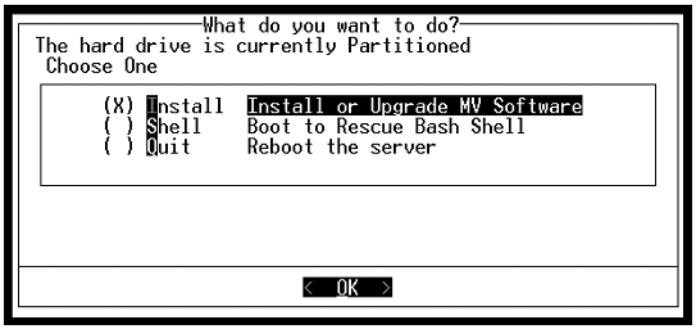
6. Type **`display`**. Press **Enter** to verify that the settings changed. The system displays the message **Sending only CR**.
7. Close the dialog box.

Installing Communication Manager

Use a telnet session to install Communication Manager.

To install Communication Manager:

1. From the laptop Start menu, click **Start** > **Run**.
2. In the **Run** dialog box, type **`telnet 192.11.13.6`** and press **Enter** to view the first screen.



Note:

To navigate on these screens, use the arrow keys to move to an option, and then press the spacebar to select the option. Press **Enter** to submit the screen.

3. Select **Install**, ensure that OK is highlighted, and press **Enter**.
4. On the **Select Release Version** window, ensure that the Build line and OK are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

Once the drive is configured correctly, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

These processes can take up to 20 minutes. When the server is ready to reboot, the CD-ROM drive drawer opens. Remove the CD-ROM from the drive at this time.

The reboot can take up to 3 minutes. The Telnet session ends automatically.

Accessing the System Management Interface (SMI)

To access the Communication Manager System Management Interface:

1. Bypass any proxy servers:
   a. In Internet Explorer, click **Tools** > **Internet Options**.
   b. Click the **Connection** tab.
   c. Click **LAN Settings** in the lower right, then click **Advanced**.
   d. In the **Exceptions** box after the last entry, type 192.11.13.6.
   e. Click **OK** to close each of the dialog boxes.
2. Open the MS Internet Explorer Web browser.
3. If you are connected directly to the server, in the Address field type 192.11.13.6.
4. If you are connected remotely through a modem, in the Address field type in the IP address or the DNS host name of the server.

   Note:

   The first time you log in, you see a message asking you to install a security certificate. Accept the certificate. You can also install the certificate on your computer with the instructions in the online Help for your browser.

5. When prompted, log in.
6. When you see a message asking if you want to suppress alarms, select **Yes**.

Verify date, time, and timezone

Use the System Management Interface to change the date and time:

1. Under **Server**, click **Server Date/Time**.
2. Change the date, time, and time zone as needed.
3. Click **Submit** to effect the changes.

Important:
If you set the time zone, you ***must*** reboot the server.

Copying files to the S8510 Server

Use the **System Management Interface** to copy license files and authentication files, service packs, and SAMP update files from the Services laptop to the S8510 Server. You are not installing the files using this step, just transferring them from your PC to the server.

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the Choose File window on your computer. Find the files that you need to copy to the media server.
4. Click **Download** to copy the files to the media server. The files are automatically copied to the default file location.

Installing service pack updates, if any

Use this procedure to unpack and activate Communication Manager service pack updates.

1. Under **Server Upgrades**, select **Manage Updates**.

   If an update file you want to activate shows **packed** in the **Status** column, select the file in the **Update ID** column and click **Unpack**.

   The window shows the status of the unpacking.

   When the system displays the message **Unpacked Successfully**, click **Continue**.

   If the update ID file you want to activate shows **unpacked** in the **Status** column, select the file in the **Update ID** column and click **Activate**.

   The screen shows the status of the update. If the update requires a reboot, the system automatically reboots.

2. Click **Yes**.

3. When the system displays the **Continue** button, click **Continue**.

   The system displays the status of the update.

Creating a super-user login

Note:

A craft-level login can create the super-user login in Release 4.0 or later.

Make sure you have a login name and password that the customer would like for the superuser login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Use the **System Management Interface** to create a super-user login.

To create a login:

Note:

Make sure the customer can change this login, its password, or its permissions later.

1. Under **Security**, select **Administrator Accounts**.
2. Select **Add Login** and **Privileged Administrator** and click **Submit**.
3. In the **Login name** field, type a login name for the account. The following fields and values appear.

   Primary group: susers

   Additional groups (profile): prof18 (*prof18* is the code for the customer superuser).

   Linux shell: /bin/bash

   Home directory field: /var/home/login name (login name is the name you typed earlier.
4. Skip the **Lock this account** and **Date on which account is disabled-blank to ignore** fields.
5. In the **Select type of authentication section** select **Password**.

   Note:

   Do not lock the account or set the password to be disabled.
6. In the **Enter key or password** field and the **Re-enter key or password** field, type the password.
7. In the **Force password/key change** on next login section, leave the radio button set to the no default.
8. Click **Submit**.

Configuring the S8510 Server

The information contained in the configuration files and the SNMP screens that you printed or saved to your PC is used when you configure the S8510 Server.

The S8510 Server can be configured with one of the following methods:

- Manually enter the configuration data using the **System Management Interface** > **Installation > Configure Server**. You can use the EPW, an Excel spreadsheet, as a planning form.
- Manually enter the data into EPW and use the Avaya Installation Wizard to import the configuration information to the server. For more information on the Avaya Installation Wizard, see About the Avaya Installation Wizard and Configuring the S8510 using the Avaya Installation Wizard.
- Manually enter the data while using the Avaya Installation Wizard. If you use the Avaya Installation Wizard to configure the server, some additional configuration must be entered using the **System Management Interface** > **Administration** > **Server (Maintenance)** > **Server Configuration**. For more information see About the Avaya Installation Wizard and Configuring the S8510 using the Avaya Installation Wizard.

About the Avaya Installation Wizard

Use the Avaya Installation Wizard to:

- Set the date/time and timezone
- Configure the server
- Configure the Remote Maintenance Board
- Install the license file

  Note:

  To install the license file the server does not have to be connected to the reference IPSI. However, you have only 30 minutes before the system checks the serial number on the IPSI. To add another 30 minutes, type **`reset system 1`** and press **Enter** in a SAT session to restart the Communication Manager software.
- Install the Avaya authentication files
- Install software updates
- To use the Installation Wizard, you can either:
- Import the data from the completed *Electronic Preinstallation Worksheet* (EPW) that was filled out using the configuration information from the S8500A. When the Installation Wizard prompts you to import the Preinstallation Worksheet, click **Import EPW** and browse to the location of the EPW file on your Services laptop computer. The Installation Wizard opens the EPW and uploads the configuration data.

- Type the information manually with the completed EPW as a guide. The Installation Wizard prompts you to enter the configuration data for each step in the Configure Server section.

It is possible that additional fields will appear in Release 5.2 that did not exist on the earlier Communication Manager release running on the S8500 Server:

- Processor Ethernet: In the Set Identities screen you can assign the Processor Ethernet to an interface.
- Configure Memory: In the Configure ESS/LSP screen there is a Configure Memory heading. Under the Configure Memory heading there are two options, Standard, and Extra Large. You must select one of the options if the server is configured as an LSP or ESS server. The Extra Large option is only selected if the main server is configured as Extra Large.

Configuring the S8510 using the Avaya Installation Wizard

1. With the Web browser open, type **`192.11.13.6`** and press **Enter** in the browser address window to display the login page.
2. Log in as **`craft`** and use the initial craft password.
3. Click **Avaya Installation Wizard**.
4. Follow the prompts. For more information use **Help** on each page.

   Note:

   After you finish using the Avaya Installation Wizard (AIW), you must perform additional configuration steps.
5. If this server is an LSP or an ESS server with a main server that is configured as XL:
   a. On the **Configure ESS/LSP** page verify that the:
      - Appropriate radio button (ESS/LSP/or none) is turned on for the server type.
      - IP addresses are correct for registration and file synchronization.
      - Extra Large radio button is selected under the Configure Memory heading.
6. To configure the SAMP, use the Configure Server Web pages.

Configuring the S8510 using the Configure Server web pages

You can manually enter the configuration information using the System Management Interface (SMI):

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.
3. Select **Configure all services using the wizard** and click **Continue**.

4. The wizard steps you through each configuration screen. Enter the configuration information that you obtained from the S8500 Server in the appropriate screens and update the system.

   If this server is an LSP or an ESS server behind a main server that is configured as XL, on the **Configure ESS/LSP** page verify that the:

   - Appropriate radio button is turned on for the server type.
   - IP addresses are correct for registration and file synchronization.
   - Extra Large radio button is selected under the **Configure Memory** heading.

License File (if not installed with AIW)

To install the RFA license file using the System Management Interface (SMI):

1. Under **Security** click **License File**.
2. Select either:
   - **Install the license file I previously downloaded** if you have already downloaded the file to this server
   - **Install the license file specified below** and then browse the connected computer for the license file.
3. Click **Submit**.

Authentication File (if not installed with AIW)

To install the authentication file using the System Management Interface (SMI):

1. Under **Security** click **Authentication File**.
2. Select either:
   - **Install the Authentication file I previously downloaded** if you have already downloaded the file to this server
   - **Install the Authentication file specified below** and then browse the connected computer for the license file.
3. Click **Install**.

   Note:

   The system responds with a successful message. If you get a filesync failed message, ignore it.

Product ID (if not installed with AIW)

Note:

If not set using AIW, then you need to set the product ID.

To set the Product ID:

1. Access the server command line interface.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt type **`productid -p`** *##########* where **`productid`** is the Product ID that you received from the customer or the ART tool and *##########* is the 10-digit number.
4. Press **Enter**.
5. At the prompt type **`productid -r`** *##########* where **`productid`** is the Product ID of the SAMP and *##########* is the 10-digit number.

Reboot the server

Important:
Set the timezone before this reboot and do not change the timezone after the reboot.

It is necessary to reboot the server to initialize server settings that are restored but not yet activated.

To reboot the server:

1. On the System Management Interface (SMI), under **Administration** > **Server (Maintenance) > Server**, click **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Select **Restart server after shutdown**.
4. Click **Shutdown**.

Wait about 3 minutes.

Connecting the network cables

Use the **Configure Server Set Identities** screen that you copied in Copy the configuration information for the S8500, and *Front view of S8510 Server* and *Back view of S8510 Server* as a guide to connect the cables to the S8510. For example, if the **Set Identities** screen from the S8500 indicated that Control Network A was connected to Ethernet 0, you would connect the cable labeled Control Network A to Ethernet 0 on the S8510 Server.

Note:
The IPSIs and the port networks reset automatically. The approximate out-of-service time is 5 minutes and then call processing might be on the S8510 Server.

After approximately 30 minutes, verify that the system is functioning satisfactorily. Check and clear alarms.

Connecting the SAMP cables

The SAMP card is installed in PCI-e slot 1 of the S8510 Server and is powered externally. The SAMP supports one USB interface and two 10/100 Ethernet ports that are located on the back of the S8510 Server. See Figure 20 for connectivity.

Figure 20: SAMP Connections

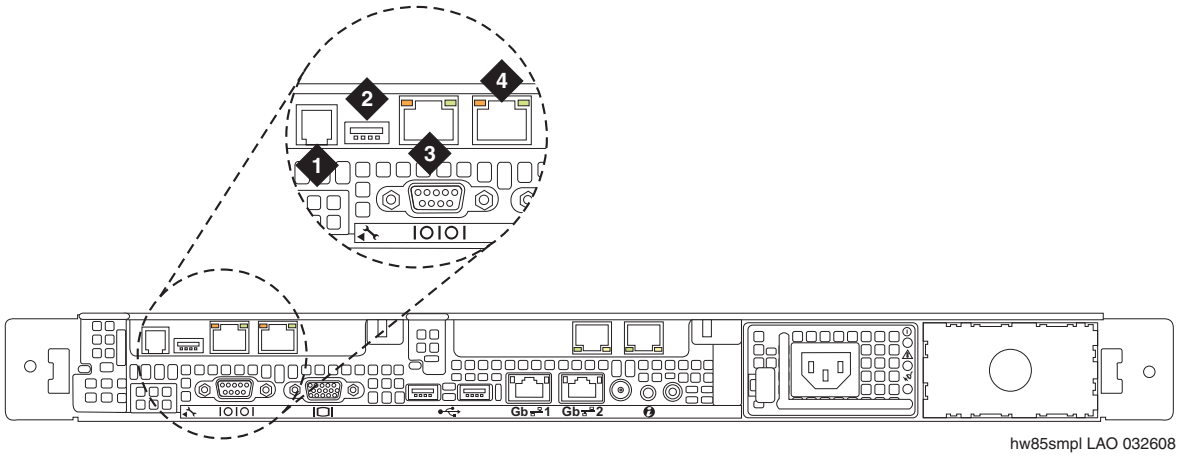


Figure notes:

1. **External Power Supply**
2. **USB Port for Modem**
3. **Not Used (Eth 1)**
4. **Services Port (Eth 2)**

Verifying the server connection to the customer LAN

To verify connectivity:

1. Using Internet Explorer, connect to the S8510 Server.
2. Log in as **craft**
3. Click **Administration > Server (Maintenance)**.
4. Under Diagnostics click **Ping.**
5. Under Endpoints to Ping select **All IPSI's**, **UPS's** to verify connectivity to these units.
6. Click **Execute Ping**.
7. Verify that all endpoints respond correctly.

Enabling firewall settings

The firewall settings should have been completed by the Installation wizard. For the media server to receive SNMP traps from the UPS and the Avaya Ethernet switch, the snmptrap,162/udp port must be enabled. Verify that the port is enabled on the **System Management Interface (SMI)**:

1. Under **Security**, click **Firewall**.
2. Scroll down to the snmptrap 162/udp row and select the **Input to Server** box.

   The **Output to Server** box can be left as is, either selected or clear.
3. Click **Submit**.

Restoring SNMP configuration (if needed)

If there was data for SNMP agents, traps, or filters copied or printed from the S8500 Server, enter the information in the S8510 Server. You may have to obtain the SNMPV3 authentication password and the privacy password from the customer before proceeding.

1. Under **Alarms** click **SNMP Agents** and complete the fields.
2. Under **Alarms** click **SNMP Traps** to add the trap destination(s).
3. Under **Alarms** click **Filters** to add the filters.

Installing SAMP firmware

You might need to update the SAMP firmware if the most current version is not installed. Information about the versions that require updates should be included in your project planning information.

For information on how to update the firmware on the SAMP installed on the S8510 Server, see *Avaya Server Availability Management Processor (SAMP): Avaya S8510 Server* (03-602923).

Restoring the translations (main server only)

Use this procedure to restore translations on the main server only. If this is an LSP or ESS server, go to Testing the system using SAT commands. After the LSP or ESS server registers with the main server, the main server sends a copy of the translations to the LSP or ESS server.

To restore the translations to the S8510:

1. Connect the compact flash reader/writer cord to either USB port on the back or the front of the server.
2. Insert the compact flash card with the backed-up translations into the bottom slot of the drive.
3. Under **Data Backup/Restore**, click **View/Restore Data**.

4. Select **Local CompactFlash Card**.
5. Click **View**.

   Important:
   Do not attempt to restore a file name that starts with a os_ or full_. Restore the *.xln file only.

6. Select the correct translation file and both **Force** options.
7. Click **Restore**.
8. Click **Restore History** and select the desired file that you want to restore.
9. Click **Status** to view the Restore status.

When the restoration is complete, the system displays the following message:

backup: 0: restore of <filepath/filename> completed successfully.

Reset the system

To reset the system:

1. Start a SAT session and log in.
2. Type **`reset system 4`** and press **Enter**.

Testing the system using SAT commands

To test the system:

1. Start a SAT session.
2. Type **`list station`** and press **Enter**.

   Verify that the stations on this server are the same as the stations that were on the S8500 Server.

3. Perform the necessary administration. For example, use the **`add duplication administration`** command.

Testing the system using the System Management Interface (SMI)

To test the system:

1. Using Internet Explorer, log into the S8510 Server.
2. Click **Administration > Server (Maintenance)**.

3. Under **Server** click **Status Summary**. Verify that the Server Hardware and the Processes fields say okay.
4. Under **Diagnostics** select **Ping**
5. Under Endpoints to Ping, select **All IPSIs, UPSs**
6. Click **Execute Ping**
7. From a computer on the customer LAN, use Internet Explorer to connect to the S8510 Server.
8. Log in as **craft**

This action verifies that connectivity exists and that the customer can log in to perform administration or other tasks.

Resolving alarms

To resolve alarms:

1. Under Alarms, click **Current Alarms**.
2. Under Server Alarms, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the migration. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431).
   - *Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers, (03-300430).*

Enabling alarms to INADS by way of a modem

1. Start an SSH session on the server.
2. Type **`almenable -d b`** and press **Enter**.
3. To verify that the alarms are enabled, type **`almenable`** and press **Enter**.

Enabling alarms to INADS by way of the SNMP module

Note:

Perform this procedure only if the installation includes a Secure Service Gateway (SSG).

To enable alarms on the servers:

1. Start an SSH session on the server.

2. Type **`almsnmpconf -d`** ***`ipaddress`*** **`-c`** ***`communityname`*** and press **Enter**, where ***`ipaddress`*** is the trap receiver address for the SSG device and ***`communityname`*** is the community string name that the SSG device requires.
3. Type **`almsnmpconf`** and press **Enter** and verify that the correct information is entered.
4. Type **`almenable -s y`** and press **Enter**.
5. Type **`almenable`** and press **Enter** and verify that alarm origination is enabled on the SNMP module. If used, also verify that alarm origination by way of a modem is still enabled.
6. Log off.

Enable the modem to receive calls

To enable the modem to receive calls:

1. Use the System Management Interface and click **Modem** under the **Security** heading.
2. Select the desired setting for accessing the system through the modem.

Enabling scheduled maintenance

To schedule daily maintenance:

- Reset the settings that were recorded in Disabling scheduled maintenance.

Checking for translation corruption with the SAT

To check for translation corruption, type **`newterm`** and press **Enter**.

If you see the following message

Warning: Translation corruption detected

follow the normal escalation procedure for translation corruption.

If no corruption is detected, continue with Saving translations (main server only).

Saving translations (main server only)

Enter **`save translation all`**. Press **Enter**.

If this operation is unsuccessful, follow the normal escalation procedures before continuing.

Backing up files to the network

To back up files to a server on the network:

1. Under **Data Backup/Restore**, click **Backup Now**.

2. Under **Data Sets**, click **Full Backup**.
3. Under **Backup Method**, select the backup method.
4. Fill in the fields **User Name**, **Password**, **Host Name**, and **Directory**.
5. Click **Start Backup** to start the back up process.

Releasing alarm suppression (optional)

If you complete the migration well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait.

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **craft** or **dadmin**.
3. Type **`almsuppress -n`**. Press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the S8510 Server

Unplug the laptop from the services port.

Migrating an Avaya S8400 Server to an S8500-Series Server

Use these procedures to migrate from an existing Avaya S8400 Server to the Avaya S8500-Series Server. The existing S8400 server must be standard reliability. In a new installation, the S8400 Server is installed only in the Avaya G650 Media Gateway. In a migration, the server is installed only in the G600 and CMC1 Avaya Media Gateways.

To migrate an existing S8400 Server, remove the TN8400 S8400 Server circuit pack and replace the S8412AP IP Interface circuit pack with one TN2312BP IPSI circuit pack to control the one port network (PN).

This migration affects service because you must power down the media gateway to remove the TN8400 Server and replace the TN812AP SIPI circuit packs.

Important:

The S8500A Server is not supported on Communication Manager 5.0 and later releases. Refer to the table of Server Migration Paths on page 50 for possible migrations that include Communication Manager Release 5.2.

Checklists

Before you go on site, perform the following tasks:

:

✓	Task	Description
	Verify that your Services laptop has the appropriate hardware.	Correct hardware components include: ● 40 MB available disk space ● direct Ethernet cable ● serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● CD-ROM drive
	Verify that your Services laptop has the appropriate software.	Correct software components include: ● Windows 2000/XP operating system ● Terminal emulation program: HyperTerminal or other ● TCP/IP networking software: bundled with the Windows OS ● Web browser: Internet Explorer 5.0 or later
	Obtain appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the equipment of the customer.
	Obtain the serial number of the servers, if necessary.	You need a new license file and authentication file. You need the serial number from the reference SIPI or IPSI and the SAP order number to generate a new license file and authentication file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	You use this CD to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your laptop	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your laptop	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current firmware.available	The following firmware are on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs For the most current versions, go to the Avaya Support Web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download license and authentication files to your Services laptop.	New license file and authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) Web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	Verify that you have copied all necessary files to your computer	These files can include: • service packs • license file • authentication file • firmware for programmable circuit packs
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

Before you go on site for a migration, complete the following additional tasks before starting the migration:

✓	Task	Description
	About 2 weeks before the migration, freeze the translations. Use a spare flash card to collect the translations locally.	For more information on where and how to send the translations, contact the STS scheduling desk at 720-444-9418. STS updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For forms and more information, contact the STS scheduling desk at 720-444-9418.
	About 2 business days before the migration, create a trouble ticket to contact the STARS team.	Whenever an S8400 server is upgraded from R3.1 onwards, and a new authentication file is requested, ASG access (remote and on-site) is impacted. You need assistance from the Service Tools and Application Remote Support (STARS) team to ensure successful ASG access before and after the upgrade. To contact the STARS team, use http://stars.avaya.com/ticket/requests/request.asp
	Mark the ticket status as CRITICAL.	Indicate text in the ticket to notify the STARS team that you are upgrading an S8x00 server. Include the date of the upgrade and the FL and product or alarm ID of the system. The STARS team contacts you on how to access your product before and after the upgrade. A temporary ASG product ID is created for you and your team to use for access during the time of the upgrade.
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.

✓	Task	Description
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.
	Copy the translation file from STS to a directory on the Services laptop.	File size is usually in the range of 1-4 megabytes.

2 of 2

On site migration checklist

Before you go on site for a migration, complete the following additional tasks before starting the migration:

✓	Task	Description
	The customer supplies an open EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack. Verify that this rack is installed correctly.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on how to install the rail, see the documentation that comes with the rail kit.
	Verify that you have the license file that the file includes the licensed features.	Use the License File link on the System Management Interface (SMI) to verify.
	Verify that you have the Avaya authentication file.	Use the Authentication File link on the System Management Interface (SMI) to verify.

Documentation checklist for migrations

For a list of documents that Avaya recommends you have on hand for the migration, see Resources on page 35.

You also need the following additional documentation:

✓	Task	Description
	Quick Start for Hardware Installation: Avaya S8500-Series Media Server (555-245-701)	A quick reference guide that provides physical installation and connection information.
	Installing and Configuring the Avaya S8500-Series Media Server (03-300143)	Provides installation instructions for the S8500-Series Server.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.
	Installing the Avaya S8510 Server Family and Its Components (03-602918)	Provides installation instructions for the S8510 Server and Its Components

Performing a migration

The information in this section assumes that the S8500-Series Server complex is installed, configured, and operational. See the appropriate books for information on physically installing the server and installing and configuring Communication Manager.

CAUTION:

This migration affects service. When the port network is turned off, the system drops all calls. Service returns when the port network is powered up and the S8500-Series Server takes control of it.

Note:

You must install the Communication Manager license on the S8500-Series Server before the migration is completed.

Premigration administration

This migration is a service-affecting event. The S8400 Server must be turned off to remove the TN8400 Media Server and TN8412AP S8400 IP Interface circuit packs. Before you turn off the port network, you must perform the following premigration administration.

Connecting to the server

To connect to the server:

1. Connect the computer to the services port on the front of the server.
2. Start a SAT session using Native Configuration Manager or Avaya Site Administration.
3. Log in as **craft**.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:
   a. **`list configuration all`**
   b. **`list trunk-group`**
   c. **`list hunt-group`**

   If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.
2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

Although the migrated translations are already copied to the server, you must save the translations in case you need to back out of the migration.

Note:

Save translations to a flash card.

To save translations:

1. To save translations to the system disk, type **`save translation`**. Press **Enter**.

   The system responds with **Command successfully completed**.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

   If you experience trouble connecting to the Web page, go to Clearing the Web browser cache on the laptop on page 230.

Backing up recovery system files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Select the data sets, including **Avaya Call Processing (ACP) translations** and **Save ACP translations prior to backup**. Do *not* select **Full Backup** because this option does not save translations.

   Note:

   If you back up to a compact flash, Avaya recommends that you use a different flashcard from the one with the prior release translations. You might need these translations if you need to back out of the upgrade, migration, or conversion procedure.
3. Select **FTP** as the backup method and complete the necessary information.

4. Click **Start Backup** to start the back up process.

Migration tasks

You can reuse the translations from the existing system when you migrate to an S8500-Series Server.

Note:

You must install the new Communication Manager license file on the server before you make the change or the system will not run.

Verifying hardware

Ensure that you have the migration specific hardware on hand.

Turning off the power to the port network

CAUTION:

Ensure that you have completed the premigration administration. For more information, see Premigration administration on page 388.

To turn off power:

1. From the bash prompt on the Services laptop, type **shutdown system** and press **Enter** to perform a graceful shutdown.
2. Wait until the Shutdown Complete LED on the lower portion of the faceplate of the Server is solid green
3. Turn off the power to all media gateways. Unplug the power cord for safety purpose.

   Note:

   Gateways with the TN8400 and TN8412 needs to be powered off. The other carriers may remain powered on.

DANGER:
The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the media gateway, pull the AC power cord from the back of the media gateway.

Shutting down the Avaya S8400 Server and powering down the Media Gateway

To shut down the Avaya S8400 Server:

1. Perform a complete server backup to the LAN or to the translations Compact Flash card (front slot of the Avaya S8400 Server).
2. Push and hold the Shutdown button (Note 1 in Figure 21: Avaya S8400 front faceplate) for more than two (2) seconds

Figure 21: Avaya S8400 front faceplate

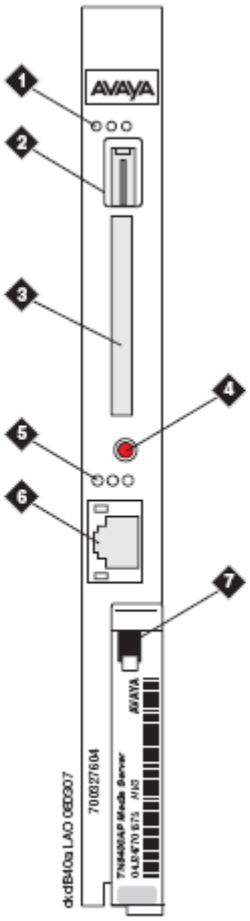


Figure notes:

1. **Shutdown button (hold for more than 2 seconds)**
2. **OK to Remove LED**
3. **Safety latch**
4. **Compact Flash slot for translations**
5. **Circuit pack failure LED (red)**

The green OK to Remove LED (Note 2 in Figure 21) flashes to indicate that shutdown is in progress.

3. When the green OK to Remove LED is on steady unlatch the circuit pack (Note 3 in Figure 21), slide it out of its slot, and set it on the antistatic mat.
4. Leave the Compact Flash card with translations in the slot (Note 4 in Figure 21).

Note:

The Avaya S8400 Server has a cable adapter attached at the rear of the carrier. Leave this adapter and its cable connections in place during the entire replacement procedure.

Removing the TN circuit packs

To remove both the circuit packs:

1. Release the latch that secures the circuit pack.
2. Pull the circuit pack straight out of the slot and free of the media gateway.

   Important:

   Remember which slot that the TN8412AP circuit pack was located. The TN8412AP Server IP Interface (SIPI) location configuration is different depending on the media gateway in which it resides.

3. Remove the cable(s) connected to the adapters first. Remove the adapters for the circuit packs from the rear of the media gateway. You can reuse the cable that connects to the TN8412AP Server IP Interface (SIPI) adapter but you won't need the cables connected to the S8400 server.

   Note:

   You can also reuse the TN8412AP Server IP Interface (SIPI) adapter for the IPSI.

Installing the IPSI

To install the IPSI:

1. Insert the TN2312BP IPSI circuit pack in the former location of the TN8412AP.
2. Install the TN2312BP IPSI adapter on the rear of the media gateway in the former location of the TN8412AP Server IP Interface (SIPI) adapter.
3. Connect the Ethernet cable into the IPSI adapter.

Turning on power to the port network

To turn on power to the port network:

1. Plug in the power cord to the back of the media gateway.
2. Push in the latch on the power supply to start power.
3. Plug one end of the power cord into the back of the power supply and the other end into a UPS or nonswitched outlet.

Turning on G650 Media Gateway

To connect the power cords:

1. Ensure that the circuit breakers at the AC load center are OFF.
2. Connect the G650 Media Gateway to a UPS or to an electrical outlet that is “nonswitched” or “always on”

   Note:
   Remove the emergency ground wire if used.

Checking AC power:

Each G650 Media Gateway uses at least one auto-ranging (90-VAC to 265-VAC) power supply:

- 47 to 63 HZ
- 500 W output
- 7.2 A (90 VAC) or 3.3 A (200 VAC)

Connecting to DC power

Each G650 Media Gateway can be equipped with a maximum of two 655A power supplies. One power supply is always provided in slot 0, and a redundant unit can be provided in slot 15. DC power is supplied by a DC feed cable to one connector on the backplane of the G650 Media Gateway. The power is then bussed to each power supply slot. AC current and DC current can be supplied to the 655A power supplies at the same time. When both AC current and DC current are present, the 655A uses AC first. The 655A power supply then changes to DC current without any interruption in service if the AC current fails.

Each G650 Media Gateway, with either a single power supply or redundant power supply, draws a maximum of 17 A of DC current.

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 22: Connecting directly to the IPSI on page 325).

Figure 22: Connecting directly to the IPSI

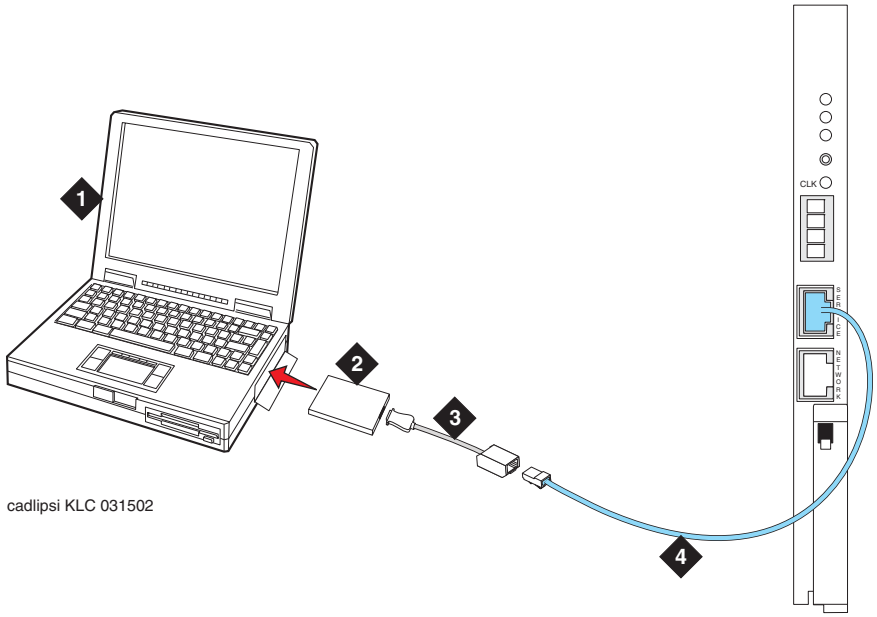


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Clearing the ARP cache on the laptop computer

You might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. This need depends on the operating system on your laptop computer. If you enter an IP address and your computer cannot connect, you might need to clear the cache.

To clear the ARP cache on the laptop:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. To open an MS-DOS command line window, type **`command`** and press **Enter**.
3. Type **`arp -d 192.11.13.6`** and press **Enter**. This command produces one of the following responses:
   - The command line prompt displays when the cache is cleared.
   - The message **The specified entry was not found** appears when the specified IP address does not currently appear in the ARP cache.
4. To access the server, type **`ping -t 192.11.13.6`** and press **Enter**.

   The **`-t`** causes the ping to repeat until you get a response. When you get a response, in about 3 minutes, wait an additional 30 seconds before you go back to the Web interface.
5. To stop the ping, type **`ctrl c`** and press **Enter**.
6. Close the MS-DOS window.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application to access the IPSI using the secure shell (SSH) protocol.

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.
2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **craft**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **show control interface** and press **Enter**.
2. To see the current settings, type **show port 1** and press **Enter**.
3. Type **set control interface *ipaddr netmask***, where ***ipaddr*** is the customer-provided IP address and ***netmask*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. To save the changes and exit the IPSI session, type **quit** and press **Enter**.
5. SSH to **192.11.13.6** and log in.
6. Type **show control interface** and press **Enter**.
   The system displays the IP address, the subnetmask, and the default gateway information.
7. Verify that the correct information was entered.
8. If a default gateway is used, enter the gateway IP address.
   Type **set control gateway *gatewayaddr***, where ***gatewayaddr*** is the customer-provided IP address for their gateway and press **Enter**.
9. To save the changes and exit the IPSI session, type **quit** and press **Enter**.

10. SSH to **192.11.13.6** and log in.
11. To verify the administration, type **`show control interface`** and press **Enter**.
12. To see the changes, type **`exit`** and press **Enter**.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

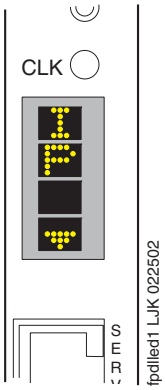
   Note:

   Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

   Note:

   The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.
2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 23: LED display that shows that the IPSI has a static IP address on page 328).

Figure 23: LED display that shows that the IPSI has a static IP address



Note:

Clear the ARP cache on the laptop before you connect to another IPSI. If you do not clear the cache, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

Postmigration administration

Perform the following tasks to complete postmigration administration.

Clearing the Web browser cache on the laptop

Due to underlying changes on Communication Manager Web pages, you might experience problems with accessing some of the pages. For example, you might see some strange behavior when using the same laptop/PC to switch in-between Communication Manager loads or releases, especially when accessing the Communication Manager server(s) through the Services port (http://192.11.13.6). This is due to how your web browser is caching information and it does not always know what is new and what is old.

For example, for Communication Manager Release 3.1 and earlier, you log into https://192.11.13.6 and it takes you to https://192.11.13.6/log-in.

But if you are in Communication Manager Release 4.0/4.1 and you log into https://192.11.13.6, it takes you to https://192.11.13.6/log-in/web-page (or something similar).

The problem is that the laptop gets confused after it has been at Release 4.0/4.1 and then you want to go to another site in pre Release 4.0. The system cannot find the old login page.

This happens only if you are switching between releases and/or loads - especially if you go backwards in releases (for example, from Release 4.1 on Server 1 to Release 3.0 on Server 2). There does not seem to be a problem going forward in releases.

If you are experiencing problems logging in to Web pages:

1. On the Internet Explorer page, select **Tools** > **Internet Options**.
2. In the Temporary Internet files section, click **Delete Cookies**.
3. Click **OK**.
4. In the Temporary Internet files section, click **Delete files**.

5. Click **OK**.
6. In the History section, click **History**.
7. Click **OK**.

Connecting to the server

To connect to the server:

1. Connect one end of the CAT5 cross-over cable to the Services port on the S8500-Series Server.
2. Connect the other end of the cable to the Services laptop.

Clearing the ARP cache on the laptop computer

You might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. This need depends on the operating system on your laptop computer. If you enter an IP address and your computer cannot connect, you might need to clear the cache.

To clear the ARP cache on the laptop:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. To open an MS-DOS command line window, type **`command`** and press **Enter**.
3. Type **`arp -d 192.11.13.6`** and press **Enter**. This command produces one of the following responses:
   - The command line prompt displays when the cache is cleared.
   - The message **The specified entry was not found** appears when the specified IP address does not currently appear in the ARP cache.
4. To access the server, type **`ping -t 192.11.13.6`** and press **Enter**.

   The **`-t`** causes the ping to repeat until you get a response. When you get a response, in about 3 minutes, wait an additional 30 seconds before you go back to the Web interface.
5. To stop the ping, type **`ctrl c`** and press **Enter**.
6. Close the MS-DOS window.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

   If you experience trouble connecting to the Web page, go to Clearing the Web browser cache on the laptop on page 230.

Migrating translation files

To migrate translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Network Device** and complete the necessary information
   - **FTP**
   - User name
   - Password
   - Host name
   - Directory.
3. Select the translation file you created back in Premigration setup on page 312.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.
5. Click **Restore** to restore the translation files.
6. Click **Restore Status**.
7. Select the first file and then scroll down and click **Review Status** to see the results of the restore.

   When the restore process completes, the screen displays **Restore is finished**.
8. Type **`reset system 4`**. Press **Enter** to load the restored translations.

If the restore process fails, the system displays an error message that states the reason for the failure. The translation file is not restored. You must resolve the reason for the failure and restart the process.

Starting a SAT session

To start a SAT session:

1. Open a terminal emulation application, such as MS HyperTerminal.
2. Type **192.11.13.6 `5023`** and press **Enter**.
3. Log on as **craft** or **dadmin**.
4. Suppress alarm origination.

Note:

Use Native Configuration Manager or Avaya Site Administration to start a SAT session.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "1" shows in any position, you must troubleshoot the problem.

   Tip:

   The pattern `0.1.1.0` usually means that a media gateway is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

3. The IPSI translations may need to be modified depending on the previous TN8412AP Server IP Interface (SIPI) circuit pack translations (using internal addresses).
   - If the TN8400 was directly connected to the TN8412, then you need to provide a network address for the new IPSI. See Setting the control interface on page 327.
   - If the TN8412AP Server IP Interface (SIPI) was directly connected to the customer network, then no further translations are needed.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct media gateway and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed media gateways

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the media gateways. Verify that the screen shows the media gateway number that is assigned to the changed media gateways.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the media gateway number of the changed media gateway and press **Enter**. Under Carrier Description, Carrier Type, verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page(http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see Upgrading firmware on the IPSIs and SIPIs on page 315.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see Upgrading firmware on the IPSIs and SIPIs on page 315.

Testing the installation

Test the complete installation. For more information, see *Installing and Configuring the Avaya S8400 Server Release 5.0 (03-300678) and/or visit: http://support.avaya.com*

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Checking for translation corruption

To check for translation corruption:

1. On the SAT, type **`newterm`** and press **Enter**.
2. If you see the following message:

Warning: Translation corruption detected . . .

then follow the normal escalation procedure for translation corruption before continuing the upgrade.

Resolving alarms

To clear alarms:

1. On the System Management Interface (SMI), under **Alarms**, click **Current Alarms** to examine the alarm log.
2. Select the server alarms that you want to clear and click **Clear**, or click **Clear All.**
3. Resolve or clear Communication Manager alarms with SAT commands and the Maintenance Commands Reference and Alarms Maintenance books.

Backing up system files

To back up the system files:

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Select the data sets, including **Avaya Call Processing (ACP) translations** and **Save ACP translations prior to backup**. An ESS server or an LSP gets translations from the main server, so there is no reason to back up the translations on an ESS server or an LSP. Do not select **Full Backup** because this option does not save translations.

   Note:

   If you back up to a flashcard, Avaya recommends that you use a different flashcard from the one with the prior release translations. You might need these translations if you need to back out of the upgrade, migration, or conversion procedure.
3. Select the backup method.
4. Click **Start Backup** to start the back up process.

Logging off all administration applications

- When you complete all the administration, log off all the applications that you used.

Registering Communication Manager

- Follow standard procedures to register the new software.

Troubleshooting the migration

For more information, see *Installing and Configuring the Avaya S8400 Server Release 5.0 (03-300678), and/or visit: http://support.avaya.com*

Returning replaced equipment

Once you determine that the port network functions, return the TN8400 S8400 Server circuit pack and any other replaced equipment to Avaya. Use established procedures.

Chapter 4: Migrating to an Avaya S8730 Server

This chapter describes how to migrate from an existing DEFINITY and Linux system to the Avaya S8730 Server.

Important:

S8700 Servers cannot be upgraded to Communication Manager 5.0 or later releases. For Communication Manager 5.0 and later releases, an S8700 Server must migrate to an S8730 Server (only path supported). For more information on how to migrate the S8700 Server see:

- Migrating from an S8700, S8710 or S8720 to an S8730 Server on page 525

The most common migrations are from non-Linux-based systems to Linux-based servers. Non-Linux-based systems include systems such as the DEFINITY ONE/S8100. Less common migrations include migrations from one Linux-based server to another. Not all non-Linux-based systems can migrate to a Linux-based server. Whether you can migrate a system depends on the supported migration path. A *migration path* refers to the platform and the software release from which you can migrate to the new platform.

Migrations from existing DEFINITY and Linux platforms

Use these procedures to migrate from existing DEFINITY and Linux platforms to the Avaya S8730 Server configuration with limited out-of-service time. The S8730 Server can be either a fiber-port network connectivity (PNC) configuration or an IP-PNC configuration or both.

Note:

Once you complete the migration to fiber-PNC, you can convert to IP-PNC.

You can migrate the following existing systems to an S8730 Server:

- DEFINITY Server R in a multicarrier cabinet (MCC)
- DEFINITY Server SI in a single carrier cabinet (SCC) or a multicarrier cabinet (MCC)
- Avaya IP600 (S8100) in a G600 Media Gateway
- DEFINITY ONE (S8100) in a compact modular cabinet (CMC)
- DEFINITY Server CSI in a CMC1 Media Gateway

You can migrate the following existing Linux systems to an S8730 Server:

- S8400
- S8500
- S8700
- S8710
- S8720, S8720XL

Hardware migrations

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

DEFINITY Server R or SI in an MCC

The migration process depends on whether the migration is to an S8730 Server with a CSS/ATM or direct-connect configuration.

S8730 MC:

If all the port networks (PNs) are connected through a CSS or ATM, Avaya recommends that you first replace the following components before you start the migration:

- Tone clocks with TN2312BP IPSI circuit packs in the processor port network (PPN)
- Expansion port networks (EPNs)

The IPSIs are hot swappable.

If all the PNs are direct-connect, Avaya recommends that you install one IPSI in the existing PPN rather than in one of the EPNs. But before you install the IPSI, you must convert the PPN to an EPN.

S8730 IP:

When you migrate an existing DEFINITY Server SI direct-connect in an MCC to the S8710 with a direct-connect configuration, you use one TN2312BP IPSI circuit pack to control from one to three PNs. Avaya recommends that you install the IPSI in the A carrier in the existing PPN

rather than in one of the EPNs. But before you install the IPSI, you must take the following steps to convert the PPN to a PN.

DEFINITY Server SI in an SCC

S8730 IP:

When you migrate an existing DEFINITY Server SI Direct-Connect in an SCC, you use one TN2312BP IPSI circuit pack to control from one to three PNs. Avaya recommends that you install the IPSI in the cabinet in the A position in the existing PPN rather than in one of the EPNs. But before you installing the IPSI, you must convert the PPN to a PN.

DEFINITY Server CSI or DEFINITY ONE/S8100 in a CMC1 Media Gateway

You can only migrate a DEFINITY Server CSI or a DEFINITY ONE/S8100 in a compact modular cabinet (CMC) to an Avaya S8700-Series with an IP-PNC configuration.

When you migrate an existing DEFINITY Server CSI or a DEFINITY ONE in a CMC1 Media Gateway, you use one TN2312BP IPSI circuit pack to control the PN. If a CSI, you replace the TN2182 Tone Clock circuit pack with the IPSI which you install in the A position of the cabinet. You also must remove the processor circuit pack. If a DEFINITY ONE, you replace the processor circuit pack with the IPSI.

This migration affects service because, if a CSI, you must turn off the CMC1 Media Gateways to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform some premigration administration.

Avaya IP600/S8100 in a G600

You can only migrate an Avaya IP600 to an Avaya S8730 Server with an IP-PNC configuration.

When you migrate an existing Avaya IP600, you use one TN2312BP IPSI circuit pack to control the PN. You replace the processor circuit pack with the IPSI in the cabinet in the A position.

This migration affects service because you must turn off the IP600 chassis to replace the processor. Before you turn off the chassis, you must perform some premigration administration.

Migration modules

This modules describe the following types of migrations:

- Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8730 Server with IP-PNC on page 343
- Migrating a DEFINITY ONE/S8100 to an S8730 Server with IP-PNC on page 377
- Migrating an Avaya IP600/S8100 to an S8730 Server with IP-PNC on page 409
- Migrating an Avaya S8400 Server to an S8730 Server on page 443
- Migrating an S8500-Series Server to an S8730 Server on page 471
- Migrating from an S8700, S8710 or S8720 to an S8730 Server on page 525

Migrating a DEFINITY Server CSI in a CMC1 Media Gateway to an S8730 Server with IP-PNC

Note:

Once you complete the migration to fiber-PNC, you can convert to IP-PNC. See Converting PNs to IP-PNC on page 55.

Use these procedures to migrate from an existing DEFINITY Server CSI in a Compact Modular Cabinet (CMC) system to the Avaya S8730 Server with IP-port network connectivity (PNC). You can only migrate a CSI in a CMC1 Media Gateway to an Avaya S8730 Server IP-PNC configuration. This procedure supports a migration to Communication Manager Release 5.x.

To migrate an existing DEFINITY Server CSI in a CMC1 Media Gateway, you use one TN2312BP IPSI circuit pack to control the one port network (PN). You must remove the TN2182 Tone Clock circuit pack and install an IPSI circuit pack in the A position. You also must remove the processor circuit pack.

This migration affects service because you must turn off the CMCs to replace the processor and tone-clock circuit packs.

Migration paths

DEFINITY Server CSI in a CMC1 Media Gateway and their releases that can be migrated to the S8730 Server IP-PNC configurations include:

- DEFINITY Release 5 through Release 10
- MultiVantage Release1.1
- Communication Manager Release 2.0 through Release 3.1.2

To migrate, in most cases, you must reenter all the translations.

Checklists

Before you go on site, perform the following tasks:

:

✓	Task	Description
	Verify that the correct hardware is installed on your Services laptop.	Correct hardware components include: ● 40 MB available disk space ● A direct Ethernet cable ● A serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● A CD-ROM drive
	Verify that the correct software is installed on your Services laptop.	Correct software includes: ● Windows 2000 or Windows 2000/XP operating system ● HyperTerminal or another terminal emulation program ● TCP/IP networking software that is bundled with the Windows OS ● Internet Explorer 5.0 or later
	Obtain the appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the logins and the passwords that you might need for the equipment of the customer.
	Obtain the serial number.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file and authentication file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	Use this CD-ROM to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware.	The following firmware is on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs **Important:** Firmware is upgraded often. To ensure that you have the latest version, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop.	New license file and authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	For DEFINITY systems only: Verify that you have the required, customer-provided network information. Obtain a completed *Electronic Preinstallation Worksheet (EPW)*.	The EPW is an Excel spreadsheet that provides the information about the network. You need this information to configure the control network components with the Avaya Installation Wizard. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard Web site.
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

For more information, see Migration paths *on page 343*.

When you migrate from a DEFINITY system, you must complete the following additional tasks before you start the migration:

✓	Task	Description
	Determine which adapters and cables you can reuse.	You cannot reuse the following items: • The C-LAN 259A adapter. You must use the adapter to the IP Media Processor for 100-Mbps speed. • The CAT3 cable that is used with C-LAN. You must use a CAT5 or better cable for 100-Mbps speed.
	CAUTION: You must complete the following twelve tasks *before* you freeze translations or save translations to an storage device that is used to read translations directly into a server.	
	Be sure to do this step before freezing translations. Verify that existing logins do not start with a number or an asterisk (*).	Linux does not support logins that start with a number or an asterisk (*). Use Avaya Terminal Emulator or Avaya Site Administration to perform a **`list logins`** command.
	Be sure to do this step before freezing translations. Verify that the functions of the TN577 Packet Gateway and the TN726B Data Line circuit packs (BX.25 links and mode two data modules) were changed to work through the C-LAN circuit packs.	Note that you cannot reuse the TN577 circuit pack. Use Avaya Terminal Emulator or Avaya Site Administration to perform a **`list node-names`** command.
	Be sure to do this step before freezing translations. Verify that the CMS and INTUITY peripherals and Distributed Communication Service (DCS) links are assigned node names and an Ethernet address.	
		1 of 3

✓	Task	Description
	Be sure to do this step before freezing translations. Remove all Mode II Data Modules before you change the S8730 Server.	The S8700 and the S8710 do not support the following data modules: • System Ports • PDMs (7400/8400 Data Modules) • PktGateway • Pkt Data Dataline • Modem Pool • System CDR PDMs • System Features Printer PDMs
	Be sure to do this step before you freeze translations. The TN750 Announcement circuit packs are not supported in the S8730 Server.	The announcements translations migrate to the S8730 Server. However, you must change the circuit pack locations to the TN2501AP Voice Announcement over LAN (VAL) circuit pack. **NOTE:** All announcement names must be unique on a TN2501AP VAL circuit pack. The announcement names cannot contain any spaces, blanks, or the following characters: • forward slash (/) • colon (:) • asterisk (*) • question mark (?) • backward slash (\) • angle brackets (<>) Type **`change announcements`** to change any names and port locations.
	Be sure to do this step before you freeze translations. On the **IP Services** screen in the **Service Type** field, remove **Alarm1** and **Alarm2**.	You first might need to change the **System Parameters Maintenance** screen before you can make any changes to the **IP Services** screen.

2 of 3

✓	Task	Description
	Be sure to do this step before you freeze translations. On the **Trunk Group** screen, change the **Measured** field from **measured** to **none**.	This action indicates that trunk group measurement reports are not required. Remember to remeasure trunk groups. Type **`list trunk-group`** to get a list of the trunk groups that are "measured" and need to be changed.
	Be sure to do this step before you freeze translations. Check the **Dial Plan** screen (or **Dial Plan Analysis Table** screen depending on the release) for 0 assigned as **attd**.	If **none**, check the **Attendant Console** screens for any buttons with **attd-qcalls** or **attd-qtime btns**. Remove these if 0 is not assigned as **attd**.
	About 2 weeks before the migration, freeze the translations. Use a flash card to collect the translations locally.	For more information on where and how to send the translations, contact the STS scheduling desk at 720-444-9418. STS updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For forms and more information, contact the STS scheduling desk at 720-444-9418.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.
	Copy the translation file from STS to a directory on the Services laptop.	File size is usually in the range of 1-4 megabytes.
		3 of 3

Presite migration checklist

Before you go on site, perform the following tasks in Table 12:

Table 12: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks in Table 13 before you start the migration:

Table 13: On site migration checklist

✓	Task	Description
	Verify that the EIA 310D 19-inch (48-cm) open equipment rack is grounded.	See the job aid titled *Approved Grounds* (555-245-772).
	For S8510, S8710, S8720, and S8730: Verify that the open, customer-supplied, EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack is properly installed and solidly secured.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on installing the rail, see the rail kit documentation.
	Verify that you have the correct cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see: • *Installing and Configuring the Avaya S8500 Media Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Media Server* (03-300145)

When you are on site for a migration from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	The customer supplies an open EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack. Verify that this rack is installed correctly and solidly secured.	Ensure that you have the screws that come with the rack for installing in square holes or with adapters. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on how to install the rail, see the rail kit documentation.
	Verify that cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs are labeled and that appropriate connectivity is provided.	The cables for TN2312BP Internet Protocol Server Interface (IPSI) circuit packs run from the control hardware rack to the port networks.
	Verify that you have the license file and that these files include the licensed features.	
	Verify that you have the Avaya authentication file.	

Documentation checklist for migrations

For a list of documents that Avaya recommends you have on hand for the migration, see Table 14.

Table 14: Documentation checklist

✓	Task	Description
	Quick Start for Hardware Installation: Avaya S8700-Series Servers (555-245-703)	A quick reference guide that provides physical installation and connection information.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.
	Installing and Configuring an Avaya S8700-Series Server (03-300145)	Provides installation instructions for the S8710 and S8720 Servers.
	Job Aid: Server and CSS Separation - Avaya S8700-Series Server (555-245-766)	Provides information on and connectivity diagrams when the S8710 or S8720 Servers are in separate locations.

Performing a migration

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

CAUTION:
This migration affects service. When the Definity One/S8100 is turned off, the system drops all calls. Service returns when the server takes control of the IPSIs.

Premigration administration

This migration is a service-affecting event. The CMCs must be turned off to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

CAUTION:
The licensing of the platform and port network connectivity attributes for the S8730 Server can be complex. See Server Migration Paths on page 50 and License and Avaya authentication files on page 47.

Connecting the IPSI to the network

After connecting to the server, power up the CMC1 cabinets:

1. Connect one end of the green CAT5 straight-through cable to the Ethernet switch on the customer network.
2. Connect the other end of the cable to the IPSI adapter on the back of the media gateway.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:
   a. **`list configuration all`**
   b. **`list trunk-group`**
   c. **`list hunt-group`**

   If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.
2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

Although the migrated translations are already copied to the server, you must save the translations in case you need to back out of the migration.

Note:

Save translations to a flash card.

To save translations:

1. To save translations to the system disk, type **`save translation`**. Press **Enter**.

   Either a **Command successfully completed** The message displays or all error messages are logged.

Translation migrations

This section describes how to migrate translation files from the existing system to the S8730 Server.

Accessing the server

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Select **yes** to suppress alarms.

   The system displays the **Communication Manager System Management Interface (SMI)**.

Checking system status

To check the system status:

1. Under Server, click **Status Summary**.
2. Verify the following information:
   - **Standby Refreshed** is set to Yes
   - **Standby Shadowing** is set to On

- **Duplication Link** is set to Up

Verifying the license file

To verify the Communication Manager license file:

1. Under Security, click **License File**.
2. Verify that the **Communication Mgr License Mode** field is set to **Normal**.

Restoring data for a migration

You cannot perform this task unless you have:

- Received the customer conversion files from the Avaya STS team.
- Saved the files on your Services laptop computer.

Accessing the server from your laptop

To access the server from your laptop:

1. Connect a crossover cable to the Services port on the back of the server.
2. Start the Web browser.
3. In the **Address** field, type **`192.11.13.6`** and press **Enter** to display the logon Web page.
4. Log in as **craft** or **dadmin**.
5. Select **yes** to suppress alarms.
6. Access **System Management Interface (SMI)** to go to the main menu.

Verifying the license file

To verify the license file:

1. Under Security, click **License File**.
2. Verify that the **MultiVantage License Mode** field is **Normal**.

Copying the translation files to the server

To copy translation files to the server:

1. Under Miscellaneous, click **Download Files**.
2. Click **Browse** and select the file that you saved on the Services laptop.
3. Click **Download** to place the file on the server.

Restoring the translation files

To restore the translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Local Directory** and click **View**. The field automatically shows the default directory.
3. Select the first file. The latest file might be at the top of the list.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.
5. Click **Restore** to restore the translation files.
6. Click **Restore Status**.
7. Select the first file, scroll down and click **Review Status** to see the results of the restore.

   When done, the screen shows the message **Restore is finished**.

If the restore process fails, the system displays an error message that states the reason for the failure and the translation file is not restored. Resolve the reason for the failure and restart the process.

Connecting to the standby server

To connect to the standby server:

1. Start a Web browser.
2. Log in as **craft** or **dadmin**.
3. Access **System Management Interface (SMI)**.
4. Under Server, click **Release Server**.
5. Click **Release**.

Connecting to the active server

To connect to the active server:

1. Start a Web browser.

2. Log in as **craft** or **dadmin**.
3. Access **System Management Interface (SMI)**.
4. Under Server, click **Status Summary** to verify that the standby server was refreshed. Do not continue until the standby server is refreshed.
5. Start a SAT session with Native Configuration Manager or Avaya Site Administration.
6. Login as **craft** or **dadmin**.

Installing the translations

To install the translations:

1. Type **`reset system 4`** and press **Enter**.
2. Return the STS-supplied PCMCIA flash card to Avaya.

To add the IPSI translations before you save translations, continue with Setting the alarm activation level on page 426.

Enabling the system for IPSI translations

To enable the system for IPSI translations:

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Verify that the **Primary Control Subnet Address** and **Secondary Control Subnet Address** (was equipped) fields are correct.

   The subnet work addresses must match the most significant three octets (the first three groups of digits in the subnet work address) of the Server IP address that appears on the control network entry from the completed Electronic Preinstallation Worksheet (EPW).

   An asterisk (*****) to the right of the **Subnet Address** field means that although a subnet work address appears, this address is incorrect. Communication Manager call processing software does not have the subnet information. After you verify the information on the screen, submit this form with or without changes to update Communication Manager with the correct subnet work information.

CAUTION:

If the information in either the **Primary Control Subnet Address** fields, the **Secondary Control Subnet Address** field, or both, is incorrect, you must change the information on the servers. Use the System Management Interface (SMI). Under Server Configuration and Upgrades, click **Configure Server** to change the server configuration. Then return here to perform Step 3.

3. Verify that the **Switch Identifier** field is set correctly for this installation. The correct Switch Identifier must be entered here before you administer the TN2312 IPSI circuit packs.
4. Verify that the **IPSI Control of Port Networks** field is set to **disabled**.
5. Press **Enter** to submit the screen.

Note:

The information that you provide depends on whether the IPSIs get static addresses or the addresses are assigned automatically through DHCP.

Adding IPSI information

To add IPSI information:

1. Type **`add ipserver-interface`** ***`PNnumber`*** where ***`PNnumber`*** is the port network number and press **Enter**.
2. When you use static addressing, in the **Host** field, type in the IP address for the IPSI in the port network that is listed in the **Location** field.
3. Verify that all the other fields are populated.
4. Press **Enter** to put the changes into effect.
5. Repeat Steps 1 through 5 for each port network.

Setting IPSI duplication (high-reliability critical-reliability only)

To set IPSI duplication:

1. Type **`change system-parameters duplication`** and press **Enter**.
2. Set the **Enable Operation of IPSI Duplication** field to **y**.

3. Press **Enter** to put the changes into effect.

Setting the alarm activation level

To set the alarm activation level:

1. Type **`change system-parameters maintenance`** and press **Enter**.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that the customer wants. The default is **none**.

Backing up translations on the S8700-series server

To back up translations:

1. S8710/S8720/S8730: Place a formatted flash card in the compact flash drive attached to a USB port.
2. Start a Web browser.
3. Log in as **craft** or **dadmin**.
4. Access **System Management Interface (SMI)**.
5. Under Data Backup/Restore, click **Backup Now**.
6. Select the data sets and the backup method.

   If you select **Save ACP translations prior to backup**, the server automatically saves the translations to the hard disk before the server saves the translations to the backup media.
7. Click **Start Backup** to start the backup process.

Migration tasks

Perform the following tasks to convert a processor port network to a port network (CMC).

Note:

If you want to make the system high reliability, you cannot reuse the Compact Modular Cabinets (CMCs). You must install Avaya G650 Media Gateways and move all the circuit packs to the G650s.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

The TN798 circuit pack or the TN2402 Processor circuit pack that contains the Audix feature is replaced with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that does not have the Audix feature. You must return the existing processor circuit pack to Avaya.

Note:

Customers also must add an ED-1E568-70G1 DEFINITY Audix Slim board and a TN2501AP Voice Announcement over LAN (VAL) circuit pack for announcements.

Changing the IP600 control chassis to a port network

To change the Avaya IP600 control chassis to a port network, you must:

- Replace the existing straight-wire WP cables, if present, with new twisted-pair I/O cables.
- Replace the processor circuit pack with a TN2312BP IP Server Interface (IPSI) circuit pack.

- Connect a CAT5 straight-through cable from the IPSI to the server through the network of the customer.

Turning off the power to the control cabinet

CAUTION:

Ensure that you have completed the premigration administration. If you do not perform the premigration administration, the system will not function. For more information, see Premigration administration on page 226.

To turn off power to the control cabinet:

1. On the faceplate of the processor, press and hold the shutdown button until the shutdown process starts.

   When you see the green light the system is shut down.

   DANGER:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the cabinet, pull the AC power cord from the back of the cabinet.

2. Unplug the power cord from the back of the cabinet to turn off the cabinet.

Replacing the processor circuit pack

To replace the processor circuit pack:

1. Remove the entire processor circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Remove the TN2182 Tone Clock circuit pack.
4. Remove the octopus cable from the connector that is associated with slot 2 on the connector panel.
5. Install the IPSI adapter to the connector that is associated with slot 2 on the connector panel.

6. Install the maintenance cable onto the 9-pin D-sub connector on the adapter. This cable is for emergency transfer and "auxsig" signal.

   Note:

   The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack takes only one slot.

7. Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit pack into slot 2.
8. Attach the new label above the circuit pack slots.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test circuit pack

You must replace the TN795 or the TN2412 circuit pack with a TN771 Maintenance/Test circuit pack. Each location must have one TN771 Maintenance/Test circuit pack.

To install the TN771 Maintenance/Test circuit pack:

- Install the TN771 circuit pack in slot 1.

  This carrier does not have a dedicated slot for the TN775 Maintenance (EPN) circuit pack.

If the cabinet does not have a TN2302AP IP Media Processor (CSI did not require it), you must install one in slot 10. For more information, see the *Adding New Hardware* book, Install and Administer IP Connectivity Hardware section.

Connecting the IPSI to the network

After connecting to the server, power up the CMC1 cabinets:

1. Connect one end of the green CAT5 straight-through cable to the Ethernet switch on the customer network.

2. Connect the other end of the cable to the IPSI adapter on the back of the media gateway.

Post-migration administration

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 24: Connecting directly to the IPSI on page 367).

Figure 24: Connecting directly to the IPSI

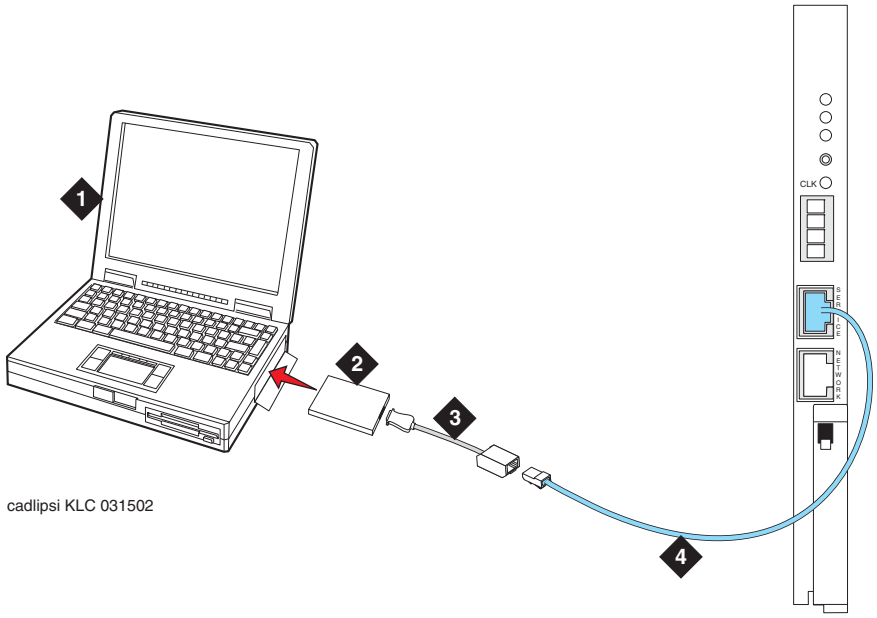


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application on the service laptop to access the server (192.11.13.6 port 22).

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.

2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

Note:

The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`** and press **Enter**.
2. To see the current settings, type **`show port 1`** and press **Enter**.
3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Verify that the correct information was entered.
5. If a default gateway is used, enter the gateway IP address.
   Type **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway and press **Enter**.
6. To save the changes and exit the IPSI session, type **`quit`** and press **Enter**.
7. SSH to **192.11.13.6** and log in.

8. To verify the administration, type **`show control interface`** and press **Enter**.
9. To see the changes, type **`exit`** and press **Enter**.

Setting the VLAN and diffserv parameters

To set the VLAN parameters and the diffserver parameters:

1. Log back in as **`craft`**.
2. To display the quality of service values, type **`show qos`** and press **Enter**.
3. If necessary, use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

   Note:
   Use **Help** to obtain syntax guidelines for these commands.

   - Type **`set vlan priority 6`**
   - Type **`set diffserv 46`**
   - Type **`set vlan tag on`**
   - Type **`set port negotiation 1 disable`**
   - Type **`set port duplex 1 full`**
   - Type **`set port speed 1 100`**
4. To check the administered values, type **`show qos`** and press **Enter**.
5. To exit, type **`quit`**. Press **Enter**.

   Important:
   Ensure that the port settings on the Ethernet switches are set to the same values as shown in the **`set port`** commands in step 3.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

Note:

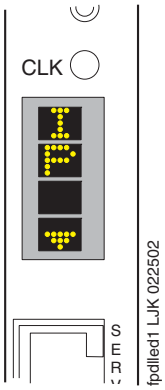
Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

Note:

The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.

2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 25).

Figure 25: LED display that shows that the IPSI has a static IP address



4. Repeat steps 1 through 3 for each IPSI circuit pack.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "1" shows in any position, you must troubleshoot the problem.

Tip:

The pattern `0.1.1.0` usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct cabinet and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Enabling control of the IPSI

To enable control of the IPSI:

Note:

Ensure that the IPSI has the same, current firmware.

CAUTION:

This procedure allows the server to take control of the IPSI-controlled port network(s). Failure to complete the steps correctly can result in no connection to the network.

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Set the **IPSI Control of Port Networks:** field to **enabled**
3. Press **Enter** to effect the change.
4. Type **`save translation`** and press **Enter**.

   The server now controls all the port networks.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.

3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating a DEFINITY ONE/S8100 to an S8730 Server with IP-PNC

Use these procedures to migrate from an existing DEFINITY ONE/S8100 system to the Avaya S8730 Server with an IP-port network connectivity (PNC) configuration. This procedure supports a migration to Communication Manager Release 5.x.

You can migrate only a DEFINITY ONE/S8100 to an Avaya S8730 Server IP-PNC configuration.

To migrate an existing DEFINITY ONE/S8100, you use one TN2312BP IPSI circuit pack to control the port network (PN). You also must replace the processor circuit pack with the IPSI.

This migration affects service. because you must turn off the control cabinet to replace the processor and tone-clock circuit packs.

Migration paths

Avaya supports the following migrations of a DEFINITY ONE/S8100 to the S8730 Server IP-PNC configurations include:

- DEFINITY Release 6 through 10
- MultiVantage Release 1.1 and 1.2
- Communication Manager Release 1.0 through Release 2.0.1

Checklists

Before you go on site, perform the following tasks:

:

✓	Task	Description
	Verify that the correct hardware is installed on your Services laptop.	Correct hardware components include: ● 40 MB available disk space ● A direct Ethernet cable ● A serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● A CD-ROM drive
	Verify that the correct software is installed on your Services laptop.	Correct software includes: ● Windows 2000 or Windows 2000/XP operating system ● HyperTerminal or another terminal emulation program ● TCP/IP networking software that is bundled with the Windows OS ● Internet Explorer 5.0 or later
	Obtain the appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the logins and the passwords that you might need for the equipment of the customer.
	Obtain the serial number.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file and authentication file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	Use this CD-ROM to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware.	The following firmware is on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs **Important:** Firmware is upgraded often. To ensure that you have the latest version, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop.	New license file and authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	For DEFINITY systems only: Verify that you have the required, customer-provided network information. Obtain a completed *Electronic Preinstallation Worksheet (EPW)*.	The EPW is an Excel spreadsheet that provides the information about the network. You need this information to configure the control network components with the Avaya Installation Wizard. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard Web site.
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

For more information, see Migration paths on page 377.

When you are migrating from a DEFINITY system, complete the following additional tasks before starting the migration:

✓	Task	Description
	Determine which adapters and cables you can reuse.	You *cannot* reuse the following items: • The C-LAN 259A adapter. You must use adapter for IP Media Processor for 100-Mbps speed. • The CAT3 cable that is used with C-LAN. You must use a CAT5 or better for 100-Mbps speed.
	CAUTION: You must complete the following seven tasks *before* you freeze translations or save translations to an MO disk that is used to read translations directly into a server. Failure to complete the tasks correctly can result in a system that does not function.	
	CAUTION: Be sure to do this step before freezing translations. Verify that the functions of the TN577 Packet Gateway and the TN726B Data Line circuit packs (BX.25 links and mode 2 data modules) were converted to work through the C-LAN circuit packs.	Note that you cannot reuse the TN577 circuit pack. Use Avaya Terminal Emulator or Avaya Site Administration to perform a **`list node-names`** command.
	Be sure to do this step before freezing translations. Verify that the CMS and INTUITY peripherals and Distributed Communication Service (DCS) links are assigned node names and an Ethernet address.	
		1 of 3

✓	Task	Description
	CAUTION: Be sure to do this step before freezing translations. Remove all Mode II Data Modules before you change to the S8730 Server.	The S8730 Server does not support the following data modules: • System Ports • PDMs (7400/8400 Data Modules) • PktGateway • Pkt Data Dataline • Modem Pool • System CDR PDMs • System Features Printer PDMs
	Be sure to do this step before you freeze translations. The TN750 Announcement circuit packs are not supported in the S8730 Server.	The announcements translations migrate to the S8730 Server. However, you must change the circuit pack locations to the TN2501AP Voice Announcement over LAN (VAL) circuit pack. **NOTE:** All announcement names must be unique on a TN2501AP VAL circuit pack. The announcement names cannot contain any spaces, blanks, or the following characters: • forward slash (/) • colon (:) • asterisk (*) • question mark (?) • backward slash (\) • angle brackets (<>) Type **`change announcements`** to change any names and port locations.
	CAUTION: Be sure to do this step before freezing translations. On the **IP Services** screen in the **Service Type** field, remove **Alarm1** and **Alarm2**.	You first might need to change the **System Parameters Maintenance** screen before you can make any changes to the **IP Services** screen.
		2 of 3

✓	Task	Description
	CAUTION: Be sure to do this step before freezing translations. On the **Trunk Group** screen, change the **Measured** field from **measured** to **none**.	This action indicates that trunk group measurement reports are not required. Remember to remeasure trunk groups. Type `list trunk-group` to get a list of the trunk groups that are "measured" and need to be changed.
	Be sure to do this step before you freeze translations. Check the **Dial Plan** screen (or **Dial Plan Analysis Table** screen depending on the release) for 0 assigned as **attd**.	If **none**, check the **Attendant Console** screens for any buttons with **attd-qcalls** or **attd-qtime btns**. Remove these if 0 is not assigned as **attd**.
	About 2 weeks before the migration, freeze the translations. • Collect the translations locally by a spare flash card.	For more information on where and how to send the translations, contact the STS scheduling desk at 720-444-9418. STS then updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative.
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you have finished installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, provided you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access still requires an ASG challenge/response. This unique craft password remains valid until a new authentication file is installed.
	Copy the translation file to a directory on the Services laptop.	File size usually is in the range of 1-4 megabytes.
		3 of 3

Presite migration checklist

Before you go on site, perform the following tasks in Table 15:

Table 15: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks in Table 16 before you start the migration:

Table 16: On site migration checklist

✓	Task	Description
	Verify that the EIA 310D 19-inch (48-cm) open equipment rack is grounded.	See the job aid titled *Approved Grounds* (555-245-772).
	For S8510, S8710, S8720, and S8730: Verify that the open, customer-supplied, EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack is properly installed and solidly secured.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on installing the rail, see the rail kit documentation.
	Verify that you have the correct cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see: • *Installing and Configuring the Avaya S8500 Media Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Media Server* (03-300145)

When you are on site for a migration from a DEFINITY system, complete the following additional tasks before you start the migration:

✓	Task	Description
	S8710: The customer supplies an open, EIA 310D (or equivalent) standard four-post, 19-inch (48-centimeter), equipment rack. Verify that this rack is installed correctly.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on how to install the rail, see the documentation that comes with the rail kit.
	You might need to move the UPSs and Ethernet switches from the two-post rack.	Ensure that you have: ● A Phillips screwdriver ● Rail kits for a four-post rack for the UPSs ● Cage nuts to attach the screws to the rack, if necessary ● At least 2 people to lift the equipment
	Verify that the cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs are labeled and that appropriate connectivity is provided.	The cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs run from the control hardware rack to the port networks.
	Verify that you have the license file and that the file includes: ● the Right-To-Use (RTU) feature ● Applicable hardware parts in the existing system ● Any hardware that you add as part of the migration	
	Verify that you have the Avaya authentication file.	

Documentation checklist for migrations

For a list of documents that you need to perform the migration, see Resources on page 35.

Additional documentation needed.

✓	Document	Description
	Quick Start for Hardware Installation: Avaya S8700-Series Media Servers (555-245-703)	A quick-reference guide that provides physical installation and connection information.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.
	Installing and Configuring an Avaya S8700-Series Media Server (03-300145)	Provides installation instructions for the S8700, S8710, S8720, and S8730 Servers.

Performing a migration

The information in this is based on the assumption that the server complex is installed, configured, and operational.

This section describes how to change an existing processor port network (PPN) to a port network (PN).

CAUTION:
This migration affects service. When the Definity One/S8100 is turned off, the system drops all calls. Service returns when the server takes control of the IPSIs.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Premigration administration

This migration is a service-affecting event. The CMCs must be turned off to replace the processor and tone clock circuit packs. Before you turn off the cabinets, you must perform the following premigration administration.

CAUTION:

The licensing of the platform and port network connectivity attributes for the S8730 Server can be complex. See Server Migration Paths on page 50 and License and Avaya authentication files on page 47.

Connecting to the processor

To connect to the processor:

Note:

You need a cross-over cable to connect your Services laptop directly to the processor.

1. Perform one of the following actions to connect the Services laptop directly into the Avaya IP600 processor circuit pack:
   - If the processor circuit pack is a TN795, place the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector directly into the RJ45 jack on the faceplate.
2. Start a terminal emulation application or Avaya Site Administration.
3. Log in as **lucent3**.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.

2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

You must save the translations in case you need to stop out of the migration. You might want to print out the translations for reference.

To save translations:

1. Type **`save translation`** and press **Enter** to save translations to the system disk.

   Either a **Command successfully completed** message displays or all error messages are logged.

Recording IP settings

Record the IP settings assigned to the processor as they can be used for the server. Verify against the filled-out *Electronic Preinstallation Worksheet*.

The following administration is done on the Services laptop connected to the processor circuit pack using telnet. To record the IP settings:

1. Select **Start** > **Run** to open the **Run** dialog box.

2. Type **`telnet 192.11.13.6`** .and press **Enter** to access the server.
3. Log in as **lucent3** to get to the LAC prompt.
4. Type **`bash`** and press **Enter** to start a BASH session.
5. Type **`setip`** and press **Enter** to show the current list of IP settings. You might see the following information:
   - cust: *IPaddress, subnet mask, gateway*
   - dns: *server name, domain name, 2 DNS server IP addresses*
   - wins: *2 WINS server IP addresses*
   - ras: *1 remote access server IP address*
6. Write down this information, *exactly* as it displays.

You must record this information exactly as it appears here. You cannot miss any periods, commas, or other punctuation marks. Record information in lowercase or uppercase as displayed.

Translation migrations

This section describes how to migrate translation files from the existing system to the S8730 Server.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Checking system status

To check the system status:

1. Under Server, click **Status Summary**.
2. Verify the following information:
   - **Standby Refreshed** is set to Yes
   - **Standby Shadowing** is set to On
   - **Duplication Link** is set to Up

Verifying the license file

To verify the Communication Manager license file:

1. Under Security, click **License File**.
2. Verify that the **Communication Mgr License Mode** field is set to **Normal**.

Restoring data for a migration

You cannot perform this task unless you have:

- Received the customer conversion files from the Avaya STS team.
- Saved the files on your Services laptop computer.

Accessing the server from your laptop

To access the server from your laptop:

1. Connect a crossover cable to the Services port on the back of the server.
2. Start the Web browser.
3. In the **Address** field, type **`192.11.13.6`** and press **Enter** to display the logon Web page.
4. Log in as **craft** or **dadmin**.
5. Select **yes** to suppress alarms.

6. Access **System Management Interface (SMI)** to go to the main menu.

Verifying the license file

To verify the license file:

1. Under Security, click **License File**.
2. Verify that the **MultiVantage License Mode** field is **Normal**.

Copying the translation files to the server

To copy translation files to the server:

1. Under Miscellaneous, click **Download Files**.
2. Click **Browse** and select the file that you saved on the Services laptop.
3. Click **Download** to place the file on the server.

Restoring the translation files

To restore the translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Local Directory** and click **View**. The field automatically shows the default directory.
3. Select the first file. The latest file might be at the top of the list.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.
5. Click **Restore** to restore the translation files.
6. Click **Restore Status**.
7. Select the first file, scroll down and click **Review Status** to see the results of the restore.

   When done, the screen shows the message **Restore is finished**.

If the restore process fails, the system displays an error message that states the reason for the failure and the translation file is not restored. Resolve the reason for the failure and restart the process.

Connecting to the standby server

To connect to the standby server:

1. Start a Web browser.
2. Log in as **craft** or **dadmin**.
3. Access **System Management Interface (SMI)**.

4. Under Server, click **Release Server**.
5. Click **Release**.

Connecting to the active server

To connect to the active server:

1. Start a Web browser.
2. Log in as **craft** or **dadmin**.
3. Access **System Management Interface (SMI)**.
4. Under Server, click **Status Summary** to verify that the standby server was refreshed. Do not continue until the standby server is refreshed.
5. Start a SAT session with Native Configuration Manager or Avaya Site Administration.
6. Login as **craft** or **dadmin**.

Installing the translations

To install the translations:

1. Type **`reset system 4`** and press **Enter**.
2. Return the STS-supplied PCMCIA flash card to Avaya.

To add the IPSI translations before you save translations, continue with Setting the alarm activation level on page 426.

Enabling the system for IPSI translations

To enable the system for IPSI translations:

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Verify that the **Primary Control Subnet Address** and **Secondary Control Subnet Address** (was equipped) fields are correct.

   The subnet work addresses must match the most significant three octets (the first three groups of digits in the subnet work address) of the Server IP address that appears on the control network entry from the completed Electronic Preinstallation Worksheet (EPW).

   An asterisk (*****) to the right of the **Subnet Address** field means that although a subnet work address appears, this address is incorrect. Communication Manager call processing software does not have the subnet information. After you verify the information on the

screen, submit this form with or without changes to update Communication Manager with the correct subnet work information.

CAUTION:

If the information in either the **Primary Control Subnet Address** fields, the **Secondary Control Subnet Address** field, or both, is incorrect, you must change the information on the servers. Use the System Management Interface (SMI). Under Server Configuration and Upgrades, click **Configure Server** to change the server configuration. Then return here to perform Step 3.

3. Verify that the **Switch Identifier** field is set correctly for this installation. The correct Switch Identifier must be entered here before you administer the TN2312 IPSI circuit packs.
4. Verify that the **IPSI Control of Port Networks** field is set to **disabled**.
5. Press **Enter** to submit the screen.

Note:

The information that you provide depends on whether the IPSIs get static addresses or the addresses are assigned automatically through DHCP.

Adding IPSI information

To add IPSI information:

1. Type **`add ipserver-interface`** ***`PNnumber`*** where ***`PNnumber`*** is the port network number and press **Enter**.
2. When you use static addressing, in the **Host** field, type in the IP address for the IPSI in the port network that is listed in the **Location** field.
3. Verify that all the other fields are populated.
4. Press **Enter** to put the changes into effect.
5. Repeat Steps 1 through 5 for each port network.

Setting IPSI duplication (high-reliability critical-reliability only)

To set IPSI duplication:

1. Type **`change system-parameters duplication`** and press **Enter**.

2. Set the **Enable Operation of IPSI Duplication** field to **y**.
3. Press **Enter** to put the changes into effect.

Setting the alarm activation level

To set the alarm activation level:

1. Type **`change system-parameters maintenance`** and press **Enter**.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that the customer wants. The default is **none**.

Backing up translations on the S8700-series server

To back up translations:

1. S8710/S8720/S8730: Place a formatted flash card in the compact flash drive attached to a USB port.
2. Start a Web browser.
3. Log in as **craft** or **dadmin**.
4. Access **System Management Interface (SMI)**.
5. Under Data Backup/Restore, click **Backup Now**.
6. Select the data sets and the backup method.

   If you select **Save ACP translations prior to backup**, the server automatically saves the translations to the hard disk before the server saves the translations to the backup media.
7. Click **Start Backup** to start the backup process.

Migration tasks

Perform the following tasks to convert a processor port network to a port network (CMC).

Note:

If you want to make the system high reliability, you cannot reuse the Compact Modular Cabinets (CMCs). You must install Avaya G650 Media Gateways and move all the circuit packs to the G650s.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Verifying hardware

Ensure that you have the conversion specific hardware on hand.

Note:

Customers who currently use the Audix feature on the S8100 must purchase a separate Audix system. The TN795 or the TN2314 Processor circuit pack that contains the Audix feature is replaced with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that does not contain the Audix feature. You must return the existing processor circuit pack to Avaya.

Note:

Customers also must add an ED-1E568-70G1 DEFINITY Audix Slim board and a TN2501AP Voice Announcement over LAN (VAL) circuit pack for announcements.

Changing the control cabinet to a port network

To change the control cabinet to a port network, you must:

- Replace the TN795 or TN2314 Processor circuit pack with a TN2312BP Internal Protocol Server Interface (IPSI) circuit pack.

- Connect a CAT5 straight-through cable from the IPSI to the server through the network of the customer.

Note:

If replacing a TN795 Processor circuit pack, you might not need the TN744D/E Call Classifier-Detector circuit pack. The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack has call classifier functionality. However, increased voice and data traffic might require the TN744D/E Call Classifier-Detector circuit pack.

Note:

If you have a TN799C or earlier C-LAN circuit pack, you must replace the TN799 circuit pack with a TN799DP C-LAN circuit pack.

Turning off the power to the control cabinet

CAUTION:

Ensure that you have completed the premigration administration. If you do not perform the premigration administration, the system will not function. For more information, see Premigration administration on page 226.

To turn off power to the control cabinet:

1. On the faceplate of the processor, press and hold the shutdown button until the shutdown process starts.

   When you see the green light the system is shut down.

   DANGER:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the cabinet, pull the AC power cord from the back of the cabinet.

2. Unplug the power cord from the back of the cabinet to turn off the cabinet.

Replacing the processor circuit pack

To replace the processor circuit pack:

1. Remove the entire processor circuit pack and place it in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
2. Remove the octopus cable from the connector that is associated with slot 2 on the connector panel.
3. Install the IPSI adapter to the connector that is associated with slot 2 on the connector panel.
4. Install the maintenance cable onto the 9-pin D-sub connector on the adapter. This cable is for emergency transfer and "auxsig" signal.

   Note:

   The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack takes only one slot.

5. Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit pack into slot 2.
6. Attach the new label above the circuit pack slots.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test circuit pack

You must replace the TN795 or the TN2412 circuit pack with a TN771 Maintenance/Test circuit pack. Each location must have one TN771 Maintenance/Test circuit pack.

To install the TN771 Maintenance/Test circuit pack:

- Install the TN771 circuit pack in slot 1.

  This carrier does not have a dedicated slot for the TN775 Maintenance (EPN) circuit pack.

If the cabinet does not have a TN2302AP IP Media Processor, you must install one in slot 10. For more information, see the *Adding New Hardware* book, Install and Administer IP Connectivity Hardware section.

Connecting the IPSI to the network

After connecting to the server, power up the CMC1 cabinets:

1. Connect one end of the green CAT5 straight-through cable to the Ethernet switch on the customer network.
2. Connect the other end of the cable to the IPSI adapter on the back of the media gateway.

Post-migration administration

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 26: Connecting directly to the IPSI on page 400).

Figure 26: Connecting directly to the IPSI

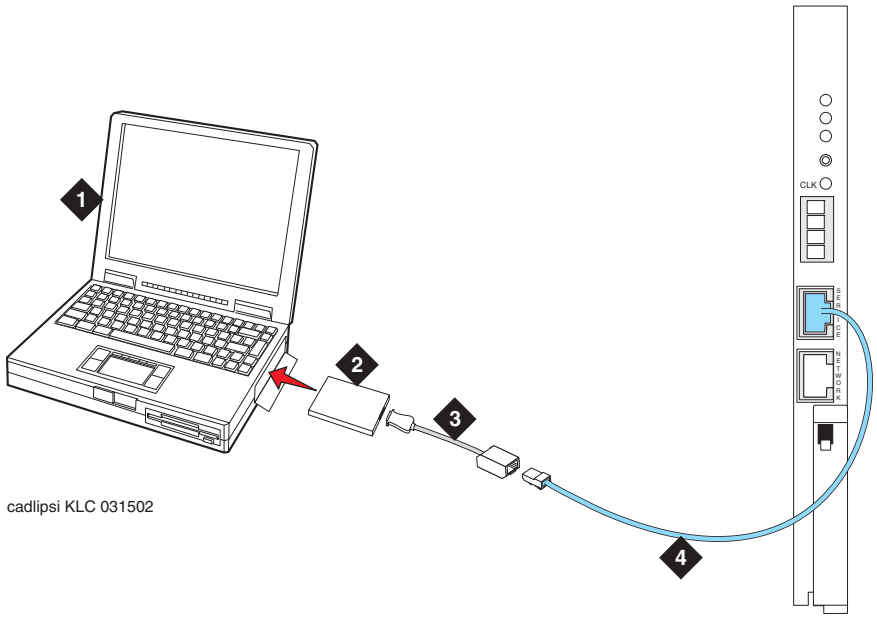


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application on the service laptop to access the server (192.11.13.6 port 22).

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.

2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`** and press **Enter**.
2. To see the current settings, type **`show port 1`** and press **Enter**.

3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Verify that the correct information was entered.
5. If a default gateway is used, enter the gateway IP address.
   Type **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway and press **Enter**.
6. To save the changes and exit the IPSI session, type **`quit`** and press **Enter**.
7. SSH to **192.11.13.6** and log in.
8. To verify the administration, type **`show control interface`** and press **Enter**.
9. To see the changes, type **`exit`** and press **Enter**.

Setting the VLAN and diffserv parameters

To set the VLAN parameters and the diffserver parameters:

1. Log back in as **`craft`**.
2. To display the quality of service values, type **`show qos`** and press **Enter**.
3. If necessary, use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

Note:

Use **Help** to obtain syntax guidelines for these commands.

- Type **`set vlan priority 6`**
- Type **`set diffserv 46`**
- Type **`set vlan tag on`**
- Type **`set port negotiation 1 disable`**
- Type **`set port duplex 1 full`**
- Type **`set port speed 1 100`**

4. To check the administered values, type **`show qos`** and press **Enter**.
5. To exit, type **`quit`**. Press **Enter**.

Important:

Ensure that the port settings on the Ethernet switches are set to the same values as shown in the **`set port`** commands in step 3.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

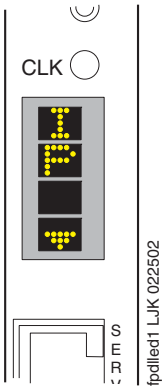
   Note:

   Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

   Note:

   The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.
2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 27).

Figure 27: LED display that shows that the IPSI has a static IP address



4. Repeat steps 1 through 3 for each IPSI circuit pack.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "`1`" shows in any position, you must troubleshoot the problem.

   Tip:

   The pattern `0.1.1.0` usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.

2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct cabinet and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Enabling control of the IPSI

To enable control of the IPSI:

Note:
Ensure that the IPSI has the same, current firmware.

CAUTION:
This procedure allows the server to take control of the IPSI-controlled port network(s). Failure to complete the steps correctly can result in no connection to the network.

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Set the **IPSI Control of Port Networks:** field to **enabled**
3. Press **Enter** to effect the change.
4. Type **`save translation`** and press **Enter**.

   The server now controls all the port networks.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the cabinets. Verify that the screen shows the cabinet number that is assigned to the changed cabinets.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the cabinet number of the changed cabinet and press **Enter**. Under Carrier Description, Carrier Type verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating an Avaya IP600/S8100 to an S8730 Server with IP-PNC

Use these procedures to migrate from an existing IP600/S8100 IP-port network connectivity (PNC) system to the S8730 Server with an IP-PNC configuration. This procedure supports a migration to Communication Manager Release 5.x.

You can migrate an IP600/S8100 only to an S8730 Server IP-PNC configuration.

When you migrate an existing IP600/S8100, you use one TN2312BP IPSI circuit pack to control the port network (PN). You also replace the processor circuit pack with the IPSI circuit pack in the cabinet in the A position.

This migration affects service because you must turn off the IP600 chassis to replace the processor and the tone-clock circuit packs.

Migration paths

You can migrate the following DEFINITY IP600/S8100 releases to the S8730 Server IP-PNC configurations:

- DEFINITY Release 9 through 10
- MultiVantage Release 1.1 and 1.2
- Communication Manager Release 1.0 through 2.0.1

Checklists

Before you go on site, perform the following tasks:

:

✓	Task	Description
	Verify that the correct hardware is installed on your Services laptop.	Correct hardware components include: ● 40 MB available disk space ● A direct Ethernet cable ● A serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● A CD-ROM drive
	Verify that the correct software is installed on your Services laptop.	Correct software includes: ● Windows 2000 or Windows 2000/XP operating system ● HyperTerminal or another terminal emulation program ● TCP/IP networking software that is bundled with the Windows OS ● Internet Explorer 5.0 or later
	Obtain the appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the logins and the passwords that you might need for the equipment of the customer.
	Obtain the serial number.	You need a new license file and authentication file. You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file and authentication file.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	Use this CD-ROM to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware.	The following firmware is on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs **Important:** Firmware is upgraded often. To ensure that you have the latest version, go to the Avaya Support web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop.	New license file and authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	For DEFINITY systems only: Verify that you have the required, customer-provided network information. Obtain a completed *Electronic Preinstallation Worksheet (EPW)*.	The EPW is an Excel spreadsheet that provides the information about the network. You need this information to configure the control network components with the Avaya Installation Wizard. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard Web site.
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

For more information, see Migration paths *on page 409*.

When you migrate from a DEFINITY system, you must complete the following additional tasks in Table 17: Premigration setup checklist *on page 413* before you start the migration:

Table 17: Premigration setup checklist

✓	Task	Description
	Determine which adapters and cables you can reuse.	You *cannot* reuse the following items: • The C-LAN 259A adapter. You must use an adapter for the IP Media Processor for 100-Mbps speed. • The CAT3 cable that is used with Control-LAN (C-LAN) circuit pack. You must use a CAT5 or better cable for 100-Mbps speed.
	Note: You may also send all G3r translations to the Avaya STS group for processing.	
	CAUTION: Perform this step before you freeze the translations. Remove all Mode II Data Modules before you change to the S8730 Server.	The S8730 Server does not support the following data modules: • System Ports • PDMs (7400/8400 Data Modules) • PktGateway • Pkt Data Dataline • Modem Pool • System CDR PDMs • System Features Printer PDMs
		1 of 3

Table 17: Premigration setup checklist

✓	Task	Description
	CAUTION: Perform this step before you freeze translations.	The TN750 Announcement circuit packs are not supported in the S8730 Servers. The announcements translations migrate to the S8730 Server. However, you must change the circuit pack locations to the TN2501AP Voice Announcement over LAN (VAL) circuit pack. **NOTE:** All announcement names must be unique on a TN2501AP VAL circuit pack. The announcement names cannot contain any spaces, blanks, or the following characters: • Forward slash (/) • Colon (:) • Asterisk (*) • Question mark (?) • Backward slash (\) • Angle brackets (<>) Type **`change announcements`** to change any names and port locations.
	CAUTION: Perform this step before freezing translations. On the **IP Services** screen in the **Service Type** field, remove **Alarm1** and **Alarm2**.	You might need to change the **System Parameters Maintenance** screen before you can make any changes to the **IP Services** screen.
	CAUTION: Perform this step before freezing translations. On the **Trunk Group** screen, change the **Measured** field from **measured** to **none**.	This action indicates that trunk group measurement reports are not required. Remember to re-measure trunk groups. To get a list of the trunk groups that are "measured" and must be changed, type **`list trunk-group`**.
		2 of 3

Table 17: Premigration setup checklist

✓	Task	Description
	CAUTION: Perform this step before freezing translations. Depending on the release, use the **`change dialplan analysis`** command and check the **Dial Plan Analysis Table** screen for 0 assigned as **attd**.	If there are none, check the **Attendant Console** screens for any buttons with **attd-qcalls** or **attd-qtime btns**. Remove these if 0 is not assigned as **attd**.
	About 2 weeks before the migration, freeze the translations. • Use a spare flash card to collect the translations locally.	For more information on how to send the translations, contact the STS scheduling desk at 720-444-9418. STS then updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail. The project manager then sends the reports and files to the field technician.
	Verify that you have the appropriate logins and the passwords to access the servers and the server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time that you log in as craft, if you access the server through the Services port. You do not need an ASG challenge and response to log in this way, even though other means of craft access requires an ASG challenge and response. This unique craft password remains valid until a new authentication file is installed.
	Copy the translation file to a directory on the Services laptop computer.	The file size usually is from 1-4 megabytes.
		3 of 3

Presite migration checklist

Complete the following tasks in Table 18: Presite migration checklist on page 416:

Table 18: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Matrix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace any TN799B/C circuit packs with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace the 259A adapter with the cable extender adapter with Comcode 848525887 and the CAT3 cable with a CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace the TN570 circuit packs with TN570B vintage 7 or later circuit packs.

On site migration checklist

When you are on site, complete the following tasks in Table 19: On site migration checklist on page 417 before you start the migration:

Table 19: On site migration checklist

✓	Task	Description
	Verify that the EIA 310D 19-inch (48-cm) open equipment rack is grounded.	See the job aid that is titled *Approved Grounds* (555-245-772).
	For the S8710 only: Verify that the customer-supplied an open EIA 310D or equivalent standard 4-post, 19-inch (48-centimeter) equipment rack and that the rack is installed correctly and solidly secured.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information, see the rail kit documentation.
	Verify that the correct cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs are labeled and that appropriate connectivity is provided.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see *Installing and Configuring the Avaya S8700-Series Server* (03-300145).
	Verify that you have the license file and that the file includes the licensed features.	Use the License File link on the System Management Interface (SMI) to verify.
	Verify that you have the Avaya authentication file.	Use the Authentication File link on the System Management Interface (SMI) to verify.

Documentation checklist for migrations

For a list of documents that Avaya recommends you have for the migration, see Table 20: Documentation checklist for migrations on page 418.

Table 20: Documentation checklist for migrations

✓	Task	Description
	Quick Start for Hardware Installation: Avaya S8700-Series Servers (555-245-703)	A quick reference guide that provides installation and connection information.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.
	Installing and Configuring an Avaya S8700-Series Server (03-300145)	Provides installation instructions for the S8710, S8720, and the S8730 Servers.
	Installing the Avaya G650 Media Gateway, 03-300685.	Provides installation instructions for the G650 Media Gateway.
	Job Aid: Server and CSS Separation - Avaya S8700-Series Server (555-245-766)	This provides connectivity information to use when the S8710, S8720, or the S8730 Servers are in separate locations.

Performing a migration

Perform the tasks in this section only after the server complex is installed, configured, and operational.

CAUTION:

This procedure affects service. When the processor port network (PPN) is turned off, the system stops all calls. Service returns when the server takes control of the IPSIs.

The following list describes general procedures:

- Turn off the processor gracefully - premigration administration
- Replace the processor circuit pack or the tone-clock circuit pack with an IPSI circuit pack.
- Replace the WP cables with twisted-pair cables.
- Connect the IPSI circuit pack to the Ethernet switch on the network of the customer.
- Assign an IP address to the IPSI circuit pack.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Premigration administration

This migration affects service. You must turn off the IP600 chassis to replace the processor. Before you turn off the chassis, you must perform the following premigration administration.

CAUTION:

The licensing of the platform and port network connectivity attributes for the S8730 Server can be complex. See Server Migration Paths on page 50 and License and Avaya authentication files on page 47.

Connecting to the processor

To connect to the processor:

Note:

You need a cross-over cable to connect your Services laptop directly to the processor.

1. Perform one of the following actions to connect the Services laptop directly into the Avaya IP600 processor circuit pack:
   - If the processor circuit pack is a TN795, place the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector directly into the RJ45 jack on the faceplate.

2. Start a terminal emulation application or Avaya Site Administration.
3. Log in as **lucent3**.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.

2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

You must save the translations in case you need to stop out of the migration. You might want to print out the translations for reference.

To save translations:

1. Type **`save translation`** and press **Enter** to save translations to the system disk.

   Either a **Command successfully completed** message displays or all error messages are logged.

Recording IP settings

You must view and record the IP settings that are assigned to the processor and use these same settings for the server. Verify the settings against the completed *Electronic Preinstallation Worksheet*.

To view these settings, perform the following administration on the Services laptop computer that is connected to the processor circuit pack by way of telnet. To record the IP settings:

1. Select **Start** > **Run** to open the **Run** dialog box.
2. Type **`telnet 192.11.13.6`** and press **Enter**.
3. Log in as **lucent3** to get to the LAC prompt.
4. Type **`bash`** and press **Enter** to start a BASH session.
5. Type **`setip`** and press **Enter** to show the current list of IP settings. You should see the following information:
   - cust: *IPaddress, subnet mask, gateway*
   - dns: *server name, domain name, two DNS server IP addresses*
   - wins: *two WINS server IP addresses*
   - ras: *one remote access server IP address*
6. Record this information exactly as the information is displayed.

Important:
Include any periods, commas, or other punctuation marks and ensure that you duplication any lowercase or uppercase letters exactly.

Migrating the translation files

This section describes how to migrate translation files from the existing system to the S8730 Server.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.

2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Checking system status

To check the system status:

1. Under Server, click **Status Summary**.
2. Verify the following information:
   - **Standby Refreshed** is set to Yes
   - **Standby Shadowing** is set to On
   - **Duplication Link** is set to Up

Verifying the license file

To verify the Communication Manager license file:

1. Under Security, click **License File**.
2. Verify that the **Communication Mgr License Mode** field is set to **Normal**.

Restoring data for a migration

You cannot perform this task unless you have:

- Received the customer conversion files from the Avaya STS team.
- Saved the files on your Services laptop computer.

Accessing the server from your laptop

To access the server from your laptop:

1. Connect a crossover cable to the Services port on the back of the server.
2. Start the Web browser.
3. In the **Address** field, type **`192.11.13.6`** and press **Enter** to display the logon Web page.
4. Log in as **craft** or **dadmin**.
5. Select **yes** to suppress alarms.
6. Access **System Management Interface (SMI)** to go to the main menu.

Verifying the license file

To verify the license file:

1. Under Security, click **License File**.
2. Verify that the **MultiVantage License Mode** field is **Normal**.

Copying the translation files to the server

To copy translation files to the server:

1. Under Miscellaneous, click **Download Files**.
2. Click **Browse** and select the file that you saved on the Services laptop.
3. Click **Download** to place the file on the server.

Restoring the translation files

To restore the translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Local Directory** and click **View**. The field automatically shows the default directory.
3. Select the first file. The latest file might be at the top of the list.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.
5. Click **Restore** to restore the translation files.
6. Click **Restore Status**.
7. Select the first file, scroll down and click **Review Status** to see the results of the restore.

   When done, the screen shows the message **Restore is finished**.

If the restore process fails, the system displays an error message that states the reason for the failure and the translation file is not restored. Resolve the reason for the failure and restart the process.

Connecting to the standby server

To connect to the standby server:

1. Start a Web browser.
2. Log in as **craft** or **dadmin**.
3. Access **System Management Interface (SMI)**.
4. Under Server, click **Release Server**.
5. Click **Release**.

Connecting to the active server

To connect to the active server:

1. Start a Web browser.
2. Log in as **craft** or **dadmin**.
3. Access **System Management Interface (SMI)**.
4. Under Server, click **Status Summary** to verify that the standby server was refreshed. Do not continue until the standby server is refreshed.
5. Start a SAT session with Native Configuration Manager or Avaya Site Administration.
6. Login as **craft** or **dadmin**.

Installing the translations

To install the translations:

1. Type **`reset system 4`** and press **Enter**.
2. Return the STS-supplied PCMCIA flash card to Avaya.

To add the IPSI translations before you save translations, continue with Setting the alarm activation level on page 426.

Enabling the system for IPSI translations

To enable the system for IPSI translations:

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Verify that the **Primary Control Subnet Address** and **Secondary Control Subnet Address** (was equipped) fields are correct.

   The subnet work addresses must match the most significant three octets (the first three groups of digits in the subnet work address) of the Server IP address that appears on the control network entry from the completed Electronic Preinstallation Worksheet (EPW).

   An asterisk (*****) to the right of the **Subnet Address** field means that although a subnet work address appears, this address is incorrect. Communication Manager call processing software does not have the subnet information. After you verify the information on the screen, submit this form with or without changes to update Communication Manager with the correct subnet work information.

   CAUTION:

   If the information in either the **Primary Control Subnet Address** fields, the **Secondary Control Subnet Address** field, or both, is incorrect, you must change the information on the servers. Use the System Management Interface (SMI). Under Server Configuration and Upgrades, click **Configure Server** to change the server configuration. Then return here to perform Step 3.
3. Verify that the **Switch Identifier** field is set correctly for this installation. The correct Switch Identifier must be entered here before you administer the TN2312 IPSI circuit packs.
4. Verify that the **IPSI Control of Port Networks** field is set to **disabled**.
5. Press **Enter** to submit the screen.

   Note:

   The information that you provide depends on whether the IPSIs get static addresses or the addresses are assigned automatically through DHCP.

Adding IPSI information

To add IPSI information:

1. Type **`add ipserver-interface`** ***`PNnumber`*** where ***`PNnumber`*** is the port network number and press **Enter**.
2. When you use static addressing, in the **Host** field, type in the IP address for the IPSI in the port network that is listed in the **Location** field.

3. Verify that all the other fields are populated.
4. Press **Enter** to put the changes into effect.
5. Repeat Steps 1 through 5 for each port network.

Setting IPSI duplication (high-reliability critical-reliability only)

To set IPSI duplication:

1. Type **`change system-parameters duplication`** and press **Enter**.
2. Set the **Enable Operation of IPSI Duplication** field to **y**.
3. Press **Enter** to put the changes into effect.

Setting the alarm activation level

To set the alarm activation level:

1. Type **`change system-parameters maintenance`** and press **Enter**.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that the customer wants. The default is **none**.

Backing up translations on the S8700-series server

To back up translations:

1. S8710/S8720/S8730: Place a formatted flash card in the compact flash drive attached to a USB port.
2. Start a Web browser.
3. Log in as **craft** or **dadmin**.
4. Access **System Management Interface (SMI)**.
5. Under Data Backup/Restore, click **Backup Now**.

6. Select the data sets and the backup method.

   If you select **Save ACP translations prior to backup**, the server automatically saves the translations to the hard disk before the server saves the translations to the backup media.

7. Click **Start Backup** to start the backup process.

Migration tasks

Perform the following tasks to change a processor port network to a port network (IP600).

Verifying hardware

Ensure that you have the migration specific hardware that you need on hand.

Note:

If customers currently are using the Audix feature on the S8100 Server, they need to purchase a separate Audix system. The TN795 or TN2314 Processor circuit pack containing the Audix feature is being replaced with a TN2312BP Internet Protocol Server Interface (IPSI) circuit pack that does not have that feature. The existing processor circuit pack must be returned to Avaya.

Note:

Customers also must add an ED-1E568-70G1 DEFINITY Audix Slim board and a TN2501AP Voice Announcement over LAN (VAL) circuit pack for announcements.

Changing the IP600 control chassis to a port network

Note:

If you replace a TN795 Processor circuit pack, you might not need the TN744D/E Call Classifier-Detector circuit pack. The TN2312BP IPSI circuit pack has call classifier functionality. However, increased voice and data traffic can require the TN744D/E Call Classifier-Detector circuit pack.

Note:

If you have a TN799C or earlier C-LAN circuit pack, you must replace the TN799 circuit pack with a TN799DP C-LAN circuit pack.

Note:

You must install the latest release of Communication Manager license file on the server before you make the change or the system will not run.

Turning off the control chassis

To turn off the control chassis:

CAUTION:

Ensure that you have completed the premigration administration. For more information, see Premigration administration on page 257.

1. Press and hold the shutdown button on the on the faceplate of the processor until the shutdown process starts.

   Ensure that you see the green light. This light indicates that the system is shut down.

   DANGER:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the chassis, pull the AC power cord from the back of the chassis.

2. To turn off the chassis, unplug the power cord from the back of the chassis.

Replacing I/O cables

On older MCC, SCC, and G600 cabinets you must replace the existing I/O cables (WP-90753, LI), which connect the backplane to the rear connector panel, with twisted pair I/O cables.

The existing I/O cables have straight, not twisted, wires. They may be mostly white with two red, or multi-colored. If the cables have multi-colored, tightly twisted wires, no replacement is necessary.

To order the DEFINITY kit with twisted pair I/O cables, use comcode 700234032.

CAUTION:
Turn off power to the carrier or media gateway being serviced. Failure to turn off the power can result in electric shock.

CAUTION:
When adding or replacing any hardware and associated cables and adapters, be sure to ground yourself against electrostatic discharge (ESD) by wearing a grounded wrist strap. Failure to follow ESD procedures can result in system damage or service disruption.

To replace the existing I/O cables:

1. For the G600 Media Gateway, you must remove the fan assembly to access the cables. Loosen the thumb screws on the fan assembly and pull it straight out as shown in Figure 28: G600 Media Gateway fan assembly removal on page 430. Leave the fan assembly off until all the wires are installed.
2. Note the orientation of the existing 10 cables. The existing I/O cables may be white and red or multicolored. They are not twisted.
3. Remove the nontwisted pair of existing I/O cables from the backplane and the connector panel slots.
4. In their place install the 10 tight-twisted pair I/O cables onto the backplane, according to the proper orientation shown in Figure 29: Proper orientation for the twisted pair I/O cables on page 431. Observe the white outline printed on the backplane for the location of each connector.
5. When viewed from the "wiring" side of the twin connectors (that is, while plugging them into the backplane) and with the connectors oriented properly for plug-in, they should look like Figure 29: Proper orientation for the twisted pair I/O cables on page 431.

   The circled pin locations are “No-Connects”; that is, they have no wires in them. At the top there is an orange-black pair on the right and a violet-brown pair on the left.

   The 50-position metal shell D connectors should be installed into the connector panel with the longer side of the D (pins 1–25) toward the right when viewed from the rear of the media gateway.

6. For the G600 Media Gateway, replace the fan unit if no other media gateways are to be installed. If you are adding more media gateways to the rack, leave the fan units off until all of the TDM cables are installed.

Figure 28: G600 Media Gateway fan assembly removal

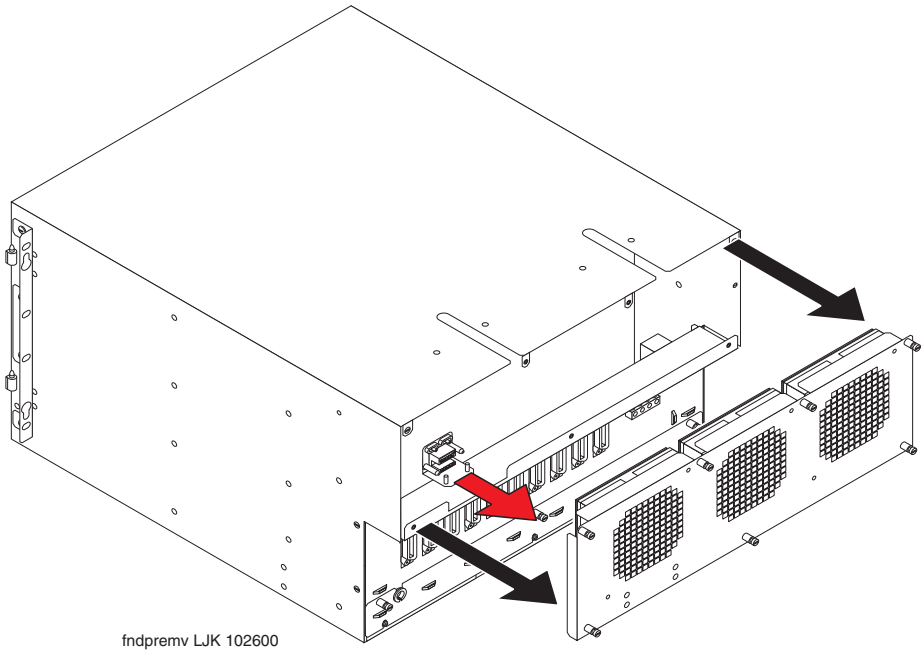


Figure 29: Proper orientation for the twisted pair I/O cables

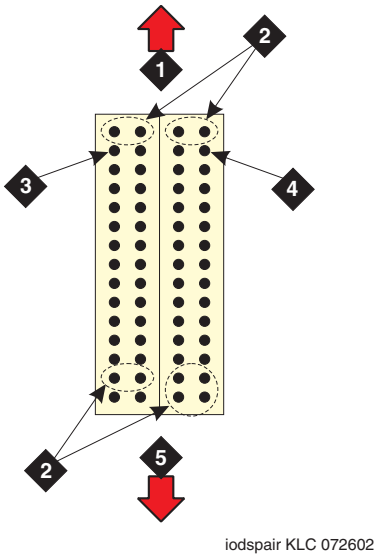


Figure notes:

1. **Top**
2. **No connects; no wires**
3. **Violet-brown**
4. **Orange-black**
5. **Bottom**

Replacing the processor circuit pack

To replace the processor circuit pack:

1. Remove the entire processor circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You want the circuit pack intact if you need to back out of the migration.
3. Remove the octopus cable from the connector that is associated with slot 2 on the backplane.
4. Install the IPSI adapter to the connector that is associated with slot 2 on the backplane.
5. Install the maintenance cable onto the 9-pin D-sub connector on the adapter. This cable is for emergency transfer and "auxsig" signal.

   Note:

   The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack takes only one slot.

6. Insert the TN2312BP Internet Protocol Server Interface (IPSI) circuit pack into slot 2.
7. Attach the new label above the circuit pack slots.

Replacing the TN799C C-LAN circuit pack

If you need to replace the TN799C Control-LAN (C-LAN) circuit pack:

1. Remove the TN799C C-LAN circuit pack.
2. Place the circuit pack in an antistatic carrier or bag. You might need to reinstall this circuit pack if you must stop the migration.
3. Insert the new TN799DP C-LAN circuit pack into the same slot.
4. Replace the 259A adapter and CAT3 cable on the connector panel.
5. Use the adapter that is provided with the new TN799 circuit pack and a CAT5 cable.

Installing TN771 Maintenance/Test circuit pack

You must replace the TN795 or the TN2412 circuit pack with a TN771 Maintenance/Test circuit pack. Each location must have one TN771 Maintenance/Test circuit pack.

To install the TN771 Maintenance/Test circuit pack:

- Install the TN771 circuit pack in slot 1.

  This carrier does not have a dedicated slot for the TN775 Maintenance (EPN) circuit pack.

Connecting the IPSI to the network

After connecting to the server, power up the CMC1 cabinets:

1. Connect one end of the green CAT5 straight-through cable to the Ethernet switch on the customer network.
2. Connect the other end of the cable to the IPSI adapter on the back of the media gateway.

Post-migration administration

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 30: Connecting directly to the IPSI on page 434).

Figure 30: Connecting directly to the IPSI

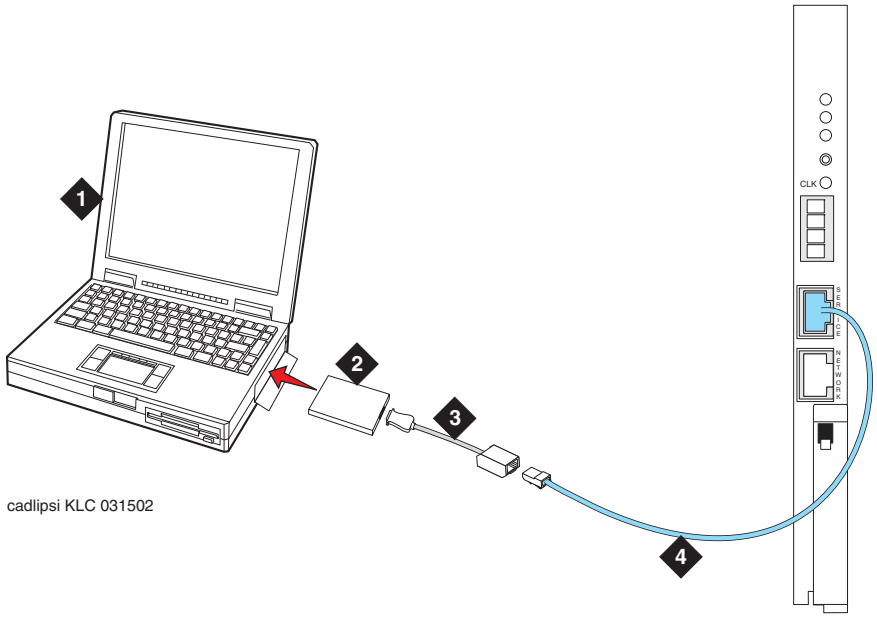


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application on the service laptop to access the server (192.11.13.6 port 22).

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.

2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

Note:

The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`** and press **Enter**.
2. To see the current settings, type **`show port 1`** and press **Enter**.
3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. Verify that the correct information was entered.
5. If a default gateway is used, enter the gateway IP address.
   Type **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway and press **Enter**.
6. To save the changes and exit the IPSI session, type **`quit`** and press **Enter**.
7. SSH to **192.11.13.6** and log in.

8. To verify the administration, type **`show control interface`** and press **Enter**.
9. To see the changes, type **`exit`** and press **Enter**.

Setting the VLAN and diffserv parameters

To set the VLAN parameters and the diffserver parameters:

1. Log back in as **`craft`**.
2. To display the quality of service values, type **`show qos`** and press **Enter**.
3. If necessary, use the following commands to set the VLAN and diffserv parameters to the recommended values shown.

   Note:
   Use **Help** to obtain syntax guidelines for these commands.

   - Type **`set vlan priority 6`**
   - Type **`set diffserv 46`**
   - Type **`set vlan tag on`**
   - Type **`set port negotiation 1 disable`**
   - Type **`set port duplex 1 full`**
   - Type **`set port speed 1 100`**
4. To check the administered values, type **`show qos`** and press **Enter**.
5. To exit, type **`quit`**. Press **Enter**.

   Important:
   Ensure that the port settings on the Ethernet switches are set to the same values as shown in the **`set port`** commands in step 3.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

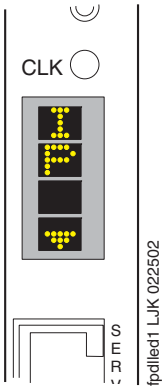
   Note:
   Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

Note:

The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.

2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 31).

Figure 31: LED display that shows that the IPSI has a static IP address



4. Repeat steps 1 through 3 for each IPSI circuit pack.

Note:

Clear the ARP cache on the laptop before you connect to another IPSI. If you do not clear the cache, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "1" shows in any position, you must troubleshoot the problem.

Tip:

The pattern `0.1.1.0` usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct cabinet and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Enabling control of the IPSI

To enable control of the IPSI:

Note:

Ensure that the IPSI has the same, current firmware.

CAUTION:

This procedure allows the server to take control of the IPSI-controlled port network(s). Failure to complete the steps correctly can result in no connection to the network.

1. Type **`change system-parameters ipserver-interface`** and press **Enter**.
2. Set the **IPSI Control of Port Networks:** field to **enabled**
3. Press **Enter** to effect the change.
4. Type **`save translation`** and press **Enter**.

   The server now controls all the port networks.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed cabinets

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the "cabinets." Verify that the cabinet number assigned to the converted cabinets shows.
2. Type **display cabinet number**, where *number* is the cabinet number of the converted cabinet. Press **Enter**. Under Carrier Description, Carrier Type verify that the number of "carriers" in use matches the number of media gateways in the rack (G600 or G650).

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.
2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page (http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885.

Testing the installation

Test the complete installation. For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Troubleshooting the migration

For more information, see the documents included on the CD, *Documentation for Communication Manager Release 5.2, Media Gateways and Servers*, 03-300151. The content of the documentation CD is available at http://avaya.com/support for viewing or downloading.

Returning replaced equipment

Once you determine that the port network functions, return the old processors and any other replaced equipment to Avaya. Use established procedures.

Migrating an Avaya S8400 Server to an S8730 Server

Use these procedures to migrate from an existing Avaya S8400 Server to the Avaya S8730 Server. The existing S8400 Server must be standard reliability. The Avaya S8400 Server being migrated may be located in a G650, G600, or CMC1 Media Gateway.

In all instances, the media gateways can be reused as a port network. However, you can add a G650 Media Gateway port network if the existing system has a port network.

To migrate an existing S8400 Server, remove the TN8400 S8400 Server circuit pack and replace the S8412AP IP Interface circuit pack with one TN2312BP IPSI circuit pack to control the one port network (PN).

This migration affects service because you must power down the media gateway to remove the TN8400 Server and replace the TN812AP SIPI circuit packs.

Disclaimer Statement: This procedure does not account for the possibility that S8400 Server may have IA770 on pre-CM5.2 or CM Messaging CM5.2 or later enabled.

Note:

The Avaya S8400 Server is not being removed neither new system(s) are being introduced to control the system that's being controlled by the S8400 Server.

Migration paths

You can migrate an Avaya S8400 Server to an S8730 Server configuration on:

- Communication Manager Release CM 3.1.x through 5.2

Checklists

Before you go on site, perform the following tasks

:

✓	Task	Description
	Verify that your Services laptop has the appropriate hardware.	Correct hardware components include: ● 40 MB available disk space ● direct Ethernet cable ● serial cable and adapter ● An RS-232 port connector ● A Network interface card (NIC) with a 10/100 BaseT Ethernet interface ● A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X ● CD-ROM drive
	Verify that your Services laptop has the appropriate software	Correct software components include: ● Windows 2000/XP operating system ● Terminal emulation program: HyperTerminal or other ● TCP/IP networking software: bundled with the Windows OS ● Web browser: Internet Explorer 5.0 or later
	Obtain appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: ● Server ● Media gateway ● TN8412AP Server IP Interface (SIPI) or IPSI circuit pack ● auxiliary equipment ● Communication Manager These logins and passwords include the equipment of the customer.
	Obtain the serial number	You need the serial number from the reference TN8412AP Server IP Interface (SIPI) or IPSI and the SAP order number to generate a new license file and authentication file, if necessary.
		1 of 3

✓	Task	Description
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	You use this CD to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your laptop.	Check which service packs you need and download files from the Avaya Support Web site at (http://avaya.com/support).
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your laptop	Check which service packs you need and download files from the Avaya Support web site at (http://avaya.com/support).
	Verify that you have the current firmware.available	The following firmware are on the software CD: • IPSIs or TN8412AP Server IP Interfaces (SIPIs) • C-LAN • MedPro • VAL circuit packs For the most current versions, go to the Avaya Support Web site at (http://avaya.com/support). Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop, if necessary.	Obtain information and download files from the Remote Feature Activation (RFA) web site at http://rfa.avaya.com.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number, 800-248-1234 or 1-720-444-5557, and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.

2 of 3

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	Verify that you have copied all necessary files to your computer	These files can include: • service packs • firmware for programmable circuit packs • license and authentication files (if necessary)
		3 of 3

Premigration setup

The premigration team must complete the following tasks. If these tasks are not completed, do not continue with the migration.

Some tasks need to be completed on site up to two weeks before starting the actual migration.

- Freeze the translations.
- Send the translations to STS.
- Get the translations back from STS by e-mail.

Before you go on site for a migration, complete the following additional tasks before starting the migration:

✓	Task	Description
	About 2 weeks before the migration, freeze the translations. Use a spare flash card to collect the translations locally.	For more information on where and how to send the translations, contact the STS scheduling desk at 720-444-9418. STS updates the translations to the latest version. This process can take 2 weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For forms and more information, contact the STS scheduling desk at 720-444-9418.
	About 2 business days before the migration, create a trouble ticket to contact the STARS team.	Whenever an S8400 server is upgraded from R3.1 onwards, and a new authentication file is requested, ASG access (remote and on-site) is impacted. You need assistance from the Service Tools and Application Remote Support (STARS) team to ensure successful ASG access before and after the upgrade. To contact the STARS team, use http://stars.avaya.com/ticket/requests/request.asp
	Mark the ticket status as CRITICAL.	Indicate text in the ticket to notify the STARS team that you are upgrading an S8x00 server. Include the date of the upgrade and the FL and product or alarm ID of the system. The STARS team contacts you on how to access your product before and after the upgrade. A temporary ASG product ID is created for you and your team to use for access during the time of the upgrade.
	Ensure that the technical support representative has access to the ASG Site Manager tool.	If an engineer who works on the Avaya WAN, is supporting the technical support representative during the upgrade, ensure that the engineer has access to the ASG Mobile tool prior to the upgrade. ASG access (remote or on site) is affected when you upgrade an S8xxx server from 1.x.x to 2.x.x and request a new authentication file.
	The STARS team provides the escalation path to report ASG troubles during the upgrade.	This event happens at least one day prior to the migration.

✓	Task	Description
	Verify that you have the appropriate logins and passwords to access the servers and server complex components.	When you finish installing the authentication file, Communication Manager has a password for all Avaya logins, including craft. This password is unique to the server of the customer. You can use the password the next time you log in as craft, if you access the server through the Services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access requires an ASG challenge and response. This unique craft password remains valid until the password is changed by installing a new authentication file.
	Copy the translation file from STS to a directory on the Services laptop.	File size is usually in the range of 1-4 megabytes.
		2 of 2

On site migration checklist

Before you go on site for a migration, complete the following additional tasks before starting the migration:

✓	Task	Description
	The customer supplies an open EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack. Verify that this rack is installed correctly.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on how to install the rail, see the documentation that comes with the rail kit.
	Verify that you have the license file that the file includes the licensed features.	Use the License File link on the System Management Interface (SMI) to verify.
	Verify that you have the Avaya authentication file.	Use the Authentication File link on the System Management Interface (SMI) to verify.

Performing a migration

The information in this section assumes that the port network is added to an existing S8730 Server complex.

CAUTION:
This migration affects service. When the port network is turned off, the system drops all calls. Service returns when the port network is powered up and the S8730 Server takes control of it.

Premigration administration

This migration is a service-affecting event. The S8400 Server must be turned off to remove the TN8400 Media Server and TN8412AP S8400 IP Interface circuit packs. Before you turn off the port network, you must perform the following premigration administration.

Connecting to the server

To connect to the server:

1. Connect the computer to the services port on the front of the server.
2. Start a SAT session using Native Configuration Manager or Avaya Site Administration.
3. Log in as **craft**.

Verifying system status

Check which groups are in- or out-of-service before the migration. After the migration, compare the after the migration list with the before the migration list to ensure that the lists are the same.

To verify system status:

1. To determine whether the system has administration, run the following commands:
   a. **`list configuration all`**
   b. **`list trunk-group`**
   c. **`list hunt-group`**

   If any command does not complete successfully, escalate the problem immediately. After the migration, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Recording node names and IP addresses

To record node names and IP addresses:

1. Note the node names and the IP addresses that are assigned to the TN2302AP IP Media Processor and the TN799C/DP C-LAN circuit packs. Ensure that these names and addresses are the same after the migration.

   Note:

   If the existing system has TN799C C-LAN circuit packs, you must replace these circuit packs with TN799DP circuit packs.
2. To get the node names for the TN2302AP IP Media Processor and TN799C/DP C-LAN circuit packs, type **`display ip-interfaces`** and press **Enter**.
3. To get the IP addresses that match the node names, type **`list node-names`** and press **Enter**.
4. Record the information for use after the migration.

Saving translations

Although the migrated translations are already copied to the server, you must save the translations in case you need to back out of the migration.

Note:

Save translations to a flash card.

To save translations:

1. To save translations to the system disk, type **`save translation`**. Press **Enter**.

   The system responds with **Command successfully completed**.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

   If you experience trouble connecting to the Web page, go to Clearing the Web browser cache on the laptop on page 230.

Backing up recovery system files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Select the data sets, including **Avaya Call Processing (ACP) translations** and **Save ACP translations prior to backup**. Do *not* select **Full Backup** because this option does not save translations.

Note:

If you back up to a compact flash, Avaya recommends that you use a different flashcard from the one with the prior release translations. You might need these translations if you need to back out of the upgrade, migration, or conversion procedure.

3. Select **FTP** as the backup method and complete the necessary information.
4. Click **Start Backup** to start the back up process.

Migration tasks

You can reuse the translations from the existing system when you migrate to an S8730 Server.

Verifying hardware

Ensure that you have the migration specific hardware on hand.

Turning off the power to the port network

CAUTION:

Ensure that you have completed the premigration administration. For more information, see Premigration administration on page 388.

To turn off power:

1. From the bash prompt on the Services laptop, type **shutdown system** and press **Enter** to perform a graceful shutdown.
2. Wait until the Shutdown Complete LED on the lower portion of the faceplate of the server is solid green
3. Turn off the power to all media gateways. Unplug the power cord for safety purpose.

Note:

Gateways with the TN8400 and TN8412 needs to be powered off. The other carriers may remain powered on.

DANGER:

The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the media gateway, pull the AC power cord from the back of the media gateway.

Shutting down the Avaya S8400 Server and powering down the Media Gateway

To shut down the Avaya S8400 Server:

1. Perform a complete server backup to the LAN or to the translations Compact Flash card (front slot of the Avaya S8400 Server).
2. Push and hold the Shutdown button (Note 1 in Figure 32: Avaya S8400 front faceplate) for more than two (2) seconds.

Figure 32: Avaya S8400 front faceplate

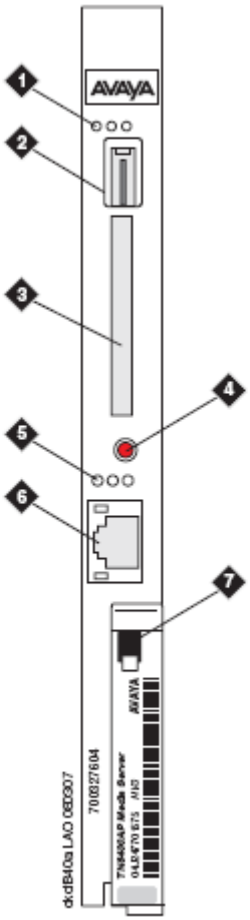


Figure notes:

1. **Shutdown button (hold for more than 2 seconds)**
2. **OK to Remove LED**
3. **Safety latch**
4. **Compact Flash slot for translations**
5. **Circuit pack failure LED (red)**

The green OK to Remove LED (Note 2 in Figure 32) flashes to indicate that shutdown is in progress.

3. When the green OK to Remove LED is on steady unlatch the circuit pack (Note 3 in Figure 32), slide it out of its slot, and set it on the antistatic mat.
4. Leave the Compact Flash card with translations in the slot (Note 4 in Figure 32).

Note:

The Avaya S8400 Server has a cable adapter attached at the rear of the carrier. Leave this adapter and its cable connections in place during the entire replacement procedure.

Removing the TN circuit packs

To remove both the circuit packs:

1. Release the latch that secures the circuit pack.
2. Pull the circuit pack straight out of the slot and free of the media gateway.

Important:

Remember which slot that the TN8412AP circuit pack was located. The TN8412AP Server IP Interface (SIPI) location configuration is different depending on the media gateway in which it resides.

3. Remove the cable(s) connected to the adapters first. Remove the adapters for the circuit packs from the rear of the media gateway. You can reuse the cable that connects to the TN8412AP Server IP Interface (SIPI) adapter but you won't need the cables connected to the S8400 server.

Note:

You can also reuse the TN8412AP Server IP Interface (SIPI) adapter for the IPSI.

Installing the IPSI

To install the IPSI:

1. Insert the TN2312BP IPSI circuit pack in the former location of the TN8412AP.
2. Install the TN2312BP IPSI adapter on the rear of the media gateway. in the former location of the TN8412AP SIPI adapter.
3. Connect the Ethernet cable into the IPSI adapter.

Turning on power to the port network

To turn on power to the port network:

1. Plug in the power cord to the back of the media gateway.
2. Push in the latch on the power supply to start power.
3. Plug one end of the power cord into the back of the power supply and the other end into a UPS or nonswitched outlet.

Turning on G650 Media Gateway

To connect the power cords:

1. Ensure that the circuit breakers at the AC load center are OFF.
2. Connect the G650 Media Gateway to a UPS or to an electrical outlet that is “nonswitched” or “always on”

   Note:

   Remove the emergency ground wire if used.

Checking AC power:

Each G650 Media Gateway uses at least one auto-ranging (90-VAC to 265-VAC) power supply:

- 47 to 63 HZ
- 500 W output
- 7.2 A (90 VAC) or 3.3 A (200 VAC)

Connecting to DC power

Each G650 Media Gateway can be equipped with a maximum of two 655A power supplies. One power supply is always provided in slot 0, and a redundant unit can be provided in slot 15. DC power is supplied by a DC feed cable to one connector on the backplane of the G650 Media Gateway. The power is then bussed to each power supply slot. AC current and DC current can be supplied to the 655A power supplies at the same time. When both AC current and DC current are present, the 655A uses AC first. The 655A power supply then changes to DC current without any interruption in service if the AC current fails.

Each G650 Media Gateway, with either a single power supply or redundant power supply, draws a maximum of 17 A of DC current.

Assigning IP addresses to the IPSI circuit packs

When you use static IP addressing, you must assign IP addresses to the IP server interface circuit packs.

Using static addressing

You can administer static IP addresses for the IPSI circuit packs. You administer the addresses directly through the Ethernet port connection on the IPSI faceplate switch which is the top port (Figure 33: Connecting directly to the IPSI on page 458).

Figure 33: Connecting directly to the IPSI

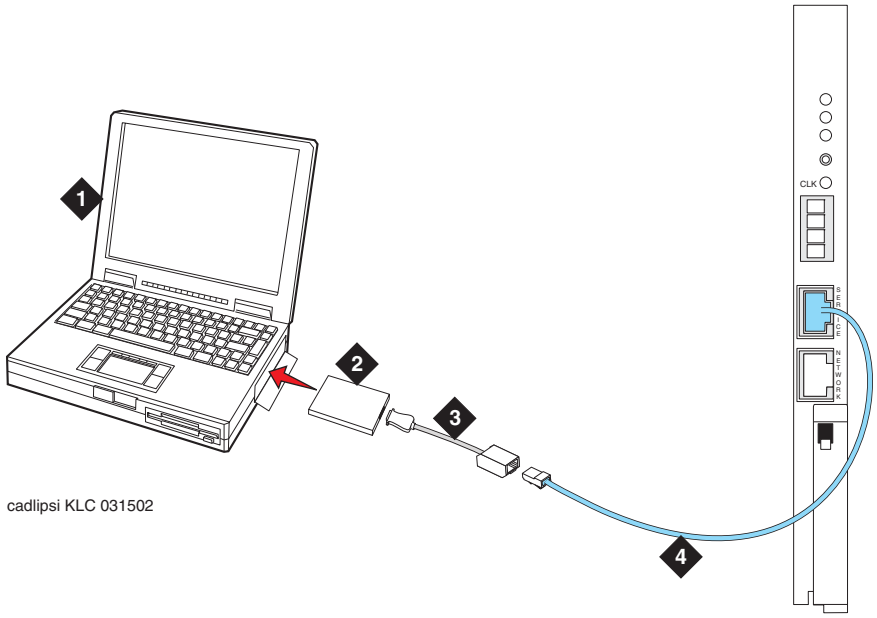


Figure notes:

1. **Services laptop**
2. **PCMCIA Network Interface Card (NIC)**
3. **NIC adapter cable (if necessary)**
4. **CAT5 cross-over cable to IPSI**

Note:

Ensure that you have the IPSI password before you continue.

Clearing the ARP cache on the laptop computer

You might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. This need depends on the operating system on your laptop computer. If you enter an IP address and your computer cannot connect, you might need to clear the cache.

To clear the ARP cache on the laptop:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. To open an MS-DOS command line window, type **`command`** and press **Enter**.
3. Type **`arp -d 192.11.13.6`** and press **Enter**. This command produces one of the following responses:
   - The command line prompt displays when the cache is cleared.
   - The message **The specified entry was not found** appears when the specified IP address does not currently appear in the ARP cache.

4. To access the server, type **`ping -t 192.11.13.6`** and press **Enter**.

   The **`-t`** causes the ping to repeat until you get a response. When you get a response, in about 3 minutes, wait an additional 30 seconds before you go back to the Web interface.

5. To stop the ping, type **`ctrl c`** and press **Enter**.
6. Close the MS-DOS window.

Logging in to the IPSI

To log in to the IPSI:

1. Use the PuTTY application to access the IPSI using the secure shell (SSH) protocol.

   Note:

   Most commands have abbreviations. For more help while you are connected to the IPSI, you can type **`help`** or **`?`**.

2. Type **`ipsilogin`** and press **Enter**. The abbreviated command is **il**.

   Note:

   The *craft* login that you use on the IPSI has a different password than the *craft* login used on the servers.

3. Log in as **`craft`**.

   Prompt = [IPADMIN]:

Setting the control interface

To set the control interface:

1. Type **`show control interface`** and press **Enter**.
2. To see the current settings, type **`show port 1`** and press **Enter**.

3. Type **`set control interface`** ***`ipaddr netmask`***, where ***`ipaddr`*** is the customer-provided IP address and ***`netmask`*** is the customer provided subnetmask and press **Enter**.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]: 
```

4. To save the changes and exit the IPSI session, type **`quit`** and press **Enter**.
5. SSH to **192.11.13.6** and log in.
6. Type **`show control interface`** and press **Enter**.
   The system displays the IP address, the subnetmask, and the default gateway information.
7. Verify that the correct information was entered.
8. If a default gateway is used, enter the gateway IP address.
   Type **`set control gateway`** ***`gatewayaddr`***, where ***`gatewayaddr`*** is the customer-provided IP address for their gateway and press **Enter**.
9. To save the changes and exit the IPSI session, type **`quit`** and press **Enter**.
10. SSH to **192.11.13.6** and log in.
11. To verify the administration, type **`show control interface`** and press **Enter**.
12. To see the changes, type **`exit`** and press **Enter**.

Resetting the IPSI

To reset the IPSI:

1. Type **`reset`** and press **Enter**
   Answer **Y** to the warning.

   Note:

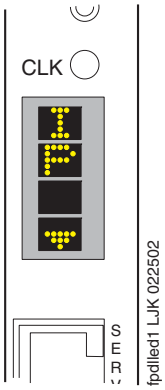
   Resetting the IPSI terminates the administration session. If further administration is required, start a new SSH session to the IPSI.

   Note:

   The IP address, subnet mask, and gateway control network settings become effective when you exit the IPADMIN session.

2. Disconnect the laptop computer from the faceplate.
3. Check the LCD. Verify that the display shows the letters I and P and a filled-in V that shows at the bottom (Figure 34: LED display that shows that the IPSI has a static IP address on page 461).

Figure 34: LED display that shows that the IPSI has a static IP address



Note:

Clear the ARP cache on the laptop before you connect to another IPSI. If you do not clear the cache, the laptop appears to stop and does not connect to the next IPSI. For more information, see Clearing the ARP cache on the laptop computer on page 230.

Postmigration administration

Perform the following tasks to complete postmigration administration.

Clearing the Web browser cache on the laptop

Due to underlying changes on Communication Manager Web pages, you might experience problems with accessing some of the pages. For example, you might see some strange behavior when using the same laptop/PC to switch in-between Communication Manager loads or releases, especially when accessing the Communication Manager server(s) through the Services port (http://192.11.13.6). This is due to how your web browser is caching information and it does not always know what is new and what is old.

For example, for Communication Manager Release 3.1 and earlier, you log into https://192.11.13.6 and it takes you to https://192.11.13.6/log-in.

But if you are in Communication Manager Release 4.0/4.1 and you log into https://192.11.13.6, it takes you to https://192.11.13.6/log-in/web-page (or something similar).

The problem is that the laptop gets confused after it has been at Release 4.0/4.1 and then you want to go to another site in pre Release 4.0. The system cannot find the old login page.

This happens only if you are switching between releases and/or loads - especially if you go backwards in releases (for example, from Release 4.1 on Server 1 to Release 3.0 on Server 2). There does not seem to be a problem going forward in releases.

If you are experiencing problems logging in to Web pages:

1. On the Internet Explorer page, select **Tools** > **Internet Options**.
2. In the Temporary Internet files section, click **Delete Cookies**.
3. Click **OK**.
4. In the Temporary Internet files section, click **Delete files**.
5. Click **OK**.
6. In the History section, click **History**.
7. Click **OK**.

Connecting to the active server

To connect to the active server:

1. Connect one end of the CAT5 cross-over cable to the Services port on the S8730 Server.
2. Connect the other end of the cable to the Services laptop.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**

   If you experience trouble connecting to the Web page, go to Clearing the Web browser cache on the laptop on page 230.

Clearing the ARP cache on the laptop computer

You might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. This need depends on the operating system on your laptop computer. If you enter an IP address and your computer cannot connect, you might need to clear the cache.

To clear the ARP cache on the laptop:

1. Click **Start** > **Run** to open the **Run** dialog box.
2. To open an MS-DOS command line window, type **`command`** and press **Enter**.
3. Type **`arp -d 192.11.13.6`** and press **Enter**. This command produces one of the following responses:
   - The command line prompt displays when the cache is cleared.
   - The message **The specified entry was not found** appears when the specified IP address does not currently appear in the ARP cache.

4. To access the server, type **`ping -t 192.11.13.6`** and press **Enter**.

   The **`-t`** causes the ping to repeat until you get a response. When you get a response, in about 3 minutes, wait an additional 30 seconds before you go back to the Web interface.
5. To stop the ping, type **`ctrl c`** and press **Enter**.
6. Close the MS-DOS window.

Busying-out the server

Note:

Perform this procedure on the standby S8730 Server.

To busy-out the standby S8730 Server:

1. Under Server, click **Busy-out Server**.
2. On the **Busy-Out Server** window, click **Busy Out**.
3. Click **Status Summary** to verify that the server is busied out.

Migrating translation files

To migrate translation files:

1. Under Data Backup/Restore, click **View/Restore Data**.
2. Select **Network Device** and complete the necessary information
   - **FTP**
   - User name
   - Password
   - Host name
   - Directory.
3. Select the translation file you created back in Backing up recovery system files on page 451. The latest file might be at the top of the list.
4. Select **Force restore if server name mismatch** and **Force restore if backup version mismatch**.
5. Click **Restore** to restore the translation files.

6. Click **Restore Status**.
7. Select the first file and then scroll down and click **Review Status** to see the results of the restore.

   When the restore process completes, the screen displays **Restore is finished**.
8. Use Native Configuration Manager or Avaya Site Administration to start a SAT session.
9. Type **`reset system 4`**. Press **Enter** to load the restored translations.

If the restore process fails, the system displays an error message that states the reason for the failure. The translation file is not restored. You must resolve the reason for the failure and restart the process.

Verifying IPSI translations

To verify IPSI translations:

1. Type **`list ipserver-interface`** and press **Enter**.
2. Verify that the ISPI circuit pack(s) are translated.

   The State of Health - C P E G column shows `0.0.0.0` for each healthy IPSI. If a "1" shows in any position, you must troubleshoot the problem.

   Tip:

   The pattern `0.1.1.0` usually means that a media gateway is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.
3. The IPSI translations may need to be modified depending on the previous TN8412AP SIPI circuit pack translations (using internal addresses).
   - If the TN8400 was directly connected to the TN8412, then you need to provide a network address for the new IPSI. See Setting the control interface on page 459.
   - If the TN8412AP Server IP Interface (SIPI) was directly connected to the customer network, then no further translations are needed.

Verifying IPSI connectivity

To verify IPSI connectivity:

1. Under Diagnostics, click **Ping**.

2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Type the correct media gateway and carrier numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying the customer data

The new translations must include all the media gateway and circuit pack administration. This data includes the:

- Media gateway
- Circuit pack administration of the changed media gateways

Verify that the data is correct.

Verifying circuit pack locations

To verify circuit pack locations:

1. Type **`list cabinet`**. Press **Enter** to view all the media gateways. Verify that the screen shows the media gateway number that is assigned to the changed media gateways.
2. Type **`display cabinet`** ***`number`***, where ***`number`*** is the media gateway number of the changed media gateway and press **Enter**. Under Carrier Description, Carrier Type, verify that the number of carriers is the number of cmc carriers in the port network.
   - For a **cmc-carrier-stack**, the number of cmc carriers in the port network.

Verifying circuit pack insertion

To verify circuit pack insertion:

1. To see the list of all the slot locations, type **`list configuration all`** and press **Enter**.

2. Verify that the circuit pack code and vintage number appears in the **Code** and **Vintage** fields. If **No board** appears in either field, a circuit pack was not installed in that slot.

Verifying the IP addresses

Ensure that the node names and IP addresses assigned to the TN2302AP IP Media Processor circuit pack and the TN799DP C-LAN circuit pack are the same as before the migration.

To verify the IP addresses:

1. To get the node names for the TN2302AP IP Media Processor circuit pack and TN799DP C-LAN circuit pack in the slots of interest, type **`list ip-interfaces`**. Press **Enter**.
2. To verify that the node names exist and that the IP addresses match the node names, type **`list node-names`**. Press **Enter**.

Checking the link status

Compare the list that you made before the migration. Ensure that the in-service or the out-of-service links match the status of the links before the migration.

To check the link status:

1. Type **`display communication-interface links`** and press **Enter**.
2. Record all the enabled links.
3. Type **`status link number`** where ***`number`*** is a number **1-99** and press **Enter**.
4. Compare which links are in service with the premigration list.
5. Repeat steps 3 and 4 for all link numbers.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the

firmware, you also can go to Avaya Support Web page(http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see Upgrading firmware on the IPSIs and SIPIs on page 315.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see Upgrading firmware on the IPSIs and SIPIs on page 315.

Testing the installation

Test the complete installation. For more information, see *Installing and Configuring the Avaya S8400 Server Release 5.0* (03-300678) *and/or visit: http://support.avaya.com*

Busying out previously busied-out trunks

- If you recorded any busyouts earlier on the main server only, you must ensure that they also are busied out after the migration.

Checking for translation corruption

To check for translation corruption:

1. On the SAT, type **`newterm`** and press **Enter**.
2. If you see the following message:

Warning: Translation corruption detected . . .

then follow the normal escalation procedure for translation corruption before continuing the upgrade.

Resolving alarms

To clear alarms:

1. On the System Management Interface (SMI) under **Alarms**, click **Current Alarms** to examine the alarm log.
2. Select the server alarms that you want to clear and click **Clear**, or click **Clear All.**
3. Resolve or clear Communication Manager alarms with SAT commands and the Maintenance Commands Reference and Alarms Maintenance books.

Backing up system files

To back up the system files:

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Select the data sets, including **Avaya Call Processing (ACP) translations** and **Save ACP translations prior to backup**. An ESS server or an LSP gets translations from the main server, so there is no reason to back up the translations on an ESS server or an LSP. Do not select **Full Backup** because this option does not save translations.

   Note:

   If you back up to a flashcard, Avaya recommends that you use a different flashcard from the one with the prior release translations. You might need these translations if you need to back out of the upgrade, migration, or conversion procedure.
3. Select the backup method.
4. Click **Start Backup** to start the back up process.

Logging off all administration applications

- When you complete all the administration, log off all the applications that you used.

Registering Communication Manager

Follow standard procedures to register the new software.

Releasing the standby server

To release the server from busyout mode, if necessary:

1. Under Server, click **Release Server**.
2. On the **Release Server** window, click **Release**.
3. To verify that the standby server is not busied out, click **Status Summary**.

Troubleshooting the migration

For more information, see *Installing and Configuring the Avaya S8400 Server Release 5.0 (03-300678), and/or visit: http://support.avaya.com*

Returning replaced equipment

Once you determine that the port network functions, return the TN8400 S8400 Server circuit pack and any other replaced equipment to Avaya. Use established procedures.

Migrating an S8500-Series Server to an S8730 Server

Use these procedures to migrate an existing S8500-Series Server to an S8730 Server configuration. In this migration, you can configure the S8730 Server but reuse the translations from the S8500-Series Server. This migration requires a new RFA license file.

With this migration, you can also upgrade to Communication Manager Release 5.x.

This migration affects service because you must turn off the S8500-Series Server before you change over to the S8730 Server.

Disclaimer Statement: This procedure does not account for the possibility that S8500/S8510 Server at CM5.2 or later may have CM Messaging enabled.

Upgrading media gateways LSPs and ESS servers

Note:

If the customer has no media gateways or no local survivable processors (LSPs), skip these tasks and go to On the first S8730 Server on page 483.

If the configuration is using media gateways and media modules and newer firmware exists for them, you must upgrade the firmware on them first. If the server is the primary controller for a media gateway equipped with an LSP or if the server is an ESS server, you must upgrade the software *before* you transfer control to the S8730 Server. The correct order is:

1. Upgrade media gateway firmware to latest version
2. Upgrade media modules firmware to latest version
3. Upgrade the LSPs
4. Upgrade the ESS server
5. Upgrade the main server

Enterprise Survivable Servers (ESS)

The migration procedures in this chapter can be used for both the main server and an ESS server. If a procedure is used for only one server type it will be noted. If the main server is migrating to an S8730 Server, the ESS servers must be:

- Upgraded to 5.x *prior* to the migration of the main server: An ESS server must be running the same or a later release than that of the main server.

  Important:
  The server type that can be used as an LSP or an ESS server changes depending on the main server type. For information on compatibility, see Table 3: LSP or ESS server types for Release 5.2.

Local Survivable Servers (LSP)

If the main server is migrating to an S8730 Server, the LSPs must be:

- Upgraded to 5.x prior to the migration of the main server. An LSP must be running the same or later release than that of the main server.

  Important:
  The server type that can be used as an LSP or an ESS server changes depending on the main server type. For information on compatibility, see Table 3: LSP or ESS server types for Release 5.2.

Prerequisites

Before you start the software migration and the server configuration, you must verify that:

- The customer has a local area network (LAN) that is set up and running and a network administrator who is available to assist you on the date of the migration.
- You have the IP addresses and the unique names for the servers.
- You have a new license file and a password file.
- The Services laptop has the correct hardware and software.
  - Windows 2000 or Windows XP operating system
  - 32-MB of RAM
  - 40-MB of available disk space
  - An RS-232 port connector
  - A network interface card (NIC) with a 10/100BaseT Ethernet interface
  - A 10/100 BaseT Ethernet, category 5 (or better), cross-connect cable with an RJ45 connector on each end (MDI to MDI-X)
  - A CD-ROM drive

- You have the current translations available for download by ProVision.
- You have a filled-out Electronic Pre-Installation Worksheet (EPW). For the blank form, see the Avaya Installation Wizard Web site (http://support.avaya.com/avayaiw). The EPW provides:
  - An IP addresses
  - A product ID
  - An Avaya Services telephone number for remote access over modem
  - An Avaya Services IP address for alarms through the network
- You have the current firmware available. Firmware for the IPSI, the C-LAN, the MedPro, and the VAL circuit packs are part of the software CD-ROM. For the latest software and firmware, see the Avaya Support Web site http://support.avaya.com. Click **Find Documentation and Downloads by Product Name**.
- You have the login IDs and the passwords to access the S8500-Series Server and the S8730 Server and the server complex components. The password includes the unique service password for that equipment of the customer.

  To obtain the password for a specific server, call ASG Conversant at 9-800-248-1234 or 1-720-444-5557. You must have the IL, FL, or product ID to get the password.

  To log in through the Services port as craft after you install the Avaya authentication file, use this password. This password does not require an ASG challenge or response.

Premigration administration

CAUTION:
The licensing of the platform and port network connectivity attributes for the S8730 Server can be complex. See Server Migration Paths on page 50 and License and Avaya authentication files on page 47.

Hardware verification

Ensure that you have the conversion specific hardware on hand. You can reuse some of the equipment and cables when you migrate from an S8500-Series Server to an S8730 Server. However, you need new equipment to complete the migration.

Upgrading firmware

Each IPSI must be on the most current and same firmware load. You might need to upgrade the firmware on the IPSI. The most current firmware load is on the installation CD. To obtain the firmware, you also can go to Avaya Support Web page(http://avaya.com/support and click **Downloads**.

First, verify the version of firmware that is currently on the IPSI circuit pack.

1. Access the **System Management Interface (SMI)** and click on **Administration > Server (Maintenance)**.
2. Under IPSI Firmware Upgrades, click **IPSI Version.** Select **Query All** and click **View**.
3. Verify the firmware release for the TN2312BP IPSI.

If necessary, upgrade the firmware on the just installed TN2313BP IP Server Interface circuit pack that you just installed. For more information, see Upgrading firmware on the IPSIs and SIPIs on page 315.

You also must upgrade the firmware on the following circuit packs, if necessary.

- UDS1 (TN464GP, TN2464BP, and TN2313AP)
- Maintenance/Test (TN771DP)
- Control-LAN (C-LAN) (TN799DP)
- IP Media Processor (TN2302AP)

For more information, see Upgrading firmware on the IPSIs and SIPIs on page 315.

Upgrading G150, G250, G350, G430, G450, G700, J4350, or J6350 Media Gateways and local survivable processors (if being used)

Note:

If the customer has no G150, G250, G350, G430, G450, G700, J4350, or J6350 Media Gateways or no local survivable processors (LSPs), skip these tasks and go to On the first S8730 Server on page 483.

If the configuration is using G150, G250, G350, G430, G450, G700, J4350, or J6350 Media Gateways and media modules and newer firmware exists for them, you must upgrade the firmware on them first. If the server is the primary controller for a G700 Media Gateway equipped with an LSP, you must upgrade the software on the LSPs *before* you transfer control to the S8730 Server. The correct order is:

1. Upgrade media gateway firmware to latest version
2. Upgrade media modules firmware to latest version
3. Upgrade the server software to latest version if using LSPs

Transfer control to the S8730 Server.

Upgrading software on the LSP

Although the LSP remains registered with the primary controller, the LSP will not accept translations if it is running an older version of the software than the software that is on the primary controller.

For more information on the software upgrade process, see:

- *Installing and Upgrading the Avaya S8300 Server*, 555-234-100.
- *Installing and Upgrading the Avaya G700 Media Gateway*, 03-603333.

CAUTION:

You must stop call processing on the LSPs during the migration process. You can stop call processing on the *active* server. If you do not stop call processing on the LSPs, all calls to the LSPs will be dropped.

Migration tasks on the S8500-Series Server

The information in this section is based on the assumption that the server complex is installed, configured, and operational.

Connecting to the server

To connect to the server:

- Use a cross-connect CAT5 cable to connect the laptop to the Services port (2) on the back of the server.

Checking for translation corruption

To check for translation corruption:

1. On the SAT, type **`newterm`** and press **Enter**.
2. If you see the following message:

   Warning: Translation corruption detected . . .

   then follow the normal escalation procedure for translation corruption before continuing the upgrade.

Disabling scheduled maintenance

To prevent scheduled daily maintenance from interfering with the migration:

1. Type **`change system-parameters maintenance`**. Press **Enter**.
2. Record the settings for the **Stop Time** and **Start Time** fields.
3. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

   or

   If scheduled maintenance is not in progress, set the **Start Time** field to a time after the migration is completed.

   For example, if you start the migration at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to 21:30.

Saving translations (main only)

The save translation command is release dependent.

Release	Load	Command	Condition
2.0	219.0	save translation lsp	If LSP is present
2.0.1	221.1	save translation lsp	If LSP is present
2.1	411.7	save translation all	If LSP is present
2.1.1	414.1	save translation all	If LSP is present
2.2	111.4	save translation all	If LSP is present
2.2.1	118.0	save translation all	If LSP is present
3.0 and later	340.3 and later	save translation all	If LSP or ESS is present

To save translations, perform the following step:

- Type **`save translation all`** and press **Enter**.
  - If this operation is unsuccessful, follow the normal escalation procedures before continuing.

Obtaining the product ID on the S8500-Series Server

To obtain the Product ID:

1. Access the server command line interface.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**. Press **Enter**.
4. Record the product ID and the RMB product ID.

Obtaining the Cluster ID

To obtain the cluster ID:

1. At the command line interface, type **`server`** Press **Enter**.
2. Save the output of the server command to your laptop using the steps outlined in How to copy the configuration screens on page 479.

Run almcall

To run almcall:

1. At the command line interface, type **`almcall`** and press **Enter**.
2. Save the output of the server command to your laptop using the steps outlined in How to copy the configuration screens on page 479.

Run almenable

To run almenable:

1. At the command line interface, type **`almenable`** and press **Enter**.
2. Save the output of the server command to your laptop using the steps outlined in How to copy the configuration screens on page 479.

Run modserve

To run modserve:

1. At the command line interface, type **`modsrv -v`** and press **Enter**.
2. Save the output of the server command to your laptop using the steps outlined in How to copy the configuration screens on page 479.

Copy the configuration information for the S8500-Series Server

The configuration information found in the **Communication Manager System Management Interface (SMI)** for the S8500-Series Server will be used to configure the S8510 Server. You ***cannot*** complete the migration without this information. You can manually copy the information in each screen (not recommended), copy and save each screen to your computer, or print each screen.

You may also use the EPW to record most of the server configuration data. The EPW can be used later to configure the S8510.

How to copy the configuration screens

Use the following steps to copy each configuration screen. When you choose to copy the screen, each screen can be stored as a separate file on your PC.

1. Create a new folder on your PC to store the configuration files that you copy. Storing the files in a new folder will make finding them easier.
2. You can copy the screens to Word, Wordpad, or Paint. Decide which application you are going to use and open it on your PC.
3. When the configuration screen is displayed on your computer, hit Alt +PrintScrn on your keyboard. The captured screen is copied into the Windows clipboard.Bring up the application you are going to copy the screen into (Word, Wordpad, or Paint):
   a. Left click on your mouse and select **Paste**. The configuration screen should appear in your application window.
   b. Click **File** and select **Save As**. Select the folder you created in step 1. In the **File Name** field, change the name of the file to match the configuration screen that you copied. Click **Save**.

Viewing the configuration screens to copy or print

In the **Communication Manager System Management Interface (SMI)**.

1. Click **Configure Server** under **Server Configuration**.
   a. In the **Review Notices** screen, click **Continue**.
   b. In the **Back Up Data** screen, click **Continue**.
   c. In the **Specify how you want to use this wizard** screen, click the **Configure all services using the wizard** radio button, then **Continue**.
   d. Print or copy the following screens:
      - **Set Identities**
      - **Configure Interfaces**
      - **Configure ESS/LSP**
      - **Configure Switches**
      - **Set DNS/DHCP**
      - **Set Static Routes**
      - **Configure Time Server**
      - **Set Modem Interface**
      - **Configure RSA**: You will use the RSA settings when you configure the RMB on the S8510.
      - **Update System**

e. After copying or printing the Configure Server screens, click **Cancel**. ***Do not*** click **Submit**.

2. Check the following screens under the **Alarms** heading for data. If the screens are administered, copy or print them.
   - **SNMP Agents**
   - **SNMP Traps**
   - **Filters**

   Note:

   The SNMPV3 authentication password and privacy password will not display on the screen.

Backing up the translation files to the compact flash

Backing up the translation files to the compact flash is the preferred method of backup for this migration. To back up the translation data set from the **Communication Manager System Management Interface (SMI)**:

1. Connect the cord of the compact flash disk into one of the USB ports on the S8500-Series Server.
2. Insert a formatted 128-MB compact flash drive into the drive.
3. On the menu, click **Data Backup/Restore** > **Backup Now**.
4. Click **Specify Data Sets** and select **Avaya Call Processing (ACP) Translations**. ***Do not*** select any other data sets.
5. Select **Local PC Cord**.
6. Click **Start Backup** to start the backup process.
7. Click **Data Backup/Restore** > **Backup History** to view the progress of the backup process.
8. When the backup is finished, disconnect the USB card reader/writer from the S8500-Series Server.

Shutting down the S8500-Series Server

To shut down the S8500-Series Server:

CAUTION:
Do not unplug a functioning server unless you first stop all processes. If you unplug a functioning server but do not stop all processes first, you can corrupt the hard disk drive.

1. Under Server, click **Shutdown Server**.
   a. Clear **Restart Server after Shutdown**.
   b. Select **Delayed shutdown**
2. Click **Shutdown**.

CAUTION:
Wait about 30 seconds.Do not hold down the power button for more than a second. If you hold the button down too long, the server to reboots.

3. Press and release the power-control button on the front of the server.

   The internal fan shuts off.

Disconnecting the cables

Label and disconnect the cables off the back of the S8500-Series Server. If you are not sure what the cable is, use the **Set Identities** screen that you captured in Copy the configuration information for the S8500-Series Server on page 478 as a reference. For example, if the **Set Identities** screen shows that Control Network A is connected to Eth0, find Eth0 on the S8500-Series Server, label the cable Control Network A, and then disconnect the cable.

Disconnect the following cables:

1. The laptop from the Services port
2. The power cord from S8500-Series Server
3. The power cord from the RSA or SAMP
4. The modem from the RS-232 port on the SAMP or RSA card
5. The LAN connection (if used) from the Ethernet port on the SAMP or RSA card
6. The cable(s) from the Ethernet ports

Remove the S8500-Series Server and the side rails from the rack

1. Remove the S8500-Series Server from the rack.
2. Remove the side rails (if present) from the rack.

On the first S8730 Server

Removing a DAL1 or installing a DAL2 card

A DAL2 is required for an S8730 Server using hardware duplication. If you are not using hardware duplication, go to Installing the first S8730 Server in the rack on page 483.

If you are using hardware duplication, verify the type of DAL board that is installed in the server by looking at the label printed on the DAL board. If both S8720 Servers have a DAL2 installed, proceed to Installing the first S8730 Server in the rack on page 483.

If you must replace a DAL1 with a DAL2, or install a DAL2, see Appendix B: DAL: Removing or Installing on page 345. Once you have replaced or installed the DAL ***on both servers***, continue with Installing the first S8730 Server in the rack on page 483.

Installing the first S8730 Server in the rack

To install the first S8730 Server in the rack:

1. Snap the rails on to the server.
2. Attach the extension rails to the rack.
3. Install the S8730 Server in the rack. For more information, see *Quick Start for Hardware Installation Avaya S8700 Series Servers* (555-245-703).

Inserting the Communication Manager software distribution CD

To insert the Communication Manager software distribution CD in the S8730 Server:

Note:

You must place the CD in the CD/DVD drive before turning on the server.

1. Use a paperclip to open the CD-ROM drive on the server.
2. Insert the Communication Manager software distribution CD in the CD/DVD drive and close the drive door.

Connecting the cables to the first S8730 Server

To connect the cables to the server:

Note:

Do not connect the fiber duplication connection cable or the duplication interface IP cable at this time to either S8730 Server.

1. The network connections depend on the type of memory duplication and the type of control network being used. Connect the network cables as described in the following table.

Control Network	Software Memory Duplication	Hardware Memory Duplication
Dedicated	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled 1) • CNB (if used) to Eth3 (right top)	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled **1**) • CNB (if used) to Eth3 (right top)
Nondedicated	• LAN/CNA to Eth2 (right bottom) • CNB (if used) to Eth3 (right top)	• LAN/CNA to Eth0 (middle bottom labeled **1**) CNB (if used) to Eth3 (right top)

Figure 35: Duplication and control network cables for hardware duplication

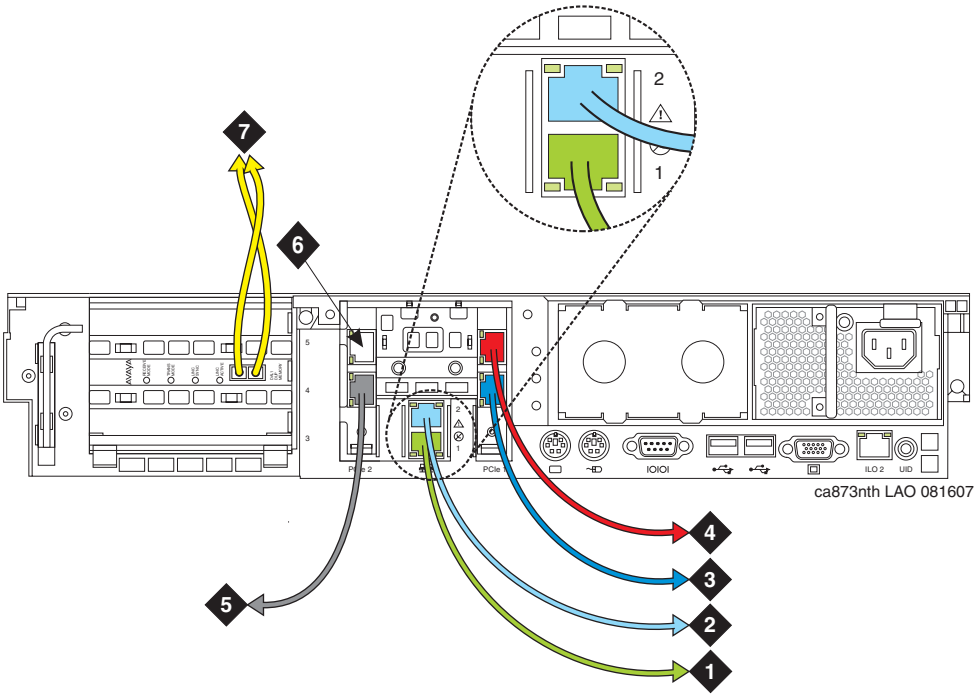


Figure notes:

1. **CNA (also LAN for nondedicated control network) — Eth0**
2. **Services port — Eth1**
3. **Duplication cable (crossover) — Eth2**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**
7. **Fiber duplication cable**

Figure 36: Duplication and control network cables for software duplication

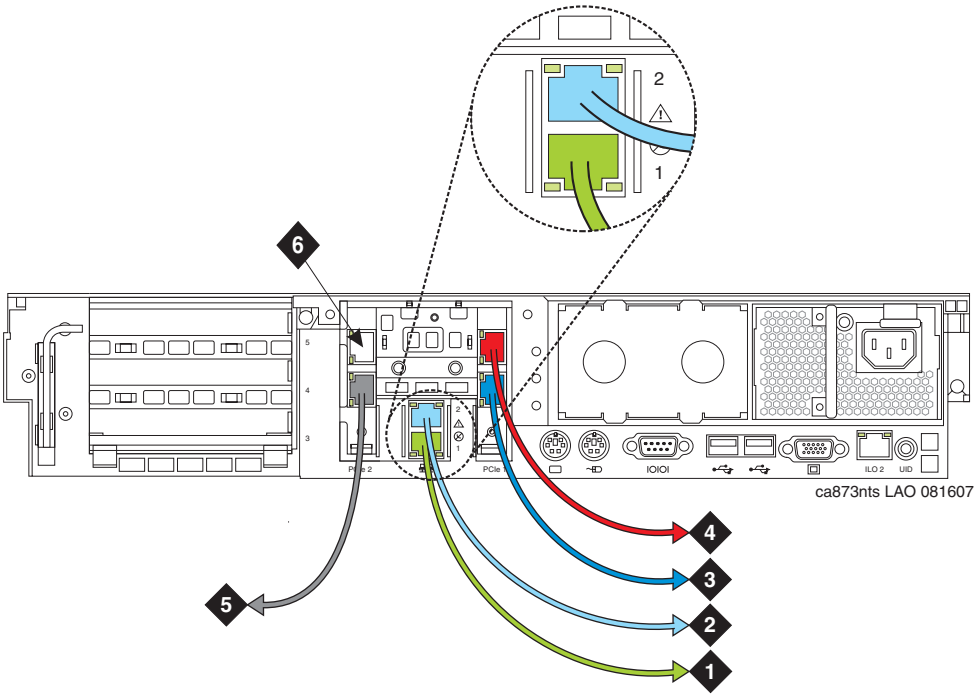


Figure notes:

1. **Duplication cable (Crossover) — Eth0**
2. **Services port — Eth1**
3. **CNA (also LAN for nondedicated control network) — Eth2**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**

2. Connect the modem to one of the USB ports.
3. Connect the power cord to the rear of the server.
4. To turn on the server, push the yellow power button on the front of the S8730.

   Note:

   Do not connect the USB flash drive at this time.

Accessing the first S8730 Server

To access the server:

1. Clear the ARP cache from the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.

2. Connect the laptop to the Services port (labeled 2) on the back of the server with a cross-connect CAT5 cable.

   For S8730 Server connections, see Figure 37.

Figure 37: Services laptop computer connected directly to the S8730 Server

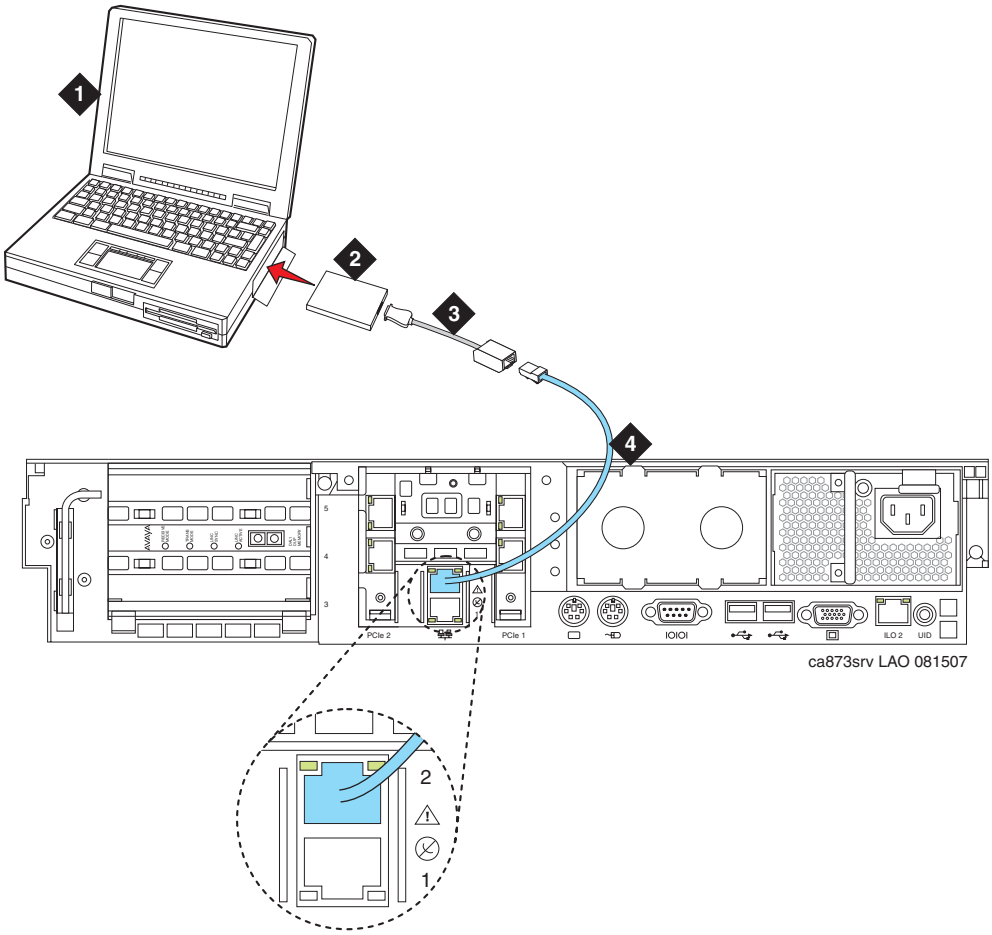


Figure notes:

1. **Services laptop**
2. **Network interface card (NIC) (not necessary if the laptop has the NIC installed)**
3. **NIC adapter cable (if necessary) (not necessary if the laptop has the NIC installed)**
4. **CAT5 crossconnect cable**

3. On your laptop computer, click **Start** > **Run** to open the **Run** dialog box,

4. Type **`ping -t 192.11.13.6`**. Press **Enter** to check connectivity between the Services laptop and the server.

Wait at least 3 minutes after turning on the server before starting a Telnet session to access the information on the CD.

Setting up a Telnet session

To set up a Telnet session:

Note:
You might need a Telnet session to perform some of the tasks in this migration.

Note:
Use a telnet session to access the information on the CD-ROM.

You can set the Microsoft Telnet application to send a carriage return (CR) and a line feed (LF) whenever you press Enter. The installation program sees this as two key presses. If you are running Windows 2000 or Windows XP, you must correct this before you copy the Remaster Program to the hard disk.

1. Click **Start** > **Run** to open the **Run** dialog box.
2. Type **`telnet`**. Press **Enter** to open a Microsoft Telnet session.
3. Type **`display`**. Press **Enter** to see the current settings.
4. Perform one of the following actions:

   If the system displays the message **Sending only CR**, close the dialog box.

   If the system displays the message **Sending both CR & LF**, continue with step 5.
5. Type **`unset crlf`**. Press **Enter**.
6. Type **`display`**. Press **Enter** to verify that the settings changed. The system displays the message **Sending only CR**.
7. Close the dialog box.

Installing Communication Manager

Use a telnet session to install Communication Manager.

To install Communication Manager:

1. From the laptop Start menu, click **Start** > **Run**.

2. In the **Run** dialog box, type **`telnet 192.11.13.6`** and press **Enter** to view the first screen.

Note:

To navigate on these screens, use the arrow keys to move to an option, and then press the spacebar to select the option. Press **Enter** to submit the screen.

3. Select **Install**, ensure that OK is highlighted and press **Enter**.

4. On the **Select Release Version** window, ensure that the Build line and OK are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

   Once the drive is configured correctly, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

   These processes can take up to 20 minutes. When the server is ready to reboot, the CD-ROM drive drawer opens. Remove the CD-ROM from the drive at this time.

   The reboot can take up to 3 minutes. The Telnet session ends automatically.

Insert the USB flash drive in the USB port

Insert the USB flash drive containing the backup in one of the USB ports. It does not matter which USB port you use.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.

2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Checking the software version

Use the Communication Manager System Management Interface (SMI) to check the software release:

- Under **Server** click **Software Version**

  Verify the release running on the server.

Verifying date and time

Use the Communication Manager System Management Interface (SMI) to change the date and time:

1. Under **Server**, click **Server Date/Time**.
2. Change the date, time, and time zone as needed.
3. To make changes, click **Submit**.

Copying files to the server (if any)

From the services laptop, copy the following to the S8730 Server:

- The software update or service pack
- RFA license file
- Avaya authentication file
- Firmware updates for programmable circuit packs and media modules might also be required. These files might be on the software CD.

  Note:

  Do not copy the Linux migration upgrade set with this method.

To copy files to the server:

1. On the System Management Interface (SMI), under **Miscellaneous**, select **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the **Choose File** window on your computer.
4. Find the files that you need to copy to the server.
5. Click **Download** to copy the file(s) to the server.

   The system automatically copies the files to the default location on the server.

Installing security and service pack updates, if any

Use this procedure to unpack and active the files that you copied in the previous step.

1. Under **Server Upgrades**, select **Manage Updates**.
2. If an update file you want to activate shows **packed** in the **Status** column:
   a. Select **update ID**
   b. Click **Unpack**
3. Wait until the system displays the message **Unpacked Successfully..** and then click **Continue**.

   The system displays the **Manage Updates** screen.
4. If the update ID you want to activate shows **unpacked** in the **Status** column:
   a. Select the **update ID**
   b. Click **Activate**

      The screen shows the status of activating the update. If a reboot or restart of Communication Manager is required, the system automatically reboots or restarts Communication Manager.
5. Click **Yes**.

   Wait until the system displays the **Continue** button.
6. Click **Continue**.

   The system displays the status of the update.

Stopping Communication Manager on the first S8730 Server

To stop Communication Manager:

- Type **`stop -acf`**. Press **Enter** to stop Communication Manager.

The system provides a continuous display of the stop operation.

Configuring the first S8730 Server

The information contained in the configuration files that you printed or saved to your PC is used when you configure the S8730 Server.

The S8730 Server can be configured with one of the following methods:

- Manually enter the configuration data using the Communication Manager System Management Interface (SMI), click Installation > Configure Server.
- Manually enter the data into EPW and use the Avaya Installation Wizard to import the configuration information to the server.
- Manually enter the data while using the Avaya Installation Wizard. If you use the Avaya Installation Wizard to configure the server, some additional configuration must be entered using the Communication Manager System Management Interface (SMI), click **Installation > Configure Server**.

Configuring the server using AIW

Use the Avaya Installation Wizard (AIW) to:

- Configure the server
- Install the new license file and the software updates

Use one of the following methods to enter the date from the filled-out *Electronic Preinstallation Worksheet* (EPW):

- Import the data from the EPW.
- Type the information manually.

To access the Installation Wizard:

1. Open the browser with the Home page.
2. Click **Avaya Installation Wizard**.

3. Follow the prompts to configure this server as "active." For more information, click Help on any page.

   Configure this server as "active."

Configuring the first server using the Configure Server web pages

If you do not want to use the AIW, you can manually enter the configuration information using the Communication Manager System Management Interface (SMI):

1. Under Server Configuration, click **Configure Server**.

   The system displays the **Review Notices** screen.
2. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. The wizard steps you through each configuration screen. Enter the configuration information that you obtained from the S8500-Series Server in the appropriate screens and update the system.

   If this server is an LSP or an ESS server behind a main server that is configured as XL:

   a. On the **Configure ESS/LSP** page verify that the:
      - Appropriate radio button is turned on for the server type.
      - IP addresses are correct for registration and file synchronization.

Verifying connectivity from the first S8730 Server to the network server

To verify that the Ethernet port is working, ping from the server to the network server where the backup files are stored.

Note:

You might need to restart your browser before doing the next steps.

1. Under Diagnostics, click **Ping**.
2. Select **Host Name Or IP address** and type the IP address of the server where the system files are stored
3. Click **Execute Ping**.

   If you can successfully ping the server, you can proceed to restore the backed up sets of files.

Restoring the translations

To restore the translations to the active server:

1. Connect the compact flash reader cord to either USB port on the back of the server.
2. Insert the compact flash card with the translations into the bottom slot of the drive.

   This card is the card that you use in Backing up the translation files to the compact flash on page 480.
3. Under **Data Backup/Restore**, click **View/Restore Data**.
4. Select **Local PC Card**.

   Note:

   If the laptop is connected to the standby server, SSH across the duplication link to the active server. The SSH address for server 1 is 192.11.13.13. The SSH address for server 2 is 192.11.13.14. Ensure that you copy the translations to the *active* server.

Verifying the first S8730 Server configuration

To verify the first S8730 Server configuration:

1. Under **Server Configuration**, click **Configure Server** to start the configure server process.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure all services using the wizard**. Click **Continue**.
4. On the **Set Identities** page, under the Select Server Duplication area, select either:
   - **This is a duplicated server using duplication hardware**
   - **This is a duplicated server using software-based duplication**
   - **This is a duplicated server using encrypted software-based duplication**

   Note:

   The physical connections to the Ethernet ports are different for hardware duplication and software duplication.
5. Click **Continue**.
6. On the **Configure Interface** page, set the speed for Ethernet ports to **AUTO SENSE**.

   Note:

   You must click through all the screens whether there are changes or not.
7. On the **Configure ESS** window:

- If the server is a primary control main, click **This is NOT an enterprise survivable server**
- If the server is an ESS server, click **This is an enterprise survivable server (ESS)**

8. Click **Continue**.
9. After checking all the pages, click **Continue** on the **Update System** screen. The Update System screen shows each configuration task as the task completes. When done, the screen shows the line **All configuration information was entered**.
10. Click **Close Window** to close the Configure Server wizard.

Confirming the product ID on the first S8730 Server

To confirm the Product ID:

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**. Press **Enter**.

Rebooting the first S8730 Server

Rebooting the S8730 Server is necessary to initialize server settings that are restored but not yet activated.

To reboot, on the Communication Manager System Management Interface (SMI):

1. Under **Server**, click **Shutdown Server**.
2. Select:
   - **Delayed Shutdown**
   - **Restart Server after Shutdown**
3. Click **Shutdown**.

Accessing the first S8730 Server

To access the first S8730 Server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.
2. Open a browser and connect to the server.
3. Log in.

4. Suppress all alarms.

Initializing and busyout on the first S8730 Server

To initialize Communication Manager:

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.

   Note:

   For the following step, the logons are release-dependent.

2. Log in as **craft** or **dadmin**.
3. Type **stop -acf**. Press **Enter** to stop Communication Manager.

   Communication Manager might already be stopped in Stopping Communication Manager on the first S8730 Server on page 493.

4. Type **server -b**. Press **Enter** to queue a busy out of the Communication Manager software.

   The system responds with the following message

   ACP not yet running, queueing busyout request.

5. Type **start -ac**. Press **Enter** to start Communication Manager and load the translations.

Configuring the ESS and the LSP for compatibility with S8730

If the main servers are S8730 or S8720 Servers configured as XL, the ESS servers and the LSPs must also be configured as XL.

The S8300B LSPs, the S8700 ESS servers, and the S8710 ESS servers can not be configured as XL and are therefore not compatible with main servers that are configured as XL.

Note:

You do not have to perform this procedure on an S8730 ESS server as it is already configured as XL.

Use the following steps to configure the ESS server or the LSP:

1. Type **stop -acfn** on the command line interface and press **Enter** to stop Communication Manager call processing.
2. On the ESS server's or the LSP's System Management Interface (SMI), under **Installation >** click **Configure Server**.

   The system displays the **Review Notices** screen.

3. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.

CAUTION:

For the next step, if you select and save as **Extra Large** you cannot revert to **Standard**. If you try to go back to **Standard**, server translation corruption occurs.

4. Select **Configure individual services** and click **Continue**.
5. In the left column, click **Configure ESS** if this is an ESS server or click **Configure LSP** if this is an LSP.
6. Under Configure Memory, select **Extra Large** and click **Change**.
7. Click **Close Window**.
8. Type `start -ac` on the command line interface and press **Enter** to restart Communication Manager call processing.
9. Type `swversion` on the command line interface and press **Enter**.

   In the **Memory Config** field, verify that the setting is **Extra Large**.

Performing an integrity check on the first S8730 Server

Use the System Management Interface (formerly known as Maintenance Web Interface) to perform an integrity check on the first S8730 Server:

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, click **All IPSIs, UPS(s), Other server(s), Ethernet switches** and click **Execute Ping**.

   If this ping fails, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300432).
3. Click **Server > Status Summary**.
4. Verify the following:

   Mode: BUSY OUT

   Server Hardware: okay

   Processes: okay
5. Select **Server > Process Status**.
6. Under Frequency, click **Display Once**.
7. Click **View**.
8. Verify all operations are **UP STANDBY**.
9. Telnet to a device outside the server and ping back to the S8730 server.
10. Under IPSI Firmware Upgrades, click **IPSI Version**.

11. Under Query Type, click **Query All** and click **View** to verify connectivity to all IPSIs.

Making the first S8730 Server active

This section describes the procedures you must perform to make the first S8730 Server active.

Accessing the first S8730 Server

To access the first S8730 Server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.
2. Open a browser and connect to the server.
3. Log in.
4. Suppress all alarms.

Releasing the first S8730 Server

To release the first S8730 Server:

Note:
Be prepared for the Access Security Gateway (ASG) challenge and response.

1. On the System Management Interface (SMI), click **Server** > **Release Server**.
2. Click **Release**.

Verifying the first S8730 Server is active

To verify the first S8730 Server is active:

1. On the System Management Interface (SMI), click **Administration > Server (Maintenance) > Server** > **Status Summary**.
2. Verify the **Mode** field is **Active**.
3. To verify the process status, click **Server** > **Process Status**.
4. Under Frequency, click **Display Once**.
5. Click **View**.
6. Verify all operations are **UP**.

Creating a super-user login

Note:

A craft level login can create the super-user login in Release 4.0 or later.

Make sure you have a login name and password that the customer would like for the superuser login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Use the **Communication Manager System Management Interface (SMI)** to create a super-user login.

To create a login:

Note:

Make sure the customer can change this login, its password, or its permissions later.

1. In the **Communication Manager System Management Interface (SMI)**, under **Security**, select **Administrator Accounts**.
2. Select **Add Login**.
3. Select **Privileged Administrator** and click **Submit**.

   The **Administrator Accounts -- Add Login: Privileged Administrator** screen appears.
4. In the **Login name** field: Type a login name for the account.
5. In the **Primary group** field: susers appears.
6. In the **Additional groups (profile)** field: prof18 appears (*prof18* is the code for the customer superuser).
7. **In the Linux shell** field: /bin/bash appears
8. In the **Home directory field**: /var/home/login name appears (login name is the name you choose in step 4.
9. Skip the **Lock this account** and **Date on which account is disabled-blank to ignore** fields.
10. In the **Select type of authentication section**: Choose **Password**.

    Note:

    Do not lock the account or set the password to be disabled.
11. In the **Enter key or password field** and the **Re-enter key or password** field: Enter the password.
12. In the **Force password/key change on next login section**: Do not check the box.
13. Click **Submit**.

    The system tells the login is added successfully.

Installing the license and authentication files

To install the RFA license file and the Avaya authentication file on the active S8730 Server:

1. To install the license file, click **Security** > **License File**.
2. Select either:
   - **Install the license file I previously downloaded** if you have already downloaded the file to this server, or
   - **Install the license file specified below** and then browse the connected computer for the license file.
3. Click **Submit**.
4. To install the authentication file, click **Security** > **Authentication File**.
5. Select either:
   - **Install the license file I previously downloaded** if you have already downloaded the file to this server, or
   - **Install the license file specified below** and then browse the connected computer for the license file.
6. Click **Install**.

   Note:

   The system responds with a successful message. If you get a filesync failed message, ignore it.

Stopping and starting the ESS servers

If this an ESS server, you must stop the Communication Manager process and then restart it after installing the license file. Doing this ensures that the new RFA license takes full effect.

1. On a server command line interface, run the **`stop -caf`** command.

   The system provides a continuos display of the stop operation. This allows you to determine when the process completes.
2. On a server command line interface, run the **`start -ca`** command.

   The system provides a continuous display of the start operation. This allows you to determine when the process completes.

Verifying server operation

Verify that the following operations work on the new server:

- A station to station call
- An outside call
- An incoming call
- A call that follows a coverage path to voice mail.
  a. Verify that the light on the station comes on after you leave a voice mail message.
  b. Call into voice mail and retrieve the mail message.
  c. Verify that the light goes out after retrieving the voice mail.

On the second S8730

Verifying the DAL2 card

A DAL2 card is required for each S8730 Server using hardware duplication. If you are not using hardware duplication, go to Installing the second S8730 Server in the rack on page 502.

If you are using hardware duplication, verify the type of DAL board that is installed in the server by looking at the label printed on the DAL board. If the S8730 already has a DAL2, go to Installing the second S8730 Server in the rack on page 502. If you need to install a DAL2, use the instructions outlined in Appendix B: DAL: Removing or Installing on page 345.

Installing the second S8730 Server in the rack

To install the second S8730 Server in the rack:

1. Install the slide on the server.
2. Install the rails in the rack.
3. Install the S8730 Server in the rack. For more information, see *Quick Start for Hardware Installation: S8700 Series Servers* (03-300145).

Inserting the Communication Manager software distribution CD

To insert the Communication Manager software distribution CD in the S8720 Server:

Note:

You must place the CD in the CD/DVD drive before turning on the server.

1. Use a paperclip to open the CD-ROM drive on the server.
2. Insert the Communication Manager software distribution CD in the CD/DVD drive and close the drive door.

Connecting the cables to the second S8730 Servers

To connect the cables to the second server:

Note:

Do not connect the fiber duplication connection cable or the duplication interface IP cable at this time to either S8730 Server

1. The network connections depend on the type of memory duplication and the type of control network being used. Connect the network cables as described in the following table.

Control Network	Software Memory Duplication	Hardware Memory Duplication
Dedicated	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled 1) • CNB (if used) to Eth3 (right top)	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled **1**) • CNB (if used) to Eth3 (right top)
Nondedicated	• LAN/CNA to Eth2 (right bottom) • CNB (if used) to Eth3 (right top)	• LAN/CNA to Eth0 (middle bottom labeled **1**) CNB (if used) to Eth3 (right top)

Figure 38: Duplication and control network cables for hardware duplication

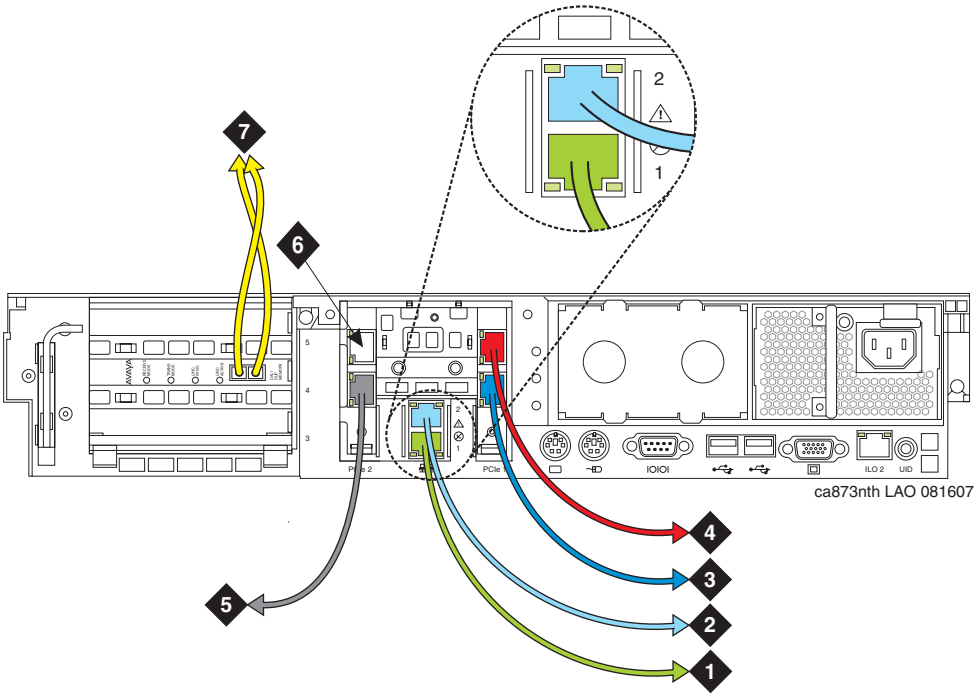


Figure notes:

1. **CNA (also LAN for nondedicated control network)— Eth0**
2. **Services port — Eth1**
3. **Duplication cable (crossover)— Eth2**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**
7. **Fiber duplication cable**

Figure 39: Duplication and control network cables for software duplication

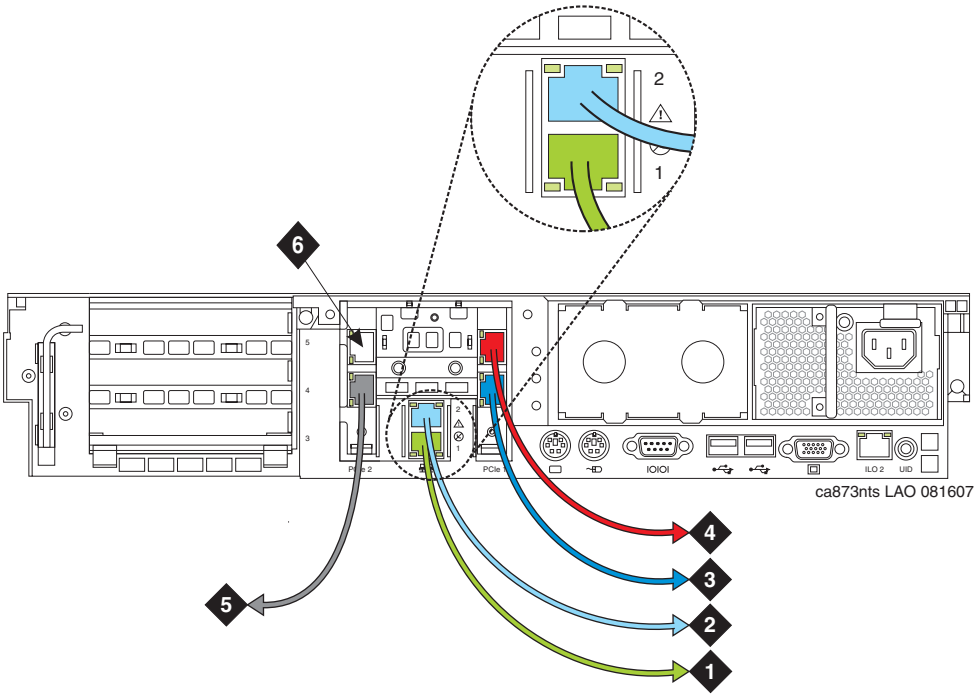


Figure notes:

1. **CNA (also LAN for nondedicated control network) — Eth0**
2. **Services port — Eth1**
3. **Duplication cable (Crossover— Eth2)**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**

2. Connect the modem to one of the USB ports.
3. Connect the power cord to the rear of the server.
4. To turn on the server, push the yellow button.

Note:

Do not connect the USB flash drive at this time.

Accessing the server

To access the server:

1. Clear the ARP cache from the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. On your laptop computer, click **Start** > **Run** to open the **Run** dialog box,
4. Type **`ping -t 192.11.13.6`**. Press **Enter** to check connectivity between the Services laptop and the server.
5. Wait at least 3 minutes after turning on the server before starting a Telnet session to access the information on the CD.

Installing Communication Manager

Use a telnet session to install Communication Manager.

To install Communication Manager:

1. From the laptop Start menu, click **Start** > **Run**.
2. In the **Run** dialog box, type **`telnet 192.11.13.6`**. Press **Enter** to view the first screen.

Note:

To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

3. Select **Install**, ensure that OK is highlighted and press **Enter**.
4. On the **Select Release Version** window, ensure that the Build line and <OK> are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

   Once the drive is properly configured, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

   These processes can take up to 20 minutes. When the server is ready to reboot, the CD-ROM drive drawer opens. You must remove the CD from the drive at this time.

   The reboot can take up to 3 minutes. The telnet session drops automatically.

Insert the USB flash drive in the USB port

Insert the USB flash drive containing the backup in one of the USB ports. It does not matter which USB port you use.

Accessing the second S8730 Server

To access the second S8730 Server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.
2. Open a browser and connect to the server.
3. Log in.
4. Suppress all alarms.

Checking the software version

Use the Communication Manager System Management Interface (SMI) to check the software release:

- Under **Server** click **Software Version**

  Verify the release running on the server.

Verifying date and time

Use the Communication Manager System Management Interface (SMI) to change the date and time:

1. Under **Server**, click **Server Date/Time**.
2. Change the date, time, and time zone as needed.
3. To make changes, click **Submit**.

Copying files to the second S8730 Server (if any)

If a software update (service pack) is required, you must copy the update file from the services laptop to the server.

Note:

You do not need to download an RFA license file to this server. The license will shadow over from the other server.

Firmware updates for programmable circuit packs and media modules might also be required. These files might be on the software CD.

Note:

Do not copy the Linux migration upgrade set with this method.

To copy files to the server:

1. On the System Management Interface (SMI), under **Miscellaneous**, select **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the **Choose File** window on your computer.
4. Find the files that you need to copy to the server.
5. Click **Download** to copy the file(s) to the server.

   The system automatically copies the files to the default location on the server.

Installing security and service pack updates, if any

Use this procedure to unpack and active the files that you copied in the previous step.

1. Under **Server Upgrades**, select **Manage Updates**.
2. If an update file you want to activate shows **packed** in the **Status** column:
   a. Select **update ID**
   b. Click **Unpack**
3. Wait until the system displays the message **Unpacked Successfully..** and then click **Continue**.

   The system displays the **Manage Updates** screen.
4. If the update ID you want to activate shows **unpacked** in the **Status** column:
   a. Select the **update ID**
   b. Click **Activate**

      The screen shows the status of activating the update. If a reboot or restart of Communication Manager is required, the system automatically reboots or restarts Communication Manager.
5. Click **Yes**.

   Wait until the system displays the **Continue** button.
6. Click **Continue**.

   The system displays the status of the update.

Stopping Communication Manager on the second S8730 Server

To stop Communication Manager:

- Type **`stop -acf`**. Press **Enter** to stop Communication Manager.

The system provides a continuous display of the stop operation.

Configuring the second S8730 Server

The information contained in the configuration files that you printed or saved to your PC is used when you configure the S8730 Server.

The S8730 Server can be configured with one of the following methods:

- Manually enter the configuration data using the Communication Manager System Management Interface (SMI), click Installation > Configure Server.
- Manually enter the data into EPW and use the Avaya Installation Wizard to import the configuration information to the server.
- Manually enter the data while using the Avaya Installation Wizard. If you use the Avaya Installation Wizard to configure the server, some additional configuration must be entered using the Communication Manager System Management Interface (SMI), click Installation > Configure Server.

Configuring the server using AIW

Use the Avaya Installation Wizard (AIW) to:

- Configure the server
- Install the new license file and the software updates

Use one of the following methods to enter the date from the filled-out *Electronic Preinstallation Worksheet* (EPW):

- Import the data from the EPW.
- Type the information manually.

To access the Installation Wizard:

1. Open the browser with the Home page.
2. Click **Avaya Installation Wizard**.

3. Follow the prompts to configure this server as "active." For more information, click Help on any page.

   Configure this server as "active."

Configuring the first server using the Configure Server web pages

If you do not want to use the AIW, you can manually enter the configuration information using the Communication Manager System Management Interface (SMI):

1. Under Server Configuration, click **Configure Server**.

   The system displays the **Review Notices** screen.
2. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. The wizard steps you through each configuration screen. Enter the configuration information that you obtained from the S8500 Server in the appropriate screens and update the system.

   If this server is an LSP or an ESS server behind a main server that is configured as XL:

   a. On the **Configure ESS/LSP** page verify that the:
      - Appropriate radio button is turned on for the server type.
      - IP addresses are correct for registration and file synchronization.

Verifying connectivity from the second S8730 Server to the network server

To verify that the Ethernet port is working, ping from the server to the network server where the backup files are stored.

Note:

You might need to restart your browser before doing the next steps.

1. Under Diagnostics, click **Ping**.
2. Select **Host Name Or IP address** and type the IP address of the server where the system files are stored
3. Click **Execute Ping**.

   If you can successfully ping the server, you can proceed to restore the backed up sets of files.

Restoring the translations

To restore the translations to the active server:

1. Connect the compact flash reader cord to either USB port on the back of the server.
2. Insert the compact flash card with the translations into the bottom slot of the drive.

   This card is the card that you use in Backing up the translation files to the compact flash on page 480.
3. Under **Data Backup/Restore**, click **View/Restore Data**.
4. Select **Local PC Card**.

   Note:

   If the laptop is connected to the standby server, SSH across the duplication link to the active server. The SSH address for server 1 is 192.11.13.13. The SSH address for server 2 is 192.11.13.14. Ensure that you copy the translations to the *active* server.
5. Click **View**.

   Note:

   For the next step, the correction translation file is the most recent file.
6. Select the correct translation file and both Force options.
7. Click **Restore**.
8. Click **Restore History** and select the desired file that you want to restore.
9. Click **Status** to view the Restore status.

   When the restoration is complete, the system displays the following message:

   Backup: 0: Restore of <filepath/filename> is completed successfully.

Verifying the second S8730 Server configuration

Use this step to verify the configuration information and to make any necessary changes:

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure all services using the wizard**. Click **Continue**.
4. On the **Set Identities** page, under the Select Server Duplication area, select either:
   - **This is a duplicated server using duplication hardware**

- **This is a duplicated server using software-based duplication**
- **This is a duplicated server using encrypted software-based duplication**

Note:

The physical connections to the Ethernet ports are different for hardware duplication and software duplication.

5. Click **Continue**.
6. On the **Configure Interface** page, set the speed for all Ethernet ports to **AUTOSENSE**.

   Note:

   You must click through all the screens whether there are changes or not.

7. On the **Configure ESS** window:
   - If the server is a primary control main, click **This is NOT an enterprise survivable server**
   - If the server is an ESS server, click **This is an enterprise survivable server (ESS)**
8. Click **Continue**.
9. When you complete all the new fields, click **Continue** on the **Update System** screen. The Update System screen shows each configuration task as the task completes. When done, the screen shows the line **All configuration information was entered**.
10. Click **Close Window**.

Confirming the product ID on the second S8730 Server

To confirm the Product ID:

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**.
4. Press **Enter**.

Rebooting the second S8730 Server

Reboot is necessary to initialize server settings that are restored but not yet activated.

To reboot the second S8730 Server:

1. On the System Management Interface (SMI), under **Administration > Server (Maintenance) > Server,** click **Shutdown Server**.
2. Make the following selections:

- Select **Delay Shutdown**
- Select **Restart Server after Shutdown**

3. Click **Shutdown**.

   Wait approximately three minutes.

Accessing the second S8730 Server

To access the second S8720 Server:

1. Open a browser and connect to the server.
2. Log in. For more information, see Accessing the server command line interface with ssh protocol on page 228.
3. Suppress all alarms.

Performing an integrity check on the second S8730 Server

To perform an integrity check on the second S8730 Server:

1. On the System Management Interface (SMI), under Diagnostics, click **Ping**.
2. Under Endpoints to Ping, click **All IPSIs, UPS(s), Other server(s), Ethernet switches** and click **Execute Ping**.

   If this ping fails, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300432).
3. Click **Server** > **Status Summary**.
4. Verify the following:

   Mode: BUSY OUT

   Server Hardware: okay

   Processes: okay
5. Select **Server > Process Status**.
6. Under Frequency, click **Display Once**.
7. Click **View**.
8. Verify all operations are **UP STANDBY**.
9. Telnet to a device outside the server and ping back to the S8730 Server.
10. Under IPSI Firmware Upgrades, click **IPSI Version** (main server only).

11. Under Query Type, click **Query All** and click **View** to verify connectivity to all IPSIs (main server only).

Connecting the duplication cables

To connect the duplication cables:

- Connect the duplication cables as described in the following table.

Control Network	Software Memory Duplication See Figure 41	Hardware Memory Duplication (see Figure 40)
Dedicated	• Duplication to Eth0 (on server, labeled **1**)	• Duplication to Eth2 (1st from left on quad NIC) • Fiber to DAL2 card

Figure 40: S8730 duplication and control network cables for hardware duplication

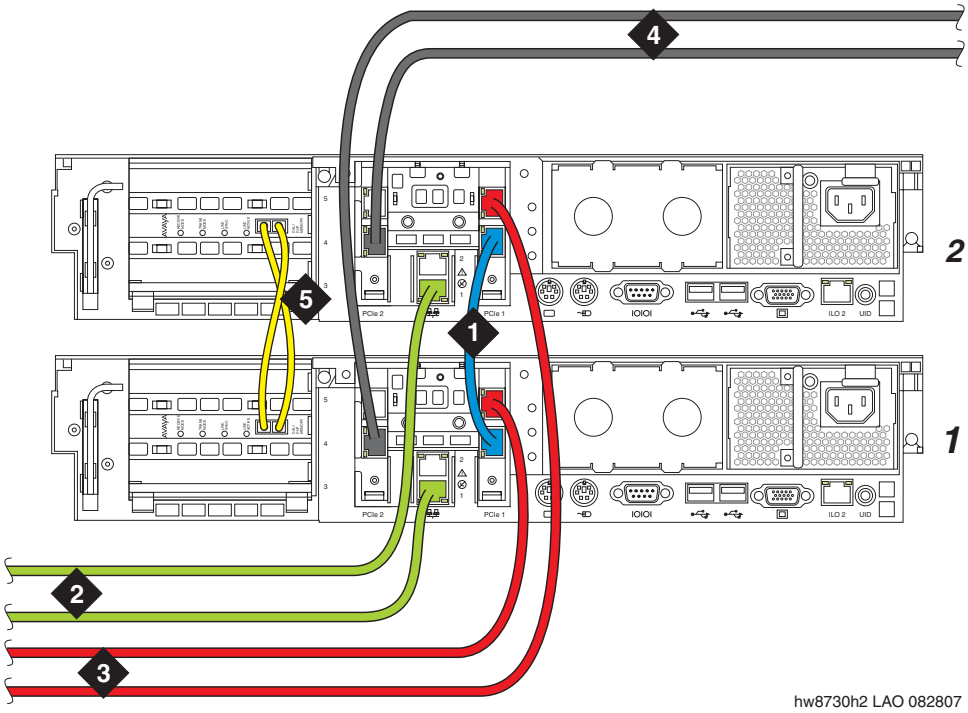


Figure notes:

1. **Server duplication link - duplication crossover cable — Eth2**
2. **CNA (also LAN for nondedicated control network) — Eth0**
3. **CNB (if used) — Eth3**

4. **LAN (if dedicated control network) — Eth4**
5. **Fiber duplication cable**

Figure 41: S8730 duplication and control network cables for software duplication

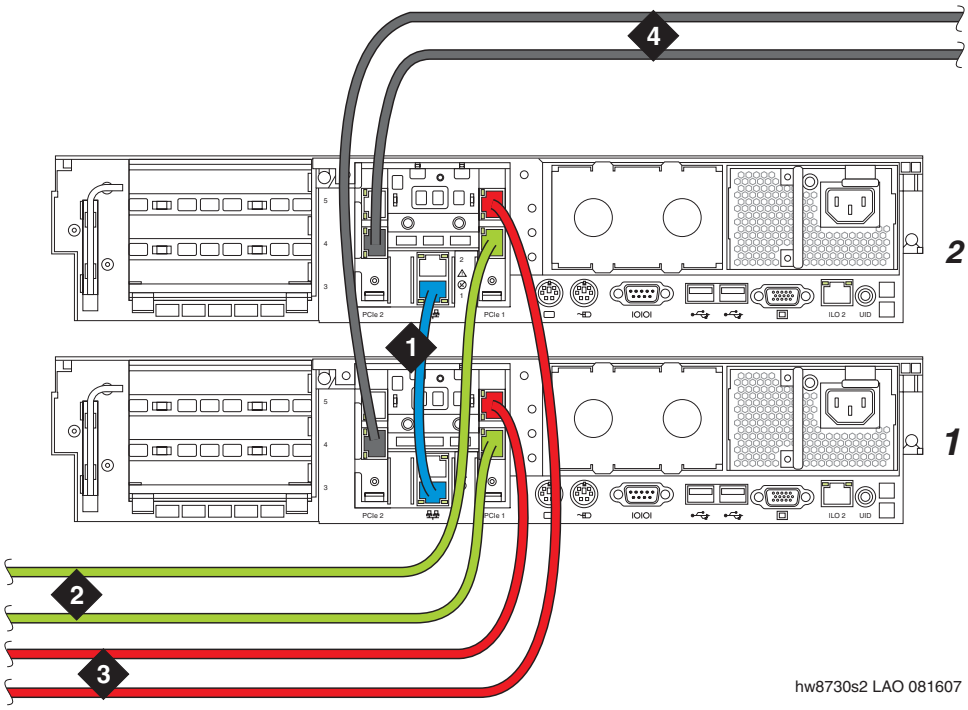


Figure notes:

1. **Duplication cable (Crossover) — Eth0**
2. **CNA (also LAN for non-dedicated control network) — Eth2**
3. **CNB (if used) — Eth3**
4. **LAN (if dedicated control network) — Eth4**

Releasing the second S8730 Server

To release the second S8730 Server:

1. On the System Management Interface (SMI), click **Server** > **Release Server**.
2. Click **Release**.

Verifying the second S8730 Server is in standby state

To verify the second S8730 Server is in a standby state:

1. On the System Management Interface (SMI), click **Server** > **Status Summary**.
2. Verify the **Mode** field is **Standby**.
3. Check the following:
   - Standby Busied is **no**
   - Standby Refreshed is **yes**
   - Standby Shadowing is **on**
4. To verify the process status, click **Server** > **Process Status**.
5. Under Frequency, click **Display Once**.
6. Click **View**.
7. Verify all operations are **UP Standby**.

Releasing alarm suppression (optional)

If you complete the migration well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait.

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **craft** or **dadmin**.
3. Type **`almsuppress -s n`**. Press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the second S8730 Server

Disconnect the Services laptop from the second S8730 Server.

On the active (first) S8730 Server

This section describes the procedures you must perform on the active (first) S8730 Server.

Accessing the active server

To access the active server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. Log in.

Resolving alarms

To resolve alarms:

1. Under Alarms and Notification, click **Current Alarms**.
2. Select the server alarms to be cleared. Click **Clear**.
3. Resolve new alarms since the migration with SAT commands. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*
   - *Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers*

Enabling scheduled maintenance

To schedule daily maintenance:

- Reset the settings that were recorded in Disabling scheduled maintenance on page 476.

Saving translations

To save translations:

- Type **`save translation all`**. Press **Enter**.

  If this operation is unsuccessful, follow the normal escalation procedures before continuing.

Backing up files on the active S8730 Server

To back up files on the active server:

1. Under Data Backup/Restore, click **Backup Now**.
2. Under Data Sets, click **Full Backup**.
3. Under Backup Method, select the backup method.
4. Click **Start Backup** to start the back up process.

Releasing alarm suppression (optional)

If you complete the migration well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait.

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **craft** or **dadmin**.
3. Type **`almsuppress -n`**. Press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the active S8730 Server

Disconnect the Services laptop from the active server.

On the standby S8730 Server

This section describes the procedures you must perform on the standby S8730 Server.

Accessing the standby server

To access the standby server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. Log in.

Resolving alarms

To resolve alarms:

1. Under Alarms and Notification, click **Current Alarms**.
2. Select the server alarms to be cleared. Click **Clear**.

Backing up files on the standby S8730 Server

To back up files on the standby server:

1. Under Data Backup/Restore, click **Backup Now**.
2. Under Data Sets, click **Full Backup**.
3. Under Backup Method, select the backup method.
4. Click **Start Backup** to start the back up process.

Releasing alarm suppression (optional)

If you complete the migration well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait.

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **craft** or **dadmin**.
3. Type **`almsuppress -n`**. Press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the standby server

Disconnect the Services laptop from the standby server.

Completing the migration

This section describes the procedures you must perform to complete the migration.

Registering the system

Follow the existing process and procedures to register the S8730 Server.

Removing customer files from the Services laptop

Remove the customer Linux migration *upgrade* set from the services laptop.

Interchanging servers (optional)

This section describes the procedures you must perform to interchange the servers.

Accessing the standby server

To access the standby server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 458 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. Log in.

Interchanging servers (optional)

To interchange the servers to check capability of the standby server to become the active server:

1. Under Server, click **Interchange Servers**.
2. Verify the settings in the following fields:
   - **Standby Busied**: no
   - **Standby Refreshed**: yes

- **Standby Shadowing**: on
- **Duplication Link**: up

3. Click **Interchange**.

   The system displays a confirmation message that the interchange has taken place.

   This server is now the active server.

Performing an integrity check on the active S8730 Server

To perform an integrity check on the active S8730 Server:

1. On the System Management Interface (SMI), under Diagnostics, click **Server** > **Status Summary**.
2. Verify the following:

   Mode: Active

   Server Hardware: okay

   Processes: okay
3. Select **Server** > **Process Status**.
4. Under Frequency, click **Display Once**.
5. Click **View**.
6. Verify all operations are **Up STANDBY**.

Migrating from an S8700, S8710 or S8720 to an S8730 Server

Use these procedures to migrate an existing S8700, S8710, or S8720 Server running Communication Manager Release 2.x, 3.x, or 4.x to an S8730 Server on Communication Manager Release 5.x. In this migration, you reuse the system and translation files from the S8700, S8710, or S8720 Servers.

If the servers are on Release 1.x, you must upgrade them to Release 1.3.2 before performing the migration to the S8730 Server. Instructions on how to upgrade to Release 1.3.2 can be found at on a older version of this book located at http://support.avaya.com.

Important:

Do not perform a standard backup of translations on the S8700 and try to restore them on the S8730. Restoring the translations on the S8730 will fail. Use the instructions found in Backing up the configuration data and translations using Linux Migration Backup to a server on the network on page 547.

You must install the Avaya S8730 Servers either:

- in a 19-inch, 4-post rack as described in the *Quick Start for Hardware Installation: Avaya S8700 Series Server* (555-245-703).
- A pullout shelf attached to the existing 2-post rack.

Enterprise Survivable Servers (ESS)

The migration procedures in this chapter can be used for both the main server and an ESS server. If a procedure is used for only one server type it will be noted. If only the main server is migrating to an S8730 Server, the ESS servers must be:

- Upgraded to 5.x *prior* to the migration of the main server: An ESS server must be running the same or a later release than that of the main server.
- An S8500-Series Server configured as XL, or an S8720 configured XL, or an S8730.

Note:

All ESS servers and LSPs must be configured as XL to be compatible with an S8730 main server. The S8700 ESS servers and the S8710 ESS servers can not be configured as XL and therefore are not compatible with an S8730 main server or an S8720 main server configured as XL. The S8300B LSP can not be configured as XL and therefore is not compatible with an S8730 main server or an S8720 main server configured as XL.

Important:

The server type that can be used as an LSP or an ESS server changes depending on the main server type. For information on compatibility, see Table 3: LSP or ESS server types for Release 5.2.

Important:

If the S8700-Series ESS, S8700, S8710, S8720, running Communication Manager Release 5.1.x or prior is migrated to S8730 running Communication Manager 5.2 or later while the main server is still running Release 5.1.x or prior, special consideration must be given to the administration for the duplex ESS. This migration module accounts for the interim period when an S8730 ESS is running Communication Manager 5.2 or later while the main server is running Communication Manager 5.1.x or prior.

Local Survivable Servers (LSP)

If the main servers are migrating to an S8730 Server, the LSPs must be:

- Upgraded to 5.x prior to the migration of the main server. An LSP must be running the same or later release than that of the main server.
- An S8500-Series Server configured as XL or an S8300C configured as XL.

Note:

All ESS servers and LSPs must be configured as XL to be compatible with an S8730 main server. The S8700 ESS servers and the S8710 ESS servers can not be configured as XL and therefore are not compatible with an S8730 main server or an S8720 main server configured as XL. The S8300B LSP can not be configured as XL and therefore is not compatible with an S8730 main server or an S8720 main server configured as XL.

Important:

The server type that can be used as an LSP or an ESS server changes depending on the main server type. For information on compatibility, see Table 3: LSP or ESS server types for Release 5.2.

Checklists

Presite checklists

Before you go on site, perform the following tasks in Table 21:

Table 21: Presite checklist

✓	Task	Description
	Verify that the correct hardware is installed on your Services laptop computer.	Correct hardware includes: • 40 MB of available disk space • A direct Ethernet cable • A serial cable and an adapter • An RS-232 port connector • A Network interface card (NIC) with a 10/100 BaseT Ethernet interface • A 10/100 BaseT Ethernet, category 5, or better, crossconnect cable with an RJ45 connector on each end, MDI to MDI-X • A CD-ROM drive
	Verify that the correct software is installed on your Services laptop computer.	Correct software includes: • Windows 2000 or Windows XP operating system • HyperTerminal or another terminal emulation program • TCP/IP networking software that is bundled with the Windows OS • Internet Explorer 5.0 or later
	Obtain the appropriate logins and passwords for all equipment and software.	For example, obtain logins and passwords for the following components: • Server • Media gateway • auxiliary equipment • Communication Manager These logins and passwords include the logins and the passwords that you might need for the equipment of the customer.
		1 of 3

Table 21: Presite checklist

✓	Task	Description
	Obtain the serial number for the servers, if necessary.	You need a new RFA license and authentication file. You need the serial number from the SIPI or IPSI and the SAP order number to generate a new license file and authentication file.
	Verify that you have the Communication Manager software distribution CD-ROM with the current software and firmware.	Use this CD-ROM to install the software on the server and upgrade the firmware.
	Verify that you have the current preupgrade or premigration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site.
	Verify that you have the current post-upgrade or post-migration service packs, if required, on your Services laptop computer.	Check which service packs you need and download files from the Avaya Support Web site.
	Verify that you have the current firmware.	The following firmware is on the software CD-ROM: • IPSIs • C-LAN • MedPro • VAL circuit packs **Important:** Firmware is upgraded often. To ensure that you have the latest version, go to the Avaya Support Web site. Click **Downloads** and select the product.
	Download the license file and the authentication file to your Services laptop.	A new RFA license and an Avaya authentication file are necessary. Obtain information and download files from the Remote Feature Activation (RFA) Web site.
	Avaya technical support representatives only: Obtain the static craft password.	Call the ASG Conversant number 800-248-1234 or 1-720-444-5557 and follow the prompts to get the password. You need the Product ID, the FL, or IL number of the customer.
		2 of 3

Table 21: Presite checklist

✓	Task	Description
	Run the Automatic Registration Tool (ART) for the INADS IP address, if necessary.	This step is necessary if the configuration of the customer INADS alarming modem has changed or if any changes were made to the system alarming configuration. ART is available only to Avaya associates. BusinessPartners can call 800-295-0099.
	For DEFINITY systems only: Verify that you have the required, customer-provided network information. Obtain a completed *Electronic Preinstallation Worksheet (EPW)*	The EPW is an Excel spreadsheet that provides the information about the network. You need this information to configure the control network components with the Avaya Installation Wizard. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard Web site.
		3 of 3

Additional tasks

Do this task only if you are not performing a full backup and restore to transfer the configuration data from the S8700 or S8710 to the S8720.

✓	Task	Description
	Verify that you have the required, customer-provided network information. Obtain a filled out *Electronic Preinstallation Worksheet (EPW)*	The EPW is an Excel spreadsheet providing the customer's network information needed to use the Avaya Installation Wizard to configure the control network components. Get the EPW from the Avaya project manager, Avaya software technician, or customer network administrator. A blank EPW is available at the Avaya Installation Wizard web site (http://support.avaya.com/avayaiw/).

Presite migration checklist

Before you go on site, perform the following tasks in Table 22:

Table 22: Presite migration checklist

✓	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations were redesigned.	Perform this task only if applicable.
	Verify that all existing circuit packs work with the new system.	Check the Communication Manager Software & Firmware Compatibility Martix at http://rfa.avaya.com.
	Replace any TN799B/C C-LAN circuit packs.	Replace with the TN799DP circuit pack.
	Replace the 259A adapter and the CAT3 cable.	Replace with the cable extender adapter, Comcode 848525887, and CAT5 or better cable.
	Replace TN570 EI circuit packs.	Replace with TN570B vintage 7 or later circuit packs.

Before you go on site for a migration from a system, complete the following additional tasks before starting the migration:

✓	Task	Description
	You might need to move the UPSs and the Ethernet switch(es) from the 2-post rack to the 4-post rack.	Ensure that you have: • A crosspoint screwdriver • Rail kits (700230741) for a 4-post rack for the UPSs • Cage nuts to attach the screws to the rack, if necessary • At least 2 people to lift the equipment

On site migration checklist

When you are on site, complete the following tasks in Table 23 before you start the migration:

Table 23: On site migration checklist

✓	Task	Description
	Verify that the EIA 310D 19-inch (48-cm) open equipment rack is grounded.	See the job aid titled *Approved Grounds* (555-245-772).
	For S8510, S8710, S8720, and S8730: Verify that the open, customer-supplied, EIA 310D (or equivalent) standard 4-post, 19-inch (48-centimeter), equipment rack is properly installed and solidly secured.	Ensure that you have the screws that come with the rack. Ensure that the rail kit for the Avaya-supplied UPS is installed on the rack or available for installation. For more information on installing the rail, see the rail kit documentation.
	Verify that you have the correct cables for the TN2312BP Internet Protocol Server Interface (IPSI) circuit packs.	The cables must be labeled and run from the control hardware rack to the port networks. Appropriate connectivity must be provided.
	Verify that you have all necessary equipment onsite.	For the list of required hardware, see: • *Installing and Configuring the Avaya S8500 Media Server* (03-300143) • *Installing and Configuring the Avaya S8700-Series Media Server* (03-300145)

Documentation checklist for migrations

For a list of documents that you need to perform the migration, see Resources on page 35.

Additional documentation needed.

✓	Document	Description
	Quick Start for Hardware Installation: Avaya S8700-Series Media Servers (555-245-703)	A quick-reference guide that provides physical installation and connection information.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides information on network connectivity.
	Installing and Configuring an Avaya S8700-Series Media Server (03-300145)	Provides installation instructions for the S8700, S8710, S8720, and S8730 Servers.

Premigration administration

This section describes the premigration administration you must perform.

Upgrading media gateways, LSPs, and ESS servers (if being used)

If newer firmware exists for a configuration using H.248 media gateways, and media modules, you must upgrade the firmware on the media gateways. If the S8700-Series Server being migrated to S8730 is the primary controller for a system that includes LSP or ESS you must upgrade the LSP and ESS before the migration of the primary controller. The recommended order is:

1. Upgrade media gateway firmware to latest version.
2. Upgrade media modules firmware to latest version.
3. Upgrade LSP software to latest version. Alternately, this step may be a server migration, for example, S8300B to S8300D migration.

Note:

Step 3 may be performed before Step 1 and 2, if the LSP is of type S8300 and you are using the S8300 LSP as a **tftp** server for H.248 media gateway and media module firmware upgrades.

4. Upgrade ESS software to latest version. Alternately, this step may be a server migration, for example, S8700 to S8730 migration.
5. Migrate the primary controller S8700, S8710, S8720 to the S8730 Server.

Duplex ESS migration workflow

CAUTION:

Do not attempt to use this abbreviated workflow as the procedure.

On each duplex ESS server, complete the following tasks:

1. Migrate the ESS.
2. Access the System Management Interface (formerly known as Maintenance Web Interface).

3. Configure the PE interface. Ensure that PE is assigned an IP-alias address and ensure that PE is assigned to the same NIC as the corporate LAN.
4. Verify that the Server A of the duplex ESS is active.

After you migrate each duplex ESS pair of servers, complete the following tasks on the main server:

1. Change the node name of server A for the duplicated pair to the node name configured for the PE interface. If the node name does not exist, define a new node name with the IP address that you configured for the PE interface of the duplex ESS.
2. Save translations.

After you migrate ALL the ESS and LSP servers in the system, migrate the main server(s):

1. Migrate the main server(s).
2. If the system has any duplicated ESS servers, administer the Server A node name of each duplicated ESS pair on its respective survivable-processor SAT screen.
3. Save translations.

Upgrading software on the LSP

Although the LSP remains registered with the primary controller, the LSP will not accept translations if it is running an older version of the software than the software that is on the primary controller.

For more information on the software upgrade process, see:

- *Installing and Upgrading the Avaya S8300 Server*, 555-234-100.
- *Installing and Upgrading the Avaya G700 Media Gateway*, 03-603333.

Hardware verification

Ensure that you have the conversion specific hardware on hand. You can reuse some of the equipment and cables when migrating an S8700, S8710, or S8720 Server to an S8730 Server.

Enterprise Survivable Servers resetting

To ensure that the ESS servers do not take over during the migration, you can reset the Network Service Timer on the ESS server to 15 minutes.

Local survivable processors

If you use local survivable processors (LSPs), and if no "recovery rule" on the gateway screen is set, either:

- shutdown LSPs before the migration of the primary controller, or
- reset the LSPs after the migration of the primary controller.

Migration tasks

This section provides the information to migrate from the current server to the S8730 Server.

Note:

The term *first S8730* or *second S8730* does not imply the actual server number. Rather this references the sequence of events in the migration.

Note:

Whenever you connect to a server, perform Clearing the ARP cache on the laptop computer on page 230 to avoid temporary internet files that might cause confusion.

On the active S8700, S8710, or S8720 Server

This section describes the procedures you must perform on the active S8700, S8710, or S8720 Server.

Configuring Telnet for Windows 2000 or WindowsXP

You can set the Microsoft Telnet application to send a carriage return (CR) and a line feed (LF) whenever you press **Enter**. The installation program sees this as two key presses.

1. On your laptop computer, click **Start** > **Run** to open the **Run** dialog box.
2. Type **`telnet`**. Press **Enter** to open a Microsoft Telnet session.
3. Type **`display`**. Press **Enter** to see the current settings.
4. Perform one of the following actions:

   If the system displays the message **Sending only CR,** close the dialog box.

   If the system displays the message **Sending both CR & LF**, continue with step 5.
5. Type **`unset crlf`**. Press **Enter**.
6. Type **`display`**. Press **Enter** to verify that the settings changed. The system displays the message **Sending only CR**.
7. Close the dialog box.

Connecting to the active server

To connect to the active server:

- Connect the laptop to the Services port (labeled 2) on the back of the server with a cross-connect CAT5 cable.

  For S8700 Server connections, see Figure 42.

Figure 42: Services laptop computer connected directly to the S8700 Server

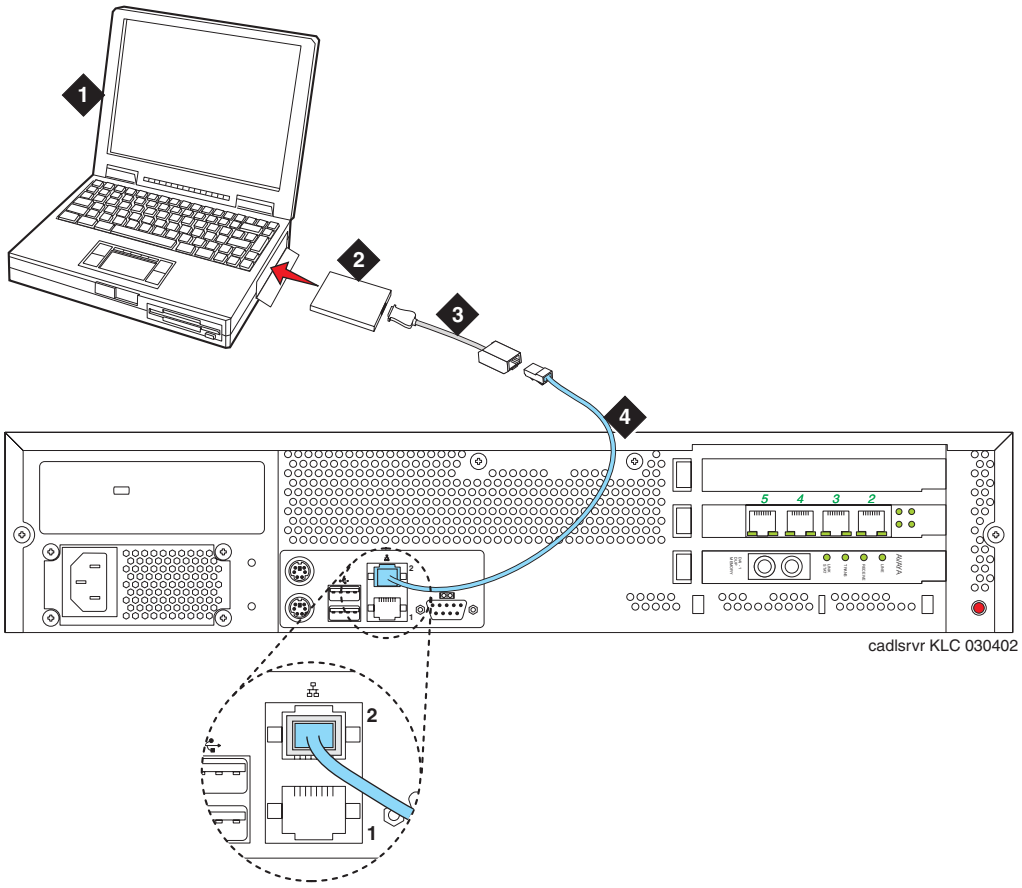


Figure notes:

1. **Services laptop**
2. **Network interface card (NIC) (not necessary if the laptop has the NIC installed)**
3. **NIC adapter cable (if necessary) (not necessary if the laptop has the NIC installed)**
4. **CAT5 crossconnect cable**

For S8710 or S8720 Server connections, see Figure 43.

Figure 43: Services laptop computer connected directly to the S8710 or S8720 Server

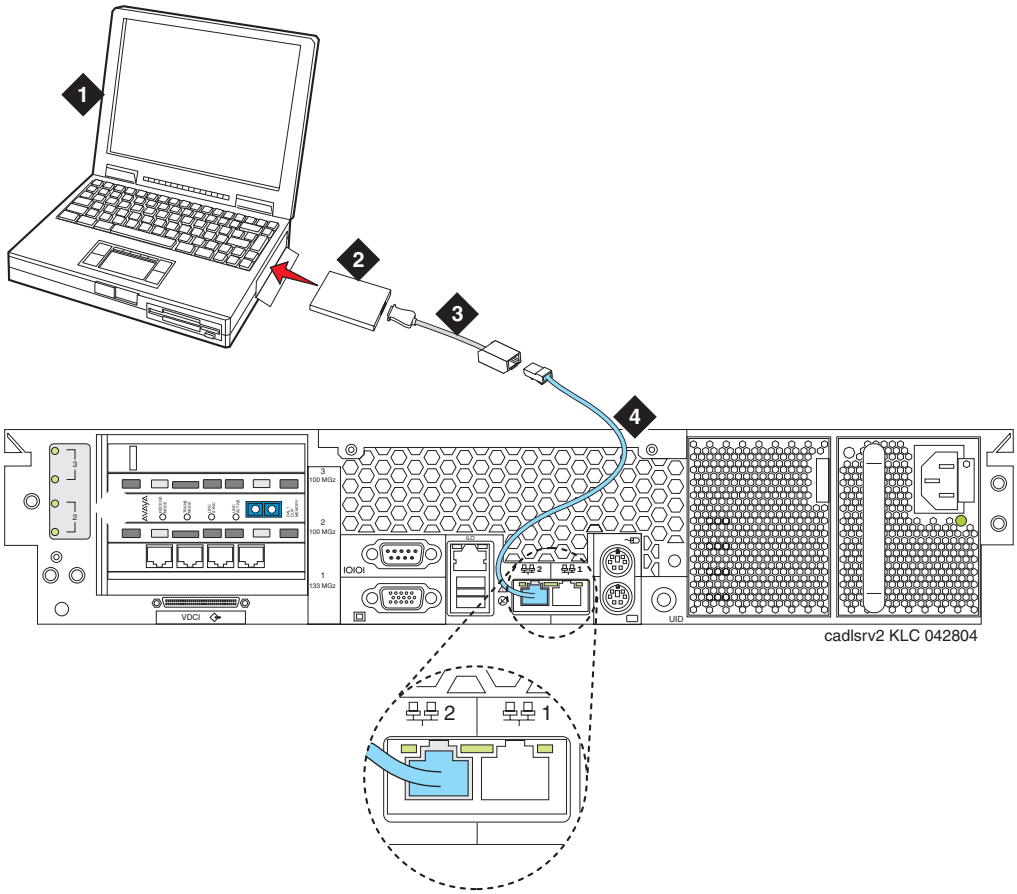


Figure notes:

1. **Services laptop**
2. **Network interface card (NIC) (not necessary if the laptop has the NIC installed)**
3. **NIC adapter cable (if necessary) (not necessary if the laptop has the NIC installed)**
4. **CAT5 crossconnect cable**

Note:

If the system currently is running Release pre-3.0, use Accessing the System Management Interface (SMI) on page 539.

If the system currently is running Release post-3.0, use secure shell (SSH).

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Checking the software release

To check the software release:

1. On the System Management Interface (SMI), click **Software Version** to see what software release is on the server.
2. If Communication Manager Release 1.0 or 1.1, upgrade to Communication Manager Release 1.3.2.

   If Communication Manager Release 1.2 or 1.3, apply the upgrade patch.

   If Communication Manager Release 2.x or higher, proceed to Clearing the ARP cache on the laptop computer on page 230.

Clearing alarms

To clear alarms:

1. If Communication Manager Release 1.x, under Alarms and Notification, click **View Current Alarms**.

   If Communication Manager Release 2.x or higher, under Alarms, click **Current Alarms**.
2. Select the server alarms to be cleared and click **Clear**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager or MS HyperTerminal.

Note:

Tasks Starting a SAT session on page 540 through Checking for translation corruption on page 542 are SAT commands and can only be done on the *active* server.

Starting a SAT session

1. Open a terminal emulation application, such as MS HyperTerminal.
2. Type **192.11.13.6 `5023`** and press **Enter**.
3. Log on as **craft** or **dadmin**.
4. Supress alarm origination.

Recording all busyouts

1. Type **`display errors`** and press **Enter**.
2. Look for type 18 errors and record any trunks that are busied out. You can return these trunks to the busyout state after the migration/upgrade.

Checking clock synchronization

To check clock synchronization:

1. Type **`status synchronization`**. Press **Enter** to verify that the clock synchronization is good.
2. Ensure that the **Switching Capabilities** field shows **enabled**.

Disabling scheduled maintenance

To prevent scheduled daily maintenance from interfering with the migration:

1. Type **`change system-parameters maintenance`**. Press **Enter**.
2. Record the settings for the **Stop Time** and **Start Time** fields.
3. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

   or

   If scheduled maintenance is not in progress, set the **Start Time** field to a time after the upgrade is completed.

   For example, if you start the upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to 21:30.

Busying out MMI circuit packs with SAT for a duplicated control network only (main server only)

CAUTION:
Multimedia-to-voice station calls are *not* preserved on an upgrade. If you do not busyout the TN787 Multimedia Interface (MMI) circuit packs, the TN787 and TN787 Multimedia Voice Conditioner ports cannot be used.

To locate all the MMI circuit packs that need to be busied out:

1. Type **`display system-parameters customer-options`** and press **Enter**.
2. Under the Multimedia Call Handling (MMCH) options, select **Basic** and **Enhanced** fields.
3. If either the `Basic` or `Enhanced` field is set to **y**, type **`list configuration all`**. Press **Enter** to locate all MMI (TN787) circuit packs.
4. If MMI circuit packs exist, type **busyout board *UUCSS*** where ***UU*** is the cabinet, ***C*** is the carrier, and ***SS*** is the slot.
5. Press **Enter** for each MMI circuit pack.

Checking for translation corruption

To check for translation corruption:

1. Type **`newterm`**. Press **Enter**.
2. If you see the following message

   Warning: Translation corruption detected . . .

   then follow the normal escalation procedure for translation corruption before continuing the upgrade.

Saving translations (main only)

The save translation command is release dependent.

Release	Load	Command	Condition
1.2	110.4	save translation	
1.3	526.5	save translation	
1.3.1	531.1	save translation lsp	If LSP present
1.3.2	536.1	save translation lsp	If LSP present
2.0	219.0	save translation lsp	If LSP present
2.0.1	221.1	save translation lsp	If LSP present
2.1	411.7	save translation all	If LSP present
2.1.1	414.1	save translation all	If LSP present
2.2	111.4	save translation all	If LSP present
2.2.1	118.0	save translation all	If LSP present
3.0 to later	340.3 and later	save translation all	If LSP or ESS present

Additional information:

- Type **`save translation`** and **HELP**. If [**`all`** or **`lsp`**] or [**`all`** or **`ess`** or **`lsp`**] displays, type **`save translation all`**. Press **Enter**.
- Type **`save translation`** and **HELP**. If [**`lsp`** or [**`ip address`**]] displays, type **`save translation lsp`**. Press **Enter**.
- Otherwise, type **`save translation`**. Press **Enter**.

To save translations, perform the following step:

- Type **`save translation`**. Press **Enter**.

  If this operation is unsuccessful, follow the normal escalation procedures before continuing.

Checking the CNC status

Note:

You can perform this step only if you have Communication Manager Release 3.0 or later.

If the system uses Control Network C (CNC), you need to check the CNC status.

To check the CNC status:

1. Access the server command line interface.
2. Log in as **`craft`** or **`dadmin`**.
3. Type **`cnc status`**. Press **Enter**.

   The system displays one of the following messages:

   Control Network C has not been configured.

   Control Network C has been configured.
4. Record the CNC setting.

Backing up the active S8700, S8710, or S8720 Server

You must do a backup for the active S8700, S8710, or S8720 Servers. For more information, see Table 24. You can back up to:

Note:

Do not use the PCMCIA flash card (for S8700). The PCMCIA flash card is not a valid option for the migration

1. A network device server on the network such as an ftp server (release dependent)

2. The USB-connected Compact Flash (for the S8710 only)

Table 24: Backup destinations for migrations

Backup destination	S8700	S8710/S8720
PCMCIA flash card	-	-
USB-connected Compact Flash	-	x[1]
SCP/SFTP/FTP server	x[2]	x

1. Preferred for S8710 or S8720

2. Preferred for S8700

The backup procedures in Table 25 are different depending on the software release currently running on your server.

Table 25: Migration to S8730, Release 5.x or later, backup, release specific

Release	Load	Web Interface for Backup	Data Set	File Name of Backup
1.2	02.0.110.4 S8700	Linux Migration Backup/Restore	N/A[1]	upgrade...tar.gz.
1.3	03.0.526.5 S8700	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
1.3.1	03.1.531.0 S8700	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
1.3.2	03.2.536.1 S8700	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.0	00.0.219.0	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.0.1	00.1.221.1	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.1	01.0.411.7	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.1.1	01.1.414.1	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.

1 of 2

Table 25: Migration to S8730, Release 5.x or later, backup, release specific (continued)

Release	Load	Web Interface for Backup	Data Set	File Name of Backup
2.2	02.0.111.4	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.2.1	02.0.118.1	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.2.2	02.2.122.0	Linux Migration Backup/Restore	N/A	upgrade...tar.gz
3.0 and later	00.0.340.3 and later	Backup Now	Full	full...tar.gz.

2 of 2

1. Data Set is not selectable by the user.

Backing up the configuration data and translations to the USB-connected Compact Flash card

Note:

This procedure is for the S8720 or the S8710 Server with Communication Manager Release 3.0 and later.

To back up the configuration data and translations to the USB-connected Compact Flash card:

1. On the System Management Interface (SMI), click Administration > Server (Maintenance) under Data Backup/Restore click **Backup Now**.
2. Under Data Sets, click **Full Backup** (release dependent).
3. Under Backup Method, click **Local PC card**.
4. In the **Retain** field, type **3**.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Check the box next to the file being backed up and click **Check Status**. When the backup is complete, the system displays the following message.

   Backup successful

Backing up the configuration data and translations to a server on the network

This procedure assumes that you are backing up from Communication Manager Release 3.0 and later.

To back up the configuration data and translations to the network:

1. Under Data Backup/Restore, click **Backup Now**.
2. Under Data Sets, click **Full Backup** (release dependent).
3. Under Backup Method, select Network Device and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** - enter the host IP address
   - **Directory** (for SFTP and FTP)
   - **File Path** (for SCP)
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Check the box next to the file being backed up and click **Check Status**. When the backup is complete, the system displays the following message.

   Backup successful

   CAUTION:
   Check the text to verify that there are no error messages. Ignoring the error message can result in no backup.

Backing up the configuration data and translations using Linux Migration Backup to the USB-connected Compact Flash card

Note:
This procedure is only for the S8710 Server with Communication Manager Release pre3.x.

To back up the configuration data and translations using the Linux Migration Backup/Restore to the USB-connected Compact Flash card:

1. Under Server Upgrades, click **Linux Migration (Backup/Restore)**.
2. Select **Initiate new backup or restore** and click **Submit**.
3. In the Backup Method section, select **Local PC Card**.

4. In the **Retain** field, type **3**.
5. Click **Submit**.
6. Under Server Upgrades, click **Linux Migration (Backup / Restore)** to review the status of the backup.
7. Select **Display status**
8. Click **Submit**.

   This window might display a **BACKUP COMPLETE** message with possible series 200 error messages. You can ignore these series 200 error messages and proceed with the backup.

Backing up the configuration data and translations using Linux Migration Backup to a server on the network

This procedure assumes that you are backing up from Communication Manager release pre2.x.

Important:
Do not perform a standard backup the translations on the S8700 and try to restore them on the S8730. Restoring the translations will fail. Use the instructions in this section to perform a Linux migration backup.

To back up the configuration data and translations using the Linux Migration Backup/Restore from the S8700, S8710, or S8720 Server to a network device:

1. Under Server Upgrades, click **Linux Migration (Backup/Restore)**.
2. Select **Initiate new backup or restore** and click **Submit**.
3. In the Backup Method section, select a network device.

   Note:
   Some releases support backup to SFTP and SCP servers.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** - enter the host IP address
   - **Directory** (for SFTP and FTP)
5. Click **Submit**.
6. Under Server Upgrades, click **Linux Migration (Backup / Restore)** to review the status of the backup.
7. Select **Display status**

8. Click **Submit**.

   This window might display a **BACKUP COMPLETE** message with possible series 200 error messages. You can ignore these series 200 error messages and proceed with the backup.

Obtaining the Product ID on the active server

To obtain the Product ID:

1. Access the server command line interface.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**. Press **Enter**.

   The **`productid`** is the product ID you received from the customer or the ART too.
4. Record the product ID.

Looking up server configuration on the active server

Perform this task if you are backing up to the customer network.

To look up and record server configuration information:

1. Under Server Configuration, click **Configure Server** to open the first page (Select server type) of the Configure Server process.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure individual services** and click **Continue**.
4. Click **Set Identities** from the main menu.
5. In the Set Identities area, record the following information for later use:
   - The host names in the **Host Name** fields.
   - Server number (from the **This is server number** field)
   - Ethernet assignments (in the Select NIC Usage area)
6. Record the Ethernet port assignment and usage for each of the five possible interfaces. For example, see Control Network A in Table 26. Notice that CNA is assigned Ethernet 0.

   Note:

   If these values are different from the defaults, physical connections to the Ethernet ports must match these settings.

Table 26: Network Interface Card usage

Control Network A (Default: Ethernet 0)	Ethernet 0
Services Port (Default: Ethernet 1)	Ethernet 1
Server Duplication Link (Default: Ethernet 2)	Ethernet 2
Control Network B (Default: Ethernet 3)	UNUSED
Corporate LAN (Default: Ethernet 4)	Ethernet 4

7. Click **Continue**.
8. In the Corporate LAN Interface section, record the following information for later use:
   - IP addresses (under the Corporate LAN Interface area)
   - Subnet mask (under the Corporate LAN Interface area)
   - Default gateway (under the Corporate LAN Interface area)

Disconnecting from the active S8700, S8710, or S8720 Server

Disconnect the Services laptop from the active server.

On the standby S8700, S8710, or S8720 Server

This section describes the procedures you must perform on the standby S8700, S8710, or S8720 Server.

Connecting to the standby server

To connect to the standby server:

- Connect the laptop to the Services port (2) on the back of the *standby* server with a cross-connect CAT5 cable.

Accessing the standby server

To access the standby server:

1. Connect the laptop to the Services port (2) on the standby server.
2. Log in. For more information, see Accessing the System Management Interface (SMI) on page 539 and return here.

Checking the software release

To check the software release:

1. On the System Management Interface (SMI), click **Software Version** to see what software release is on the server.
2. If Communication Manager Release 1.0 or 1.1, upgrade to Communication Manager Release 1.3.2.

   If Communication Manager Release 1.2 or 1.3, apply the upgrade patch.

   If Communication Manager Release 2.x or higher, go to Clearing the ARP cache on the laptop computer on page 230.

Checking the CNC status

Note:

You can perform this step only if you have Communication Manager Release 3.0 or later.

If the system uses Control Network C (CNC), you need to check the CNC status.

To check the CNC status:

1. Access the server command line interface.
2. Log in as **`craft`** or **`dadmin`**.

3. Type **`cnc status`**. Press **Enter**.

   The system displays one of the following messages:

   Control Network C has not been configured.

   Control Network C has been configured.

4. Record the CNC setting.

   The settings for this server must be the same as for the active server.

Backing up the standby S8700, S8710, or S8720 Server

You must do a backup for the standby S8700, S8710, or S8720 Servers. For more information, see Table 27. You can back up to:

Note:

Do not use the PCMCIA flash card (for S8700). The PCMCIA flash card is not a valid option for the migration

1. An ftp server on the network (release dependent)
2. The USB-connected Compact Flash (for the S8710 only)

Table 27: Backup destinations for migrations

Backup destination	S8700	S8710/S8720
PCMCIA flash card	-	-
USB-connected Compact Flash	-	x[1]
FTP/SFTP/SCP server	x[2]	x

1. Preferred for S8710 or S8720
2. Preferred for S8700

The backup procedures in Table 28 are different depending on the software release currently running on your server.

Table 28: Migration to S8730, Release 3.1 or later, backup

Release	Load	Web Interface for Backup	Data Set	File Name of Backup
1.2	02.0.110.4 S8700	Linux Migration Backup/Restore	N/A[1]	upgrade...tar.gz.
1.3	03.0.526.5 S8700	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
1.3.1	03.1.531.0 S8700	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
1.3.2	03.2.536.1 S8700	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.0	00.0.219.0	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.0.1	00.1.221.1	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.1	01.0.411.7	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.1.1	01.1.414.1	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.2	02.0.111.4	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.2.1	02.0.118.1	Linux Migration Backup/Restore	N/A	upgrade...tar.gz.
2.2.2	02.2.122.0	Linux Migration Backup/Restore	N/A	upgrade...tar.gz
3.0 and later	00.0.340.3	Backup Now	Full	full...tar.gz.

1. Data Set is not selectable by the user.

Backing up the configuration data and translations to the USB-connected Compact Flash card

Note:

This procedure is for the S8720 or for the S8710 Server running Communication Manager Release 3.0 and later.

To back up the configuration data and translations to the USB-connected Compact Flash card:

1. In the Communication Manager System Management Interface (SMI), click **Backup Now**.
2. Under Data Sets, click **Full Backup** (release dependent).
3. Under Backup Method, click **Local PC card**.
4. In the **Retain** field, type **3**.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Check the box next to the file being backed up and click **Check Status**. When the backup is complete, the system displays the following message.

   Backup successful

Backing up the configuration data and translations to a server on the network

This procedure assumes that you are backing up from Communication Manager Release 3.0 and later.

To back up the configuration data and translations to the network:

1. Under Data Backup/Restore, click **Backup Now**.
2. Under Data Sets, click **Full Backup** (release dependent).
3. In the Backup Method section, select a network device.

   Note:

   Some releases support backup to SFTP and SCP servers.

4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** - enter the host IP address
   - **Directory** (for SFTP and FTP)
5. Click **Start Backup**.
6. Click **Status** to view the backup history.

7. Check the box next to the file being backed up and click **Check Status**. When the backup is complete, the system displays the following message.

   Backup successful

   CAUTION:
   Check the text to verify that there are no error messages. Ignoring the error message can result in no backup.

Backing up the configuration data and translations using Linux Migration Backup to the USB-connected Compact Flash card

Note:
This procedure is only for the S8710 Server with Communication Manager release pre3.x.

To back up the configuration data and translations using the Linux Migration Backup/Restore to the USB-connected Compact Flash card:

1. Under Server Upgrades, click **Linux Migration (Backup/Restore)**.
2. Select **Initiate new backup or restore** and click **Submit**.
3. In the Backup Method section, select **Local PC Card**.
4. In the **Retain** field, type **3**.
5. Click **Submit**.
6. Under Server Upgrades, click **Linux Migration (Backup / Restore)** to review the status of the backup.
7. Select **Display status**
8. Click **Submit**.

   This window might display a **BACKUP COMPLETE** message with possible series 200 error messages. You can ignore these series 200 error messages and proceed with the backup.

Backing up the configuration data and translations using Linux Migration Backup to a server on the network

This procedure assumes that you are backing up from a Communication Manager release that is pre 2.x.

To back up the configuration data and translations using the Linux Migration Backup/Restore from the S8700, S8710, or S8720 Server to a server on the network:

1. Under Server Upgrades, click **Linux Migration (Backup/Restore)**.
2. Select **Initiate new backup or restore** and click **Submit**.
3. In the Backup Method section, select a network device.

Note:

Some releases support backup to SFTP and SCP servers.

4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** - enter the host IP address
   - **Directory** (for SFTP and FTP)
   - **File Path** (for SCP)
5. Click **Submit**.
6. Under Server Upgrades, click **Linux Migration (Backup / Restore)** to review the status of the backup.
7. Select **Display status**
8. Click **Submit**.

   This window might display a **BACKUP COMPLETE** message with possible series 200 error messages. You can ignore these series 200 error messages and proceed with the backup.

Obtaining the Product ID on the standby server

Note:

You might see different values for the product ID between the active and standby servers.

To obtain the Product ID:

1. Access the server command line interface.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**. Press **Enter**.

   The **`productid`** is the product ID you received from the customer or the ART tool.
4. Record the product ID.

Looking up server configuration information on the standby server

Perform this task if you are backing up to the customer network.

To look up and record server configuration information:

1. Under Server Configuration, click **Configure Server** to open the first page (Select server type) of the Configure Server process.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure individual services** and click **Continue**.
4. Click **Set Identities** from the main menu.
5. In the Set Identities area, record the following information for later use:
   - Server number (from the **This is server number** field)
   - Ethernet assignments (in the Select NIC Usage area)
6. Record the Ethernet port assignment and usage for each of the five possible interfaces. For example, see Control Network A in Table 29. Notice that CNA is assigned Ethernet 0.

   Note:

   If these values are different from the defaults, physical connections to the Ethernet ports must match these settings.

Table 29: Network Interface Card usage

Control Network A (Default: Ethernet 0)	Ethernet 0
Services Port (Default: Ethernet 1)	Ethernet 1
Server Duplication Link (Default: Ethernet 2)	Ethernet 2
Control Network B (Default: Ethernet 3)	UNUSED
Corporate LAN (Default: Ethernet 4)	Ethernet 4

7. Click **Continue**.
8. In the Corporate LAN Interface section, record the following information for later use:
   - IP addresses (under the Corporate LAN Interface area)
   - Subnet mask (under the Corporate LAN Interface area)
   - Default gateway (under the Corporate LAN Interface area)
9. Click **Close Window** to exit the **Configure Server** window.

Busying out the standby S8700, S8710, or S8720 Server

To busyout the S8700, S8710, or S8720 Server:

1. On the System Management Interface (SMI), click **Busy Out Server**.
2. On the Busy-Out Server window, click **Busy Out**.

Shutting down the standby S8700, S8710, or S8720 Server

CAUTION:
Ensure that you are connected to the *standby* S8700, S8710, or S8720 Server. Proceeding with the following steps and being connected to the incorrect server can result in service disruption.

To shut down the standby S8700, S8710, or S8720 Server:

1. Under Server, click **Shutdown server**.
2. Make the following selections:
   - Select **Delayed Shutdown**
   - Deselect **Restart server after shutdown**
3. Click **Shutdown**.

Removing the duplication cables

To remove the duplication cables:

1. Label and disconnect the duplication fiber cable (if present) from both the S8700, S8710, or S8720 Servers.
2. Label and disconnect the duplication interface IP cable from both the S8700, S8710, or S8720 Servers.

Removing the standby S8700, S8710, or S8720 Server from the rack

To remove the standby S8700, S8710, or S8720 Server from the rack:

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.

3. Disconnect the power cord from the UPS.
4. Remove the standby S8730 Server from the rack, if necessary.
5. Remove the rails from the rack.

Removing the DAL2 card, if necessary

If the S8730 already has a DAL2 installed, go to Installing the first S8730 Server in the rack on page 558. Perform this procedure only if you are reusing a DAL2 that was installed in the S8720 Server in the S8730 Server. To verify which DAL is installed, see Installing the DAL2, if necessary on page 558.

If you need to remove the DAL2 card, follow the procedures outlined in Appendix B: DAL: Removing or Installing on page 345. After you remove the DAL, return to On first S8730 Server on page 558 to continue the migration.

On first S8730 Server

This section describes the procedures you must perform on the first S8730 Server.

Installing the DAL2, if necessary

A DAL2 card is required for each S8730 Server using hardware duplication. If you are not using hardware duplication, go to Installing the first S8730 Server in the rack on page 558.

If you are using hardware duplication, verify the type of DAL board that is installed in the server by looking at the label printed on the DAL board. If you need to install a DAL2, use the instructions outlined in Appendix B: DAL: Removing or Installing on page 345. Install the DAL2 in ***both servers***. After completing the installation of the DAL2 go to Installing the first S8730 Server in the rack on page 558.

Installing the first S8730 Server in the rack

To install the first S8730 Server in the rack:

1. Snap the rails on to the server.
2. Attach the extension rails to the rack.

3. Install the S8730 Server in the rack. For more information, see *Quick Start for Hardware Installation: S8700 Series Servers* (03-300145).

Inserting the Communication Manager software distribution CD

To insert the Communication Manager software distribution CD in the CD/DVD drive of the S8730 Server:

Note:

You must place the CD in the drive *before* turning on the server.

1. Use a paperclip to open the CD-ROM drive on the server.
2. Insert the Communication Manager software distribution CD in the CD/DVD drive and close the drive door.

Connecting the cables to the first S8730 Server

To connect the cables to the server:

Note:

Do not connect the fiber duplication connection cable or the duplication interface IP cable at this time to either S8730 Server.

1. The network connections depend on the type of memory duplication and the type of control network being used. Connect the network cables as described in the following table.

Control Network	Software Memory Duplication	Hardware Memory Duplication
Dedicated	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled 1) • CNB (if used) to Eth3 (right top)	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled **1**) • CNB (if used) to Eth3 (right top)
Nondedicated	• LAN/CNA to Eth2 (right bottom) • CNB (if used) to Eth3 (right top)	• LAN/CNA to Eth0 (middle bottom labeled **1**) CNB (if used) to Eth3 (right top)

Figure 44: Duplication and control network cables for hardware duplication

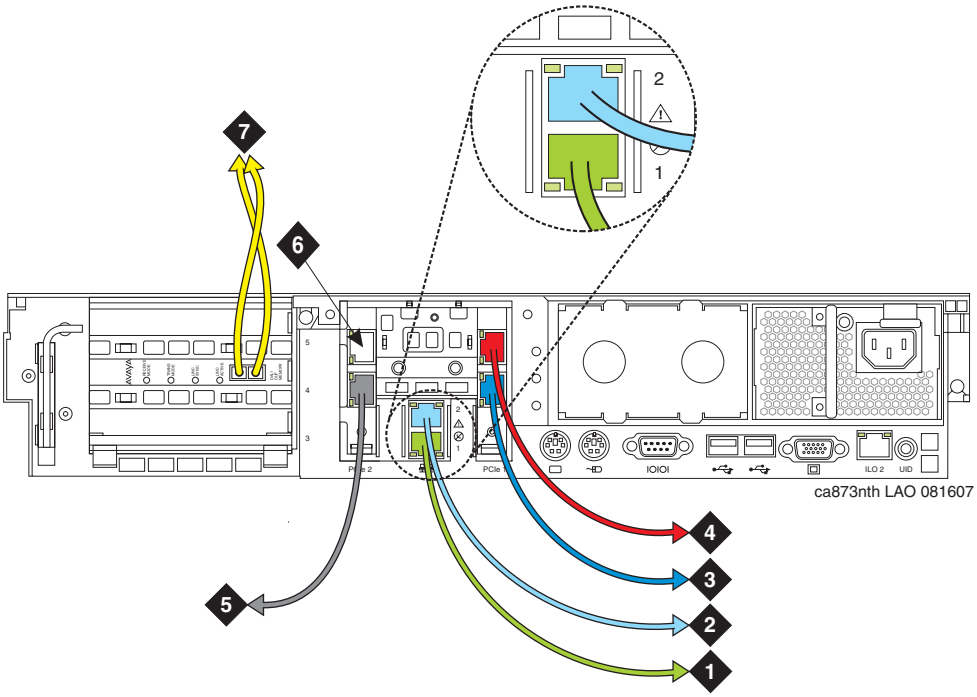


Figure notes:

1. **CNA (also LAN for nondedicated control network) — Eth0**
2. **Services port — Eth1**
3. **Duplication cable (crossover) — Eth2**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**
7. **Fiber duplication cable**

Figure 45: Duplication and control network cables for software duplication

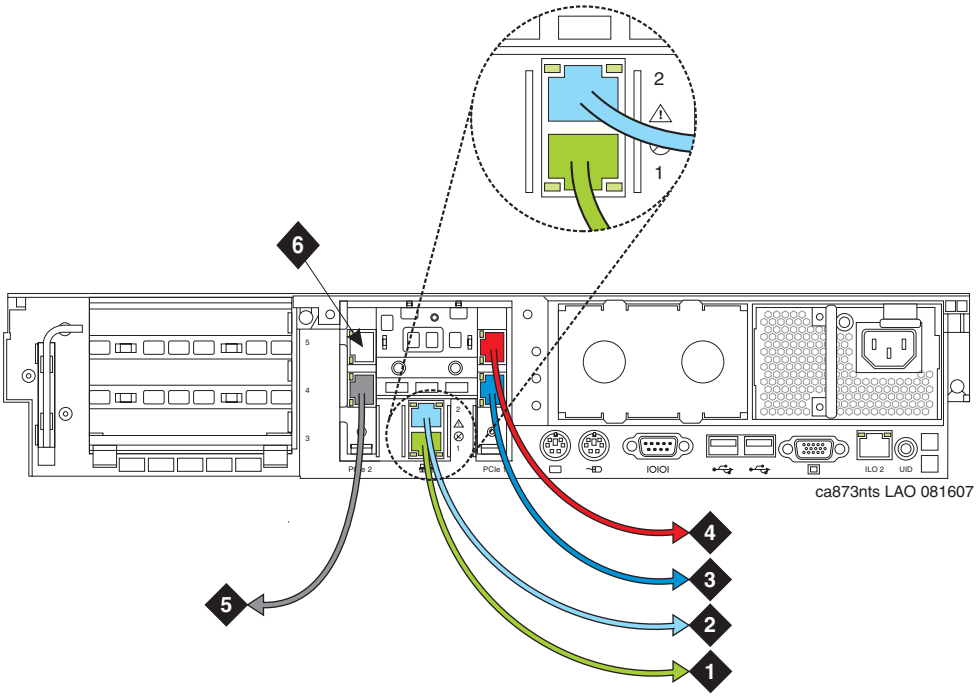


Figure notes:

1. **Duplication cable (Crossover) — Eth0**
2. **Services port — Eth1**
3. **CNA (also LAN for nondedicated control network) — Eth2**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**

2. Connect the modem to one of the USB ports.
3. Connect the power cord to the rear of the server.
4. To turn on the server, push the yellow power button on the front of the S8730.

   Note:

   Do not connect the USB flash drive at this time.

Accessing the first S8730 Server

To access the server:

1. Clear the ARP cache from the laptop if necessary. For more information, see Connecting to the active server on page 537 and return here.

2. Connect the laptop to the Services port (labeled 2) on the back of the server with a cross-connect CAT5 cable.

   For S8730 Server connections, see Figure 46.

Figure 46: Services laptop computer connected directly to the S8730 Server

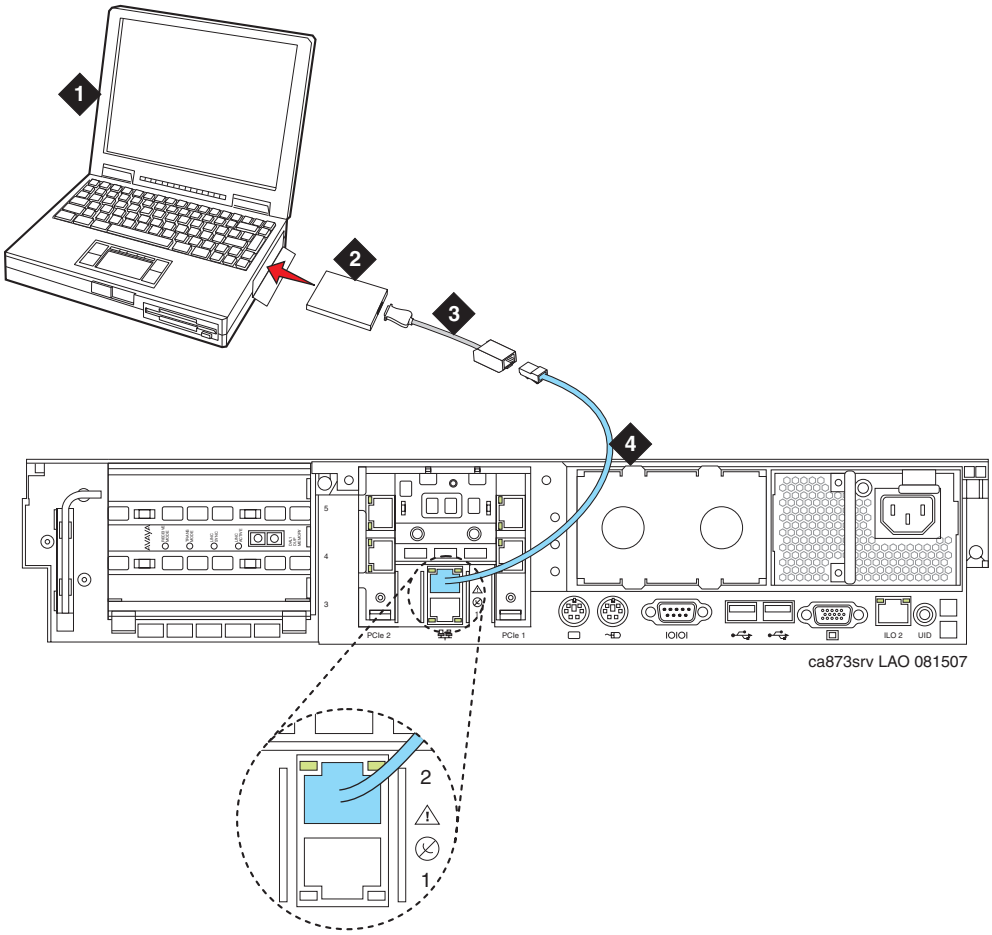


Figure notes:

1. **Services laptop**
2. **Network interface card (NIC) (not necessary if the laptop has the NIC installed)**
3. **NIC adapter cable (if necessary) (not necessary if the laptop has the NIC installed)**
4. **CAT5 crossconnect cable**

3. On your laptop computer, click **Start** > **Run** to open the **Run** dialog box,

4. Type **`ping -t 192.11.13.6`**. Press **Enter** to check connectivity between the Services laptop and the server.

Wait at least 3 minutes after turning on the server before starting a Telnet session to access the information on the CD.

Installing Communication Manager

Use a telnet session to install Communication Manager.

To install Communication Manager:

1. From the laptop Start menu, click **Start** > **Run**.
2. In the **Run** dialog box, type **`telnet 192.11.13.6`**. Press **Enter** to view the first screen.

Note:

To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

3. Select **Install**, ensure that OK is highlighted and press **Enter**.

4. On the **Select Release Version** window, ensure that the Build line and <OK> are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

   Once the drive is properly configured, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

   These processes can take up to 20 minutes. When the server is ready to reboot, the CD-ROM drive drawer opens. You must remove the CD from the drive at this time.

   The reboot can take up to 3 minutes. The telnet session drops automatically.

Insert the USB flash drive in the USB port

Insert the USB flash drive containing the backup in one of the USB ports. It does not matter which USB port you use.

Accessing the System Management Interface (SMI)

To access the server:

1. Start the Web browser.
2. In the **Address** field, type **`192.11.13.6`** and press **Enter** to open the login Web page.
3. Log in as **craft** or **dadmin**.
4. Click **yes** to suppress alarms

   The system displays the **Communication Manager System Management Interface (SMI)**.

Checking the software version

Use the Communication Manager System Management Interface (SMI) to check the software release:

- Click Administration > Server (Maintenance) > under Server click **Software Version**

  Verify the release running on the server.

Verifying date and time

Use the Communication Manager System Management Interface (SMI) to change the date and time:

1. Click Administration > Server (Maintenance) > under Server, click **Server Date/Time**.
2. Change the date, time, and time zone as needed.
3. To make changes, click **Submit**.

Copying files to the server (if any)

From the services laptop, copy the following to the S8730 Server:

- The software update or service pack
- RFA license file
- Avaya authentication file

- Firmware updates for programmable circuit packs and media modules might also be required. These files might be on the software CD.

  Note:

  Do not copy the Linux migration upgrade set with this method.

To copy files to the server:

1. On the System Management Interface (SMI), click Administration > Server (Maintenance) >

under **Miscellaneous**, select **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the **Choose File** window on your computer.
4. Find the files that you need to copy to the server.
5. Click **Download** to copy the file(s) to the server.

   The system automatically copies the files to the default location on the server.

Installing security and service pack updates, if any

Use this procedure to unpack and active the files that you copied in the previous step.

1. Under **Server Upgrades**, select **Manage Updates**.
2. If an update file you want to activate shows **packed** in the **Status** column:
   a. Select **update ID**
   b. Click **Unpack**
3. Wait until the system displays the message **Unpacked Successfully..** and then click **Continue**.

   The system displays the **Manage Updates** screen.
4. If the update ID you want to activate shows **unpacked** in the **Status** column:
   a. Select the **update ID**
   b. Click **Activate**

      The screen shows the status of activating the update. If a reboot or restart of Communication Manager is required, the system automatically reboots or restarts Communication Manager.
5. Click **Yes**.

   Wait until the system displays the **Continue** button.

6. Click **Continue**.

   The system displays the status of the update.

Stopping Communication Manager on the first S8730 Server

To stop Communication Manager:

- Type **`stop -acf`**. Press **Enter** to stop Communication Manager.

Configuring to allow restoring configuration data and translations from a server on the network

Important:
If you backed up files to the USB-connected Compact Flash, do not perform this procedure. Go to Configuring to allow restoring configuration data and translations from the USB flash card on page 568.

If you backed up to the network of the customer, you must readminister the Ethernet port connecting to the network. You must have the host name, IP address, subnet mask and default gateway for the two servers and the active server and the IP address for the Ethernet port connecting to the customer network.

To configure the network parameters:

1. Under Server Configuration, click **Configure Server** to open the first page of the Configure Server process.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure individual services**. Click **Continue**.
4. Click **Set Identities** from the main menu.
5. On the **Set Identities** window:
   a. In the **Host Name** fields, fill out the host names for each server.
   b. In the **This is server number** field, select the appropriate number. For example, if you are on server 1, select **1**.
   c. Assign the Ethernet ports. Click **Continue**.
6. In the **Configure Interfaces** window:

a. Fill in the correct IP addresses, Gateway, and Subnet mask for only the Ethernet port connected to the customer LAN.

b. Select **AUTOSENSE** for the speed of ***all*** the Ethernet interfaces.

c. Click **Change** to update the server. When the screen shows

Successfully configured ethernet interfaces.

The Ethernet ports are configured.

7. Click **Close Window** to close the Configure Server wizard.

Verifying connectivity from the first S8730 Server to the network server

To verify that the Ethernet port is working, ping from the S8730 Server to the network server where the backup files are stored.

Note:

You might need to restart your browser before doing the next steps.

1. Under Diagnostics on the S8730 Server, click **Ping**.
2. Select Host Name or IP Address and type the IP address of the server where the system files are stored
3. Click **Execute Ping**.

   If you can successfully ping the server, you can proceed to restore the backed up sets of files.

Configuring to allow restoring configuration data and translations from the USB flash card

If you backed up to the USB flash card, you must configure the server type, name, and the number to prepare for the restore procedure.

To configure to allow restoring configuration data and translations from the flash card:

1. Under Server Configuration, click **Configure Server** to open the first page of the Configure Server process.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure individual services**. Click **Continue**.

4. Click **Set Identities**. In the **Set Identities** screen:
   a. In the **Host Name** fields, fill out the host names for each server.
   b. In the **This is server number** field, select the appropriate number. For example, if you are on server 1, select **1**.
   c. Click **Continue**.
5. In the **Configure Interfaces** window:
   a. Select **AUTOSENSE** for ***all*** the Ethernet interfaces.
   b. Click **Change** to update the server.
   c. When the screen shows

      Successfully configured ethernet interfaces.

      Click **Close Window** to close the Configure Server wizard.

Restoring configuration data and translations to the first S8730 Server

Note:

The physical connections to the Ethernet ports must match the server configuration assignments that were backed up in Looking up server configuration information on the standby server on page 555. The connections to the Ethernet ports that do not match the configuration can prevent access to the server.

The restore method depends on how you backed up the data. Currently there are two ways to restore backed up data.

- Restoring data based up to the Compact Flash card (applicable only if migrating from an S8720 Server)
- Restoring data backed up to the customer network (applicable only if migrating from a S8700, S8710, or S8720 Server)

In Table 30, the restore procedure is dependent on what backup method was used.

Table 30: Migration to S8730, Release 5.x or later, using Web interface, View/Restore

S8700, S8710, or S8720		File Name of Backup
Release	**Load**	
1.2	02.0.110.4	upgrade...tar.gz.
1.3	03.0.526.5	upgrade...tar.gz.
1.3.1	03.1.531.0	upgrade...tar.gz.
1.3.2	03.2.536.1	upgrade...tar.gz.
2.0	00.0.219.0	upgrade...tar.gz.
2.0.1	00.1.221.1	upgrade...tar.gz.
2.1	01.0.411.7	upgrade...tar.gz.
2.1.1	01.1.414.1	upgrade...tar.gz.
2.2	02.0.111.4	upgrade...tar.gz.
2.2.1	02.0.118.0	upgrade...tar.gz.
2.2.2	02.2.122.0	full...tar.gz.
3.0 and later	00.0.340.3 and later	full...tar.gz.

Restoring data backed up to the Compact Flash card

Use the Communication Manager System Management Interface (SMI) to restore data based up to the Compact Flash card:

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. Click **Local PC Card**.
3. Click **View**.
4. In the **View/Restore Data Results** window:
   a. Select the file name to restore
   b. Select both force options.

   For example, the file might be called full_*custservname*_timestamp_datestamp.tar.gz where *custservname* is the customer server name from which Communication Manager is backed up.

5. Click **Restore**.
6. Click **Check Status** to view the restore progress.

   Wait for the message that says the restore was completed successfully. If the restore was successful, go to Verifying the first S8730 Server configuration on page 571.

Restoring data backed up to the customer network

To restore data backed up to the customer network from S8700, S8710, or S8720 Servers:

1. On the System Management Interface (SMI), click **View/Restore Data**.
2. Under the **View current backup contents in section**, click Network Device.

   Note:
   SFTP or SCP are also available.
3. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** - enter the host IP address
   - **Directory** (for SFTP and FTP)
   - **File Path** (for SCP)
4. In the Method section, select the network server.
5. Click **View**.
6. In the **View/Restore Data Results** window, select the file name to restore and select both force options.

   For example, the file might be called full_*custservname*_timestamp_datestamp.tar.gz where *custservname* is the customer server name from which Communication Manager is backed up.
7. Click **Restore**.
8. Click **Refresh** view the restore progress.

Verifying the first S8730 Server configuration

To verify the first S8730 Server configuration:

1. Under **Server Configuration**, click **Configure Server** to start the configure server process.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure all services using the wizard**. Click **Continue**.

4. On the **Set Identities** page, under the Select Server Duplication area, select either:
   - **This is a duplicated server using duplication hardware**
   - **This is a duplicated server using software-based duplication**
   - **This is a duplicated server using encrypted software-based duplication**

   Note:
   The physical connections to the Ethernet ports are different for hardware duplication and software duplication. For more information, see Connecting the cables to the first S8730 Server on page 559.
5. Click **Continue**.
6. On the **Configure Interface** page, set the speed for Ethernet ports to **AUTO SENSE**.

   Note:
   You must click through all the screens whether there are changes or not.
7. On the **Configure ESS** window:
   - If the server is a primary control main, click **This is NOT an enterprise survivable server**
   - If the server is an ESS server, click **This is an enterprise survivable server (ESS)**
8. Click **Continue**.
9. After checking all the pages, click **Continue** on the **Update System** screen. The Update System screen shows each configuration task as the task completes. When done, the screen shows the line **All configuration information was entered**.
10. Click **Close Window** to close the Configure Server wizard.

Configuring the Processor Ethernet interface (on the ESS)

Perform this task if you are migrating from an ESS running Communication Manager Release 5.1.x or prior to an S8730 ESS running Communication Manager 5.2 or later.

1. Under **Installation**, click **Configure Server** and follow the instructions on the wizard. Alternatively, you can configure services individually. For more information, see the online help available with the SMI.
2. On the **Set Identities** page, verify that PE is assigned to the same NIC as the corporate LAN.
3. On the **Configure Interfaces** page, assign an IP-alias address for the PE interface of the duplex ESS. PE must be assigned to the same NIC as the corporate LAN. The IP-alias address is assigned in the **Active server** field.
4. Submit the change and exit from the Configure Server wizard.

Confirming the product ID on the first S8730 Server

To confirm the Product ID:

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**. Press **Enter**.

   The **`productid`** must match the value record in Obtaining the Product ID on the standby server on page 555. If value does not match, escalate the problem immediately.

Enabling CNC, if necessary

If the CNC status in Checking the CNC status on page 543 is **Control Network C was configured**, do this procedure. Otherwise, go to Initializing and busyout the first S8730 Server on page 574.

If the system uses Control Network C (CNC):

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **`craft`** or **`dadmin`**.
3. Type **`cnc on`**. Press **Enter**.

Rebooting the first S8730 Server

Rebooting the S8730 Server is necessary to initialize server settings that are restored but not yet activated.

To reboot, on the Communication Manager System Management Interface (SMI)

1. Click **Administration > Server (Maintenance)**, under **Server**, click **Shutdown Server**.
2. Select:
   - **Delayed Shutdown**
   - **Restart Server after Shutdown**
3. Click **Shutdown**.

Accessing the first S8730 Server

To access the first S8730 Server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Connecting to the active server on page 537 and return here.
2. Open a browser and connect to the server.
3. Log in. For more information, see Accessing the System Management Interface (SMI) on page 539.
4. Suppress all alarms.

Initializing and busyout the first S8730 Server

To initialize Communication Manager:

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.

   Note:

   For the following step, the logons are release-dependent.

2. Log in as **`craft`** or **`dadmin`**.
3. Type **`stop -acf`**. Press **Enter** to stop Communication Manager.

   Communication Manager might already be stopped in Stopping Communication Manager on the first S8730 Server on page 567.

4. Type **`server -b`**. Press **Enter** to queue a busy out of the Communication Manager software.

   The system responds with the following message

   ACP not yet running, queueing busyout request.

5. Type **`start -ac`**. Press **Enter** to start Communication Manager and load the translations.

Configuring the ESS and the LSP for compatibility with S8730

If the main servers are S8730 or S8720 Servers configured as XL, the ESS servers and the LSPs must also be configured as XL.

The S8300B LSPs, the S8700 ESS servers, and the S8710 ESS servers can not be configured as XL and are therefore not compatible with main servers that are configured as XL.

Note:

You do not have to perform this procedure on an S8730 ESS server as it is already configured as XL.

Use the following steps to configure the ESS server or the LSP:

1. Type **`stop -acfn`** on the command line interface and press **Enter** to stop Communication Manager call processing.
2. On the ESS server's or the LSP's System Management Interface (SMI), under **Installation >** click **Configure Server**.

   The system displays the **Review Notices** screen.
3. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.

   CAUTION:

   For the next step, if you select and save as **Extra Large** you cannot revert to **Standard**. If you try to go back to **Standard**, server translation corruption occurs.
4. Select **Configure individual services** and click **Continue**.
5. In the left column, click **Configure ESS** if this is an ESS server or click **Configure LSP** if this is an LSP.
6. Under Configure Memory, select **Extra Large** and click **Change**.
7. Click **Close Window**.
8. Type **`start -ac`** on the command line interface and press **Enter** to restart Communication Manager call processing.
9. Type **`swversion`** on the command line interface and press **Enter**.

   In the **Memory Config** field, verify that the setting is **Extra Large**.

Performing an integrity check on the first S8730 Server

Use the System Management Interface (SMI) to perform an integrity check on the first S8730 Server:

1. Click Administration > Server (Maintenance), under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, click **All IPSIs, UPS(s), Other server(s), Ethernet switches** and click **Execute Ping**.

   If this ping fails, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300432).
3. Click **Server > Status Summary**.

4. Verify the following:

   Mode: BUSY OUT

   Server Hardware: okay

   Processes: okay
5. Select **Server > Process Status**.
6. Under Frequency, click **Display Once**.
7. Click **View**.
8. Verify all operations are **UP STANDBY**.
9. Telnet to a device outside the server and ping back to the S8730 server.
10. Under IPSI Firmware Upgrades, click **IPSI Version**.
11. Under Query Type, click **Query All** and click **View** to verify connectivity to all IPSIs.

Making the first S8730 Server active

This section describes the procedures you must perform to make the first S8730 Server active.

Shutting down the active S8700, S8710, or S8720 Server

WARNING:
Proceeding with the steps outlined in this section will cause a service interruption if service is being provided by this server.

To connect the Services laptop to the active S8700, S8710, or S8720 Server:

Note:
For this task, ensure that you are on the S8700, S8710, or S8720 Server.

1. Connect the laptop to the Services port (labeled port 2) on the back of the *active* server with a cross-connect CAT5 cable.
2. On the System Management Interface (SMI), under Server, click **Shutdown Server**.
3. Make the following selections:
   - Select **Delay Shutdown**
   - Clear **Restart Server after Shutdown**
   - Select **Shut down even if this is the active server**
4. Click **Shutdown**.
5. On your laptop computer, click **Start** > **Run** to open the **Run** dialog box.
6. Type **`ping -t 192.11.13.6`**. Press **Enter**.
7. When the ping command does not respond, disconnect the server from the Services laptop.

   The LEDs might still be lit.

Accessing the first S8730 Server

To access the first S8730 Server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Connecting to the active server on page 537 and return here.
2. Open a browser and connect to the server.
3. Log in. For more information, see Accessing the System Management Interface (SMI) on page 539.

4. Suppress all alarms.

Releasing the first S8730 Server

To release the first S8730 Server:

Note:
Be prepared for the Access Security Gateway (ASG) challenge and response.

1. On the System Management Interface (SMI), click **Server** > **Release Server**.
2. Click **Release**.

Verifying the first S8730 Server is active

To verify the first S8730 Server is active:

1. On the System Management Interface (SMI), click **Server** > **Status Summary**.
2. Verify the **Mode** field is **Active**.
3. To verify the process status, click **Server** > **Process Status**.
4. Under Frequency, click **Display Once**.
5. Click **View**.
6. Verify all operations are **UP**.

Creating a super-user login

Note:
A craft level login can create the super-user login in Release 4.0 or later.

Make sure you have a login name and password that the customer would like for the superuser login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Use the **Communication Manager System Management Interface (SMI)** to create a super-user login.

To create a login:

Note:
Make sure the customer can change this login, its password, or its permissions later.

1. In the **Communication Manager System Management Interface (SMI)**, under **Security**, select **Administrator Accounts**.
2. Select **Add Login**.
3. Select **Privileged Administrator** and click **Submit**.

   The **Administrator Accounts -- Add Login: Privileged Administrator** screen appears.
4. In the **Login name** field: Type a login name for the account.
5. In the **Primary group** field: susers appears.
6. In the **Additional groups (profile)** field: prof18 appears (*prof18* is the code for the customer superuser).
7. **In the Linux shell** field: /bin/bash appears
8. In the **Home directory field**: /var/home/login name appears (login name is the name you choose in step 4.
9. Skip the **Lock this account** and **Date on which account is disabled-blank to ignore** fields.
10. In the **Select type of authentication section**: Choose **Password**.

    Note:

    Do not lock the account or set the password to be disabled.
11. In the **Enter key or password field** and the **Re-enter key or password** field: Enter the password.
12. In the **Force password/key change on next login section**: Do not check the box.
13. Click **Submit**.

    The system tells the login is added successfully.

Installing the license and authentication files

To install the RFA license file and the Avaya authentication file on the active S8730 Server:

1. To install the license file, click **Security** > **License File**.
2. Select either:
   - **Install the license file I previously downloaded** if you have already downloaded the file to this server, or
   - **Install the license file specified below** and then browse the connected computer for the license file.
3. Click **Submit**.
4. To install the authentication file, click **Security** > **Authentication File**.

5. Select either:
   - **Install the license file I previously downloaded** if you have already downloaded the file to this server, or
   - **Install the license file specified below** and then browse the connected computer for the license file.
6. Click **Install**.

   Note:

   The system responds with a successful message. If you get a filesync failed message, ignore it.

Stopping and starting the ESS servers

If this an ESS server, you must stop the Communication Manager process and then restart it after installing the license file. Doing this ensures that the new RFA license takes full effect.

1. On a server command line interface, run the **`stop -caf`** command.

   The system provides a continuos display of the stop operation. This allows you to determine when the process completes.
2. On a server command line interface, run the **`start -ca`** command.

   The system provides a continuous display of the start operation. This allows you to determine when the process completes.

Verifying server operation

Verify that the following operations work on the new server:

- A station to station call
- An outside call
- An incoming call
- A call that follows a coverage path to voice mail.
  a. Verify that the light on the station comes on after you leave a voice mail message.
  b. Call into voice mail and retrieve the mail message.
  c. Verify that the light goes out after retrieving the voice mail.

Verifying connectivity between the first S8730 Server and port networks, LSPs, and ESS servers

Note:

This procedure is performed on the active main server.

To verify connectivity between the first S8720 and port networks, LSPs, and ESS servers:

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. On the SAT, type **`list sys-link`**. Press **Enter**.
3. Type **`list survivable`**. Press **Enter**.
4. Type **`status ess clusters`**. Press **Enter**.

   If ESS clusters are not registered, follow the normal escalation procedures.
5. Type **`status ess port-networks`**. Press **Enter**.

   If any port networks controlled by an ESS are **down**, type **`get forced-takeover ipserver-interface all`**. Press **Enter**.

   If the port networks are still **down**, follow the normal escalation procedures.

Removing the remaining S8700, S8710, or S8720 Server

This section describes the procedures you must perform to remove the remaining S8700, S8710, or S8720 Server.

Removing the S8700, S8710, or S8720 Server from the rack

To remove the S8700, S8710, or S8720 Server from the rack:

1. Label and disconnect cables.
2. Disconnect the Services laptop.
3. Remove the S8700, S8710, or S8720 Server from the rack.

Removing the DAL2 card, if necessary

Use the procedure found in Appendix B: DAL: Removing or Installing on page 345 > Removing the DAL on page 349 if the S8720 you are migrating from used a DAL2 card and you are reusing the DAL2 card in the S8730

On the second S8730 Server

This section describes the procedures you must perform on the second S8730 Server.

Verifying the DAL2 card

A DAL2 card is required for each S8730 Server using hardware duplication. If you are not using hardware duplication, go to Installing the second S8730 Server in the rack on page 582.

If you are using hardware duplication, verify the type of DAL board that is installed in the server by looking at the label printed on the DAL board. If the S8730 already has a DAL2, go to Installing the second S8730 Server in the rack on page 582. If you need to install a DAL2, use the instructions outlined in Appendix B: DAL: Removing or Installing on page 345.

Installing the second S8730 Server in the rack

To install the second S8730 Server in the rack:

1. Install the slide on the server.
2. Install the rails in the rack.
3. Install the S8730 Server in the rack. For more information, see *Quick Start for Hardware Installation: S8700 Series Servers* (03-300145).

Inserting the Communication Manager software distribution CD

To insert the Communication Manager software distribution CD in the CD/DVD drive S8730 Server:

Note:

You must place the CD in the drive *before* turning on the server.

1. Use a paperclip to open the CD-ROM drive on the server.
2. Insert the Communication Manager software distribution CD in the CD/DVD drive and close the drive door.

Connecting the cables to the second S8730 Servers

To connect the cables to the second server:

Note:

Do not connect the fiber duplication connection cable or the duplication interface IP cable at this time to either S8730 Server

1. The network connections depend on the type of memory duplication and the type of control network being used. Connect the network cables as described in the following table.

Control Network	Software Memory Duplication	Hardware Memory Duplication
Dedicated	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled 1) • CNB (if used) to Eth3 (right top)	• LAN to Eth4 (left bottom) • CNA to Eth0 (middle bottom labeled **1**) • CNB (if used) to Eth3 (right top)
Nondedicated	• LAN/CNA to Eth2 (right bottom) • CNB (if used) to Eth3 (right top)	• LAN/CNA to Eth0 (middle bottom labeled **1**) CNB (if used) to Eth3 (right top)

Figure 47: Duplication and control network cables for hardware duplication

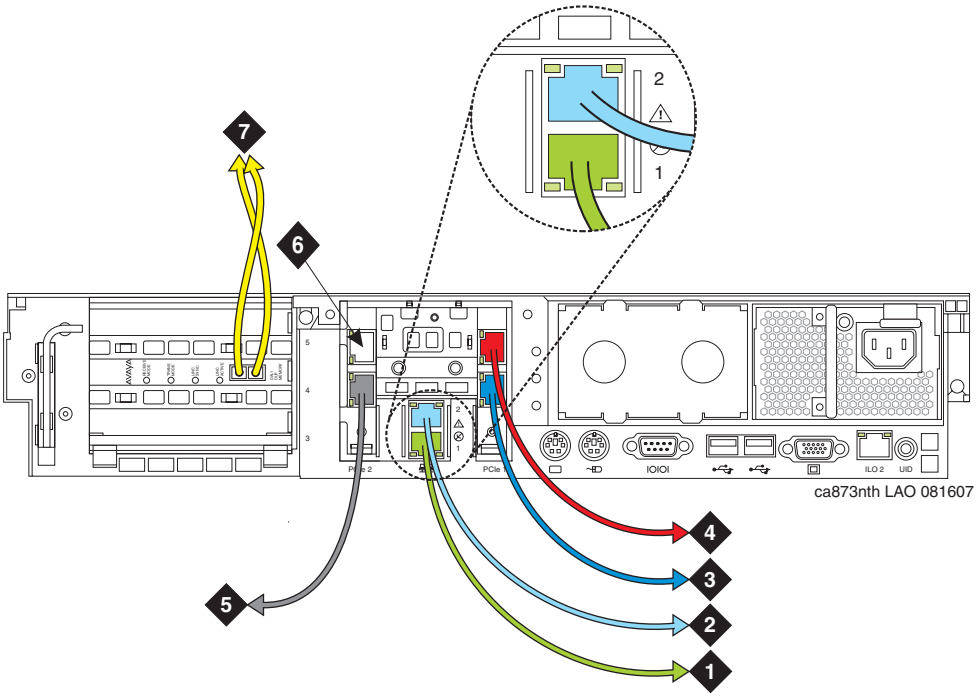


Figure notes:

1. **CNA (also LAN for nondedicated control network)— Eth0**
2. **Services port — Eth1**
3. **Duplication cable (crossover)— Eth2**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**
7. **Fiber duplication cable**

Figure 48: Duplication and control network cables for software duplication

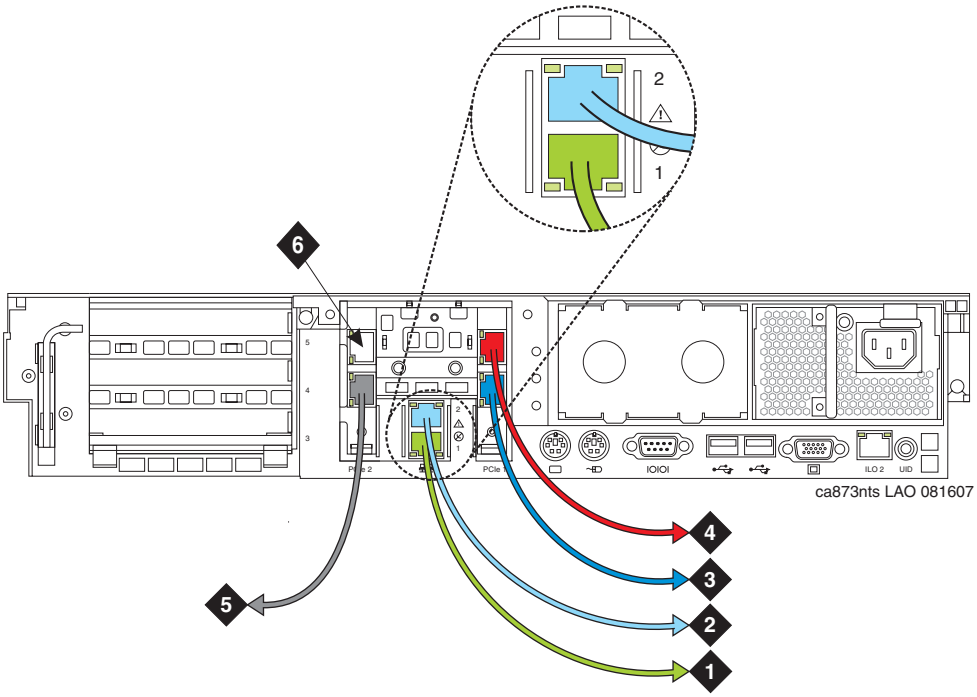


Figure notes:

1. **CNA (also LAN for nondedicated control network) — Eth0**
2. **Services port — Eth1**
3. **Duplication cable (Crossover— Eth2)**
4. **CNB (if used) — Eth3**
5. **LAN (if dedicated control network) — Eth4**
6. **Eth5: not used**

2. Connect the modem to one of the USB ports.
3. Connect the power cord to the rear of the server.
4. To turn on the server, push the yellow button.

   Note:

   Do not connect the USB flash drive at this time.

Accessing the server

To access the server:

1. Clear the ARP cache from the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 230 and return here.

2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. On your laptop computer, click **Start** > **Run** to open the **Run** dialog box,
4. Type **`ping -t 192.11.13.6`**. Press **Enter** to check connectivity between the Services laptop and the server.
5. Wait at least 3 minutes after turning on the server before starting a Telnet session to access the information on the CD.

Installing Communication Manager

Use a telnet session to install Communication Manager.

To install Communication Manager:

1. From the laptop Start menu, click **Start** > **Run**.
2. In the **Run** dialog box, type **`telnet 192.11.13.6`**. Press **Enter** to view the first screen.

Note:

To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

3. Select **Install**, ensure that OK is highlighted and press **Enter**.

4. On the **Select Release Version** window, ensure that the Build line and <OK> are highlighted. Press **Enter** to partition the hard disk and reformat the partitions.

   Once the drive is properly configured, the program starts the installation process and reports the progress.

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

   These processes can take up to 20 minutes. When the server is ready to reboot, the CD-ROM drive drawer opens. You must remove the CD from the drive at this time.

   The reboot can take up to 3 minutes. The telnet session drops automatically.

Insert the USB flash drive in the USB port

Insert the USB flash drive containing the backup in one of the USB ports. It does not matter which USB port you use.

Accessing the second S8730 Server

To access the second S8730 Server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 230 and return here.
2. Open a browser and connect to the server.
3. Log in. For more information, see Accessing the System Management Interface (SMI) on page 539.
4. Suppress all alarms.

Checking the software version

Use the Communication Manager System Management Interface (SMI) to check the software release:

- Under **Server** click **Software Version**

  Verify the release running on the server.

Verifying date and time

Use the Communication Manager System Management Interface (SMI) to change the date and time:

1. Under **Server**, click **Server Date/Time**.
2. Change the date, time, and time zone as needed.
3. To make changes, click **Submit**.

Copying files to the second S8730 Server (if any)

If a software update (service pack) is required, you must copy the update file from the services laptop to the server.

Note:

You do not need to download an RFA license file to this server. The license will shadow over from the other server.

Firmware updates for programmable circuit packs and media modules might also be required. These files might be on the software CD.

Note:

Do not copy the Linux migration upgrade set with this method.

To copy files to the server:

1. On the System Management Interface (SMI), under **Miscellaneous**, select **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the **Choose File** window on your computer.
4. Find the files that you need to copy to the server.
5. Click **Download** to copy the file(s) to the server.

   The system automatically copies the files to the default location on the server.

Installing security and service pack updates, if any

Use this procedure to unpack and active the files that you copied in the previous step.

1. Under **Server Upgrades**, select **Manage Updates**.
2. If an update file you want to activate shows **packed** in the **Status** column:
   a. Select **update ID**
   b. Click **Unpack**
3. Wait until the system displays the message **Unpacked Successfully..** and then click **Continue**.

   The system displays the **Manage Updates** screen.
4. If the update ID you want to activate shows **unpacked** in the **Status** column:
   a. Select the **update ID**
   b. Click **Activate**

      The screen shows the status of activating the update. If a reboot or restart of Communication Manager is required, the system automatically reboots or restarts Communication Manager.
5. Click **Yes**.

   Wait until the system displays the **Continue** button.
6. Click **Continue**.

   The system displays the status of the update.

Stopping Communication Manager on the second S8730 Server

To stop Communication Manager:

- Type **`stop -acf`**. Press **Enter** to stop Communication Manager.

The system provides a continuous display of the stop operation.

Configuring to allow restoring configuration data and translations from a server on the network

Important:
If you backed up files to the USB-connected Compact Flash, do not perform this procedure. Go to Configuring to allow restoring configuration data and translations from the USB flash card on page 568.

If you backed up to the customer network, you must readminister the Ethernet port connecting to the network. You must have the host name, IP address, subnet mask and default gateway for the two servers and the active server and the IP address for the Ethernet port connecting to the customer's network.

To configure the network parameters:

1. Under Server Configuration, click **Configure Server** to open the first page of the Configure Server process.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure individual services**. Click **Continue**.
4. Click **Set Identities** from the main menu.
5. On the **Set Identities** window:
   - In the **Host Name** fields, fill out the host names for each server.
   - In the **This is server number** field, select the appropriate number. For example, if you are on server 1, select **1**.
   - Assign the Ethernet ports. Click **Continue**.

6. In the **Configure Interfaces** window, fill in the correct IP addresses, Gateway, and Subnet mask only for the Ethernet port connected to the customer LAN. Select the speed **AUTOSENSE** for all the Ethernet interfaces

   Click **Change** to update the server. When the screen shows

   Successfully configured ethernet interfaces.

   The Ethernet ports are configured.
7. Click **Close Window** to close the Configure Server wizard.

Verifying connectivity to the network server

To verify that the Ethernet port is working, ping from the S8730 Server to the network server where the backup files are stored.

Note:

You might need to restart your browser before doing the next steps.

1. Under **Diagnostics**, click **Ping**.
2. Select Host Name or IP Address and type the IP address of the server where the system files are stored.
3. Click **Execute Ping**.

   If you can successfully ping the server, you can proceed to restore the backed up sets of files.

Configuring to allow restoring configuration data and translations from the USB flash card

If you backed up to the USB flash card, you must configure the server type, name, and the number to prepare for the restore procedure. Keep to these instructions and ***do not*** make any other changes.

To configure to allow restoring configuration data and translations from the flash card:

1. Under **Server Configuration**, click **Configure Server.**
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure individual services**. Click **Continue**.
4. Click **Set Identities** from the main menu.
5. On the **Set Identities** window:

a. In the **Host Name** fields, fill out the host names for each server.

b. In the **This is server number** field, select the appropriate number. For example, if you are on server 1, select **1**.

c. Click **Continue**.

6. In the **Configure Interfaces** window:

a. Select the speed **AUTOSENSE** for ***all*** the Ethernet interfaces.

b. Click **Change** to update the server.

c. When the screen shows

Successfully configured ethernet interfaces.

Click **Close Window** to close the Configure Server wizard.

Restoring configuration data and translations to the second S8730 Server

Note:

The physical connections to the Ethernet ports must match the server configuration assignments that were backed up in Backing up the active S8700, S8710, or S8720 Server on page 543. The connections to the Ethernet ports that do not match the configuration can prevent access to the server.

The restore method depends on how you backed up the data. Currently there are two ways to restore backed up data.

- Restoring data based up to the Compact Flash card (applicable only if migrating from an S8710 Server)
- Restoring data backed up to the customer network (applicable only if migrating an S8700, S8710, or S8720 Server)

In Table 31, the restore procedure is dependent on what backup method was used.

Table 31: Migration to S8730, Release 5.x or later, using Web interface, View/Restore

S8700, S8710, S8720		File Name of Backup
Release	**Load**	
1.2	02.0.110.4	upgrade...tar.gz.
1.3	03.0.526.5	upgrade...tar.gz.
1.3.1	03.1.531.0	upgrade...tar.gz.

Table 31: Migration to S8730, Release 5.x or later, using Web interface, View/Restore

S8700, S8710, S8720		File Name of Backup
Release	**Load**	
1.3.2	03.2.536.1	upgrade...tar.gz.
2.0	00.0.219.0	upgrade...tar.gz.
2.0.1	00.1.221.1	upgrade...tar.gz.
2.1	01.0.411.7	upgrade...tar.gz.
2.1.1	01.1.414.1	upgrade...tar.gz.
2.2	02.0.111.4	upgrade...tar.gz.
2.2.1	02.0.118.0	upgrade...tar.gz.
2.2.2	02.2.122.0	full...tar.gz.
3.0	00.0.340.3	full...tar.gz.
3.0.1 and later	00.1.346.0 and later	full...tar.gz.

Restoring data backed up to the Compact Flash card

Note:

This procedure is applicable only if migrating from an S8710 Server.

Use the Communication Manager System Management Interface (SMI) to restore data based up to the Compact Flash card:

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. Click **Local PC Card**.
3. Click **View**.
4. In the **View/Restore Data Results** window:
   a. Select the file name to restore
   b. Select both force options.

   For example, the file might be called full_*custservname*_timestamp_datestamp.tar.gz where *custservname* is the customer server name from which Communication Manager is backed up.
5. Click **Restore**.
6. Click **Check Status** to view the restore progress.

Restoring data backed up to the customer network

To restore data backed up to the customer network from S8700, S8710, or S8720 Servers:

1. On the System Management Interface (SMI), click **View/Restore Data**.
2. Under the **View current backup contents in section**, click **Network Device**.

   Note:
   SFTP or SCP are also available.
3. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** - enter the host IP address
   - **Directory** (for SFTP and FTP)
   - **File Path** (for SCP)
4. In the Method section, select the method such as ftp.
5. Click **View**.
6. In the **View/Restore Data Results** window, select the file name to restore and select both force options.

   For example, the file could be called full_*custservname*_timestamp_datestamp.tar.gz where *custservname* is the customer server name from which Communication Manager is backed up.
7. Click **Restore**.
8. Click **Refresh** view the restore progress.

Verifying the second S8730 Server configuration

Use this step to verify the configuration information and to make any necessary changes:

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** through the Review Notices to get to the **Specify how you want to use this wizard** page.
3. Select **Configure all services using the wizard**. Click **Continue**.
4. On the **Set Identities** page, under the Select Server Duplication area, select either:
   - **This is a duplicated server using duplication hardware**
   - **This is a duplicated server using software-based duplication**
   - **This is a duplicated server using encrypted software-based duplication**

Note:

The physical connections to the Ethernet ports are different for hardware duplication and software duplication. For more information, see Connecting the cables to the first S8730 Server on page 559.

5. Click **Continue**.
6. On the **Configure Interface** page, set the speed for all Ethernet ports to **AUTOSENSE**.

   Note:

   You must click through all the screens whether there are changes or not.

7. On the **Configure ESS** window:
   - If the server is a primary control main, click **This is NOT an enterprise survivable server**
   - If the server is an ESS server, click **This is an enterprise survivable server (ESS)**
8. Click **Continue**.
9. When you complete all the new fields, click **Continue** on the **Update System** screen. The Update System screen shows each configuration task as the task completes. When done, the screen shows the line **All configuration information was entered**.
10. Click **Close Window**.

Configuring the Processor Ethernet interface (on the ESS)

Perform this task if you are migrating from an ESS running Communication Manager Release 5.1.x or prior to an S8730 ESS running Communication Manager 5.2 or later.

1. Under **Installation**, click **Configure Server** and follow the instructions on the wizard. Alternatively, you can configure services individually. For more information, see the online help available with the SMI.
2. On the **Set Identities** page, verify that PE is assigned to the same NIC as the corporate LAN.
3. On the **Configure Interfaces** page, assign an IP-alias address for the PE interface of the duplex ESS. PE must be assigned to the same NIC as the corporate LAN. The IP-alias address is assigned in the **Active server** field.
4. Submit the change and exit from the Configure Server wizard.

Confirming the product ID on the second S8730 Server

To confirm the Product ID:

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **`craft`** or **`dadmin`**.
3. At the prompt, type **`productid`**.
4. Press **Enter**.

   The **`productid`** should match the value record in Obtaining the Product ID on the active server on page 548. If value does not match, escalate the problem immediately.

Enabling CNC, if necessary

If the CNC status in Checking the CNC status on page 543 is **Control Network C has been configured**, do this procedure. Otherwise, go to Rebooting the second S8730 Server on page 596.

If the system uses Control Network C (CNC):

- Type **`cnc on`**.
- Press **Enter**.

Rebooting the second S8730 Server

Reboot is necessary to initialize server settings that are restored but not yet activated.

To reboot the second S8730 Server:

1. On the System Management Interface (SMI), under Server, click **Shutdown Server**.
2. Make the following selections:
   - Select **Delay Shutdown**
   - Select **Restart Server after Shutdown**
3. Click **Shutdown**.

   Wait approximately three minutes.

Accessing the second S8730 Server

To access the second S8720 Server:

1. Open a browser and connect to the server.
2. Log in. For more information, see Accessing the server command line interface with ssh protocol on page 228.
3. Suppress all alarms.

Performing an integrity check on the second S8730 Server

To perform an integrity check on the second S8730 Server:

1. On the System Management Interface (SMI), under Diagnostics, click **Ping**.
2. Under Endpoints to Ping, click **All IPSIs, UPS(s), Other server(s), Ethernet switches** and click **Execute Ping**.

   If this ping fails, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300432).
3. Click **Server** > **Status Summary**.
4. Verify the following:

   Mode: BUSY OUT

   Server Hardware: okay

   Processes: okay
5. Select **Server > Process Status**.
6. Under Frequency, click **Display Once**.
7. Click **View**.
8. Verify all operations are **UP STANDBY**.
9. Telnet to a device outside the server and ping back to the S8730 Server.
10. Under IPSI Firmware Upgrades, click **IPSI Version** (main server only).
11. Under Query Type, click **Query All** and click **View** to verify connectivity to all IPSIs (main server only).

Connecting the duplication cables

To connect the duplication cables:

- Connect the duplication cables as described in the following table.

Control Network	Software Memory Duplication See Figure 50	Hardware Memory Duplication (see Figure 49)
Dedicated	• Duplication to Eth0 (on server, labeled **1**)	• Duplication to Eth2 (1st from left on quad NIC) • Fiber to DAL2 card

Figure 49: S8730 duplication and control network cables for hardware duplication

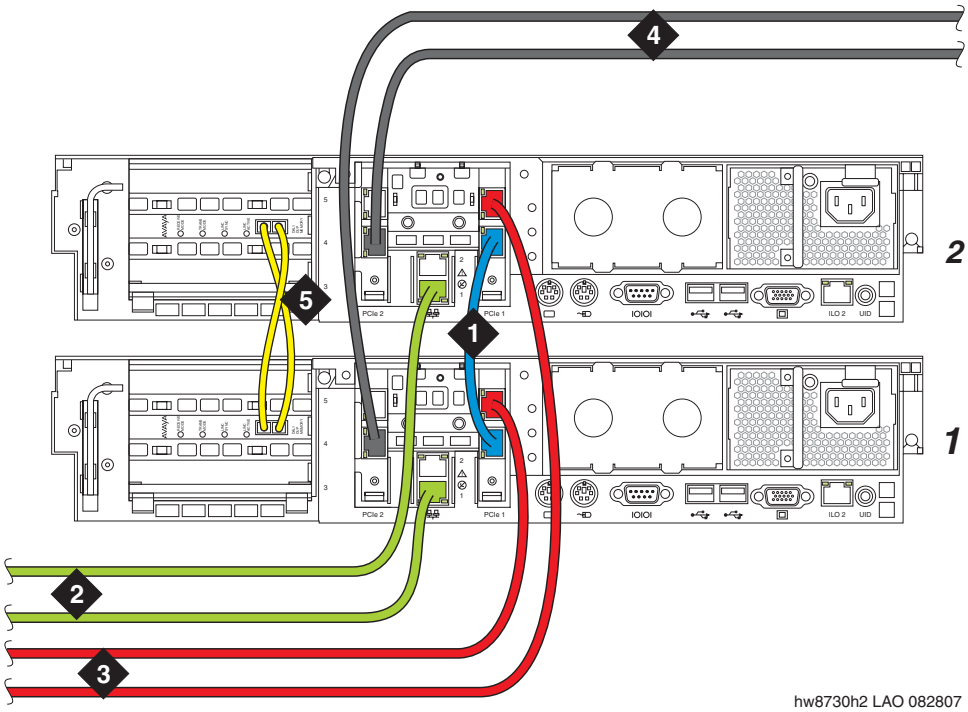


Figure notes:

1. **Server duplication link - duplication crossover cable — Eth2**
2. **CNA (also LAN for nondedicated control network) — Eth0**
3. **CNB (if used) — Eth3**
4. **LAN (if dedicated control network) — Eth4**
5. **Fiber duplication cable**

Figure 50: S8730 duplication and control network cables for software duplication

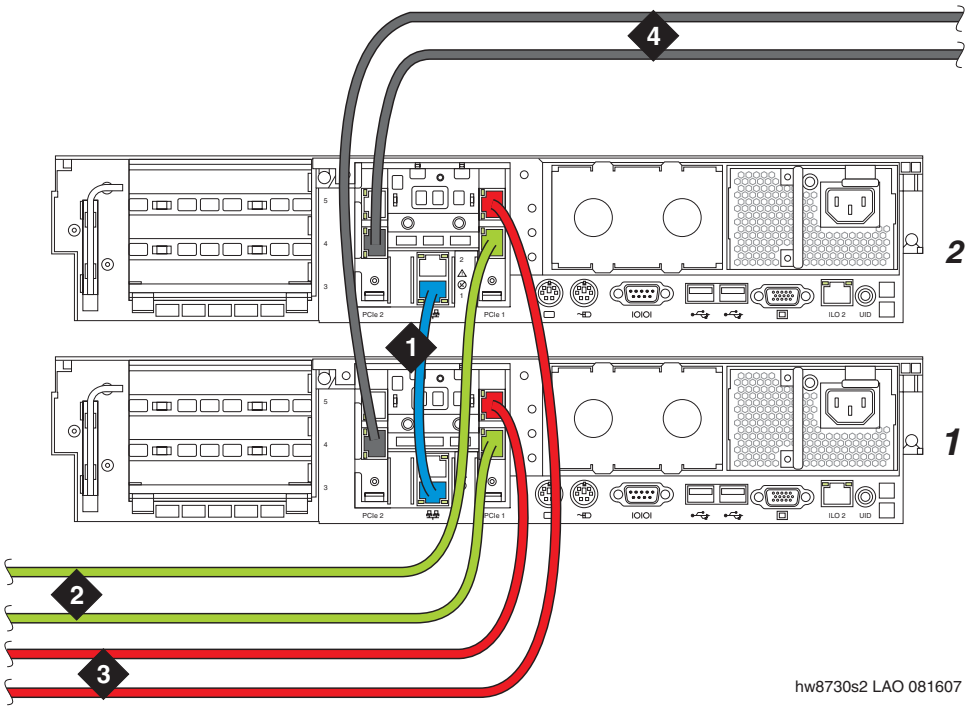


Figure notes:

1. **Duplication cable (Crossover) — Eth0**
2. **CNA (also LAN for non-dedicated control network) — Eth2**
3. **CNB (if used) — Eth3**
4. **LAN (if dedicated control network) — Eth4**

Releasing the second S8730 Server

To release the second S8730 Server:

1. On the System Management Interface (SMI), click **Server** > **Release Server**.
2. Click **Release**.

Verifying the second S8730 Server is in standby state

To verify the second S8730 Server is in a standby state:

1. On the System Management Interface (SMI), click **Server** > **Status Summary**.
2. Verify the **Mode** field is **Standby**.

3. Check the following:
   - Standby Busied is **no**
   - Standby Refreshed is **yes**
   - Standby Shadowing is **on**
4. To verify the process status, click **Server** > **Process Status**.
5. Under Frequency, click **Display Once**.
6. Click **View**.
7. Verify all operations are **UP Standby**.

Setting Server A/Server 1 active for ESS, if necessary

Skip this task if the servers you are migrating are S8700-Series Server configured as main servers.

Note:

Perform this task after you have migrated from an ESS running Communication Manager Release 5.1.x or prior to an S8730 ESS running Communication Manager 5.2 or later; and before you upgrade the MAIN Server from Communication Manager Release 5.1.x to Communication Manager Release 5.2 or later.

Note:

The term Server A refers to one of the two servers in a duplicated ESS. An S8700-Series ESS that is running on Communication Manager Release 5.2 or later will register and filesync to the main server running Communication Manager Release 5.1.x or prior, only if the Server A of the ESS is active. Typically, Server A will be the Server 1 as identified in the **ID** field in the output of the CLI command **server**, or in the **ID** field in the output of the **Server > Status Summary** screen in the SMI.

To interchange the servers, if necessary:

1. Access the System Management Interface (SMI) of the standby ESS.
2. Under **Server**, click **Interchange Servers.**
3. Click **Interchange**

The system displays a confirmation message that the interchange has taken place. This server is now the active server.

Administering the node name for the IP-alias address for the duplicated ESS servers (after ESS upgrade and pre-upgrade Main)

Skip this task if the servers you are migrating are S8700-Series Server configured as main servers.

Note:

Perform this task after you have migrated a duplicated ESS server from Communication Manager Release 5.1.x or prior to Communication Manager Release 5.2 or later, and before you migrate the MAIN Servers from Communication Manager Release 5.1.x to Communication Manager Release 5.2 or later.

At the SAT of the MAIN Server:

1. Type **`change node-names ip xxx`** and press **Enter**, where **`xxx`** is the node name of the Active Server IP Address (IP-alias) of the duplicated ESS servers.

   If the node name already exists, confirm that the IP Address is correctly matching the PE Active Server IP Address (IP-alias) of the duplex ESS; press Cancel to exit the node-names screen, skip to step 5.

   If the node name xxx does not exist, add a new node name, using steps 2-4.

   CAUTION:

   Choose this node name carefully. If you need to change it after the migration, you must delete the ESS and readminister it. Do not delete or re-use the node name for server A because you will need this node name later, when you migrate the main server.

2. *(for new node name only)* In the **Name** field, enter the node name.
3. *(for new node name only)* In the **IP Address** field, enter the PE Active Server IP Address of the duplex ESS.
4. *(for new node name only)* submit your changes to the node-names screen.
5. Type change **`system-parameters ess`** and press **Enter**.
6. Administer the node name of Server A by the node name that you defined for the PE interface of the duplex ESS for the ESS server that you are changing.
7. Type save translation all and press **Enter**.
   The ESS server registers with the main server and receives filesyncs.

Administering the node name for Server A (main server only)

Skip this task if the servers you are migrating are S8700-Series ESS.

Note:

Perform this task after you migrate the S8700-Series main servers from Communication Manager Release 5.1.x or prior to Communication Manager Release 5.2 or later; and if the main has administered Survivable Servers of Type “ESS D” as observed on the list survivable-processor screen.

Note:

The **system-parameters ess** screen is no longer available after the migration to Communication Manager Release 5.2 or later. The translation data that was held in **system-parameters ess** screen is now located in the **survivable-proccessor** screen.

The Server A node name in the System Parameters ESS SAT screen of the pre-upgrade main is transferred to the ACTIVE SERVER IP Address field in the Survivable Processor SAT screen of the migrated main. The SERVER A Node Name is set to blank in the Survivable Processor screen. Because the node name for Server A is blank on the Survivable Processor Screen, an alarm (ESS alarm 799) is generated on the main server.

At the SAT of the MAIN Server:

Tip:

Run the **`list survivable-processor`** command and search for **ESS D** to locate the servers that need administering.

1. Type **`change survivable-processor`** ***`New-node-name`*** and press **Enter**.

   Where ***`New-node-name`*** is the node name assigned to the ESS. The node name can be determined from the **list survivable-processor** screen.

2. Administer the node name of the ESS server A.

   The alarm clears after the Server A node name is administered for the duplex ESS.

Releasing alarm suppression (optional)

If you complete the migration well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait.

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **craft** or **dadmin**.

3. Type **`almsuppress -s n`**. Press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the second S8730 Server

Disconnect the Services laptop from the second S8730 Server.

On the active (first) S8730 Server

This section describes the procedures you must perform on the active (first) S8730 Server.

Accessing the active server

To access the active server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Connecting to the active server on page 537 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. Log in. For more information, see Accessing the System Management Interface (SMI) on page 539.

Resolving alarms

To resolve alarms:

1. Under Alarms and Notification, click **Current Alarms**.
2. Select the server alarms to be cleared. Click **Clear**.
3. Resolve new alarms since the migration with SAT commands. For more information, see:

- *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*
- *Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers*

Enabling scheduled maintenance

To schedule daily maintenance:

- Reset the settings that were recorded in Disabling scheduled maintenance on page 541.

Saving translations

To save translations:

- Type **`save translation all`**. Press **Enter**.

  If this operation is unsuccessful, follow the normal escalation procedures before continuing.

Backing up files on the active S8730 Server

To back up files on the active server:

1. Under Data Backup/Restore, click **Backup Now**.
2. Under Data Sets, click **Full Backup**.
3. Under Backup Method, select the backup method.
4. Click **Start Backup** to start the back up process.

Releasing alarm suppression (optional)

If you complete the migration well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait.

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **craft** or **dadmin**.
3. Type **`almsuppress -n`**. Press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the active S8730 Server

Disconnect the Services laptop from the active server.

On the standby S8730 Server

This section describes the procedures you must perform on the standby S8730 Server.

Accessing the standby server

To access the standby server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 230 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. Log in. For more information, see Accessing the System Management Interface (SMI) on page 539.

Resolving alarms

To resolve alarms:

1. Under Alarms and Notification, click **Current Alarms**.
2. Select the server alarms to be cleared. Click **Clear**.

Backing up files on the standby S8730 Server

To back up files on the standby server:

1. Under Data Backup/Restore, click **Backup Now**.
2. Under Data Sets, click **Full Backup**.
3. Under Backup Method, select the backup method.
4. Click **Start Backup** to start the back up process.

Releasing alarm suppression (optional)

If you complete the migration well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait.

1. Use the PuTTY application to reaccess the server with the secure shell (SSH) protocol.
2. Log in as **craft** or **dadmin**.
3. Type **`almsuppress -n`**. Press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the standby server

Disconnect the Services laptop from the standby server.

Completing the migration

This section describes the procedures you must perform to complete the migration.

Registering the system

Follow the existing process and procedures to register the S8730 Server.

Removing customer files from the Services laptop

Remove the customer Linux migration *upgrade* set from the services laptop.

Interchanging servers (optional)

This section describes the procedures you must perform to interchange the servers.

Accessing the standby server

To access the standby server:

1. Clear the ARP cache on the laptop if necessary. For more information, see Clearing the ARP cache on the laptop computer on page 230 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. Log in. For more information, see Accessing the System Management Interface (SMI) on page 539.

Interchanging servers (optional)

To interchange the servers to check capability of the standby server to become the active server:

1. Under Server, click **Interchange Servers**.
2. Verify the settings in the following fields:
   - **Standby Busied**: no
   - **Standby Refreshed**: yes
   - **Standby Shadowing**: on
   - **Duplication Link**: up
3. Click **Interchange**.

   The system displays a confirmation message that the interchange has taken place.

   This server is now the active server.

Performing an integrity check on the active S8730 Server

To perform an integrity check on the active S8730 Server:

1. On the System Management Interface (SMI), under Diagnostics, click **Server** > **Status Summary**.

2. Verify the following:

   Mode: Active

   Server Hardware: okay

   Processes: okay
3. Select **Server** > **Process Status**.
4. Under Frequency, click **Display Once**.
5. Click **View**.
6. Verify all operations are **Up STANDBY**.

Appendix A: Accessing the server

You must have access to the server for administration. The following computers and software are the supported access points for accessing the server for initial configuration, aftermarket additions, and continuing maintenance:

- Personal computers.
- Services laptop computers equipped with a network interface card (NIC).
- Terminal emulation program.
- Web browser.

You can access the server either directly or remotely over the customer network or over a modem. Connecting directly and remotely over the customer network are the preferred methods. Remote access over a modem is for Avaya maintenance access only.

Connecting to the server directly

To access the server directly, plug a laptop computer into the services port on the server.

- On the S8300 Server plug the CAT5 cable into the services port on the front as shown in Figure 51: A services laptop computer that is connected directly to the S8300 Server on page 612.
- On the S8500 Server, as shown in Figure 52: A services laptop computer that is connected directly to the S8500 Server on page 613, and the S8700-series Server, as shown in Figure 53: A services laptop computer that is connected directly to the S8700 Server on page 614, plug one end of a crossconnect CAT5 cable into the services port. This port defaults to port 2 (Eth1), On the back of the server, plug the other end into the NIC on your computer. You might need a NIC adapter.

For more information about connectivity for your server, see

- Figure 51: A services laptop computer that is connected directly to the S8300 Server on page 612
- Figure 52: A services laptop computer that is connected directly to the S8500 Server on page 613
- Figure 53: A services laptop computer that is connected directly to the S8700 Server on page 614
- Figure 54: A services laptop computer that is connected directly to the S8710 Server or S8720 Server (S8710 Server shown) on page 615.

- Figure 55: A services laptop computer that is connected directly to the S8730 Server on page 616

Figure 51: A services laptop computer that is connected directly to the S8300 Server

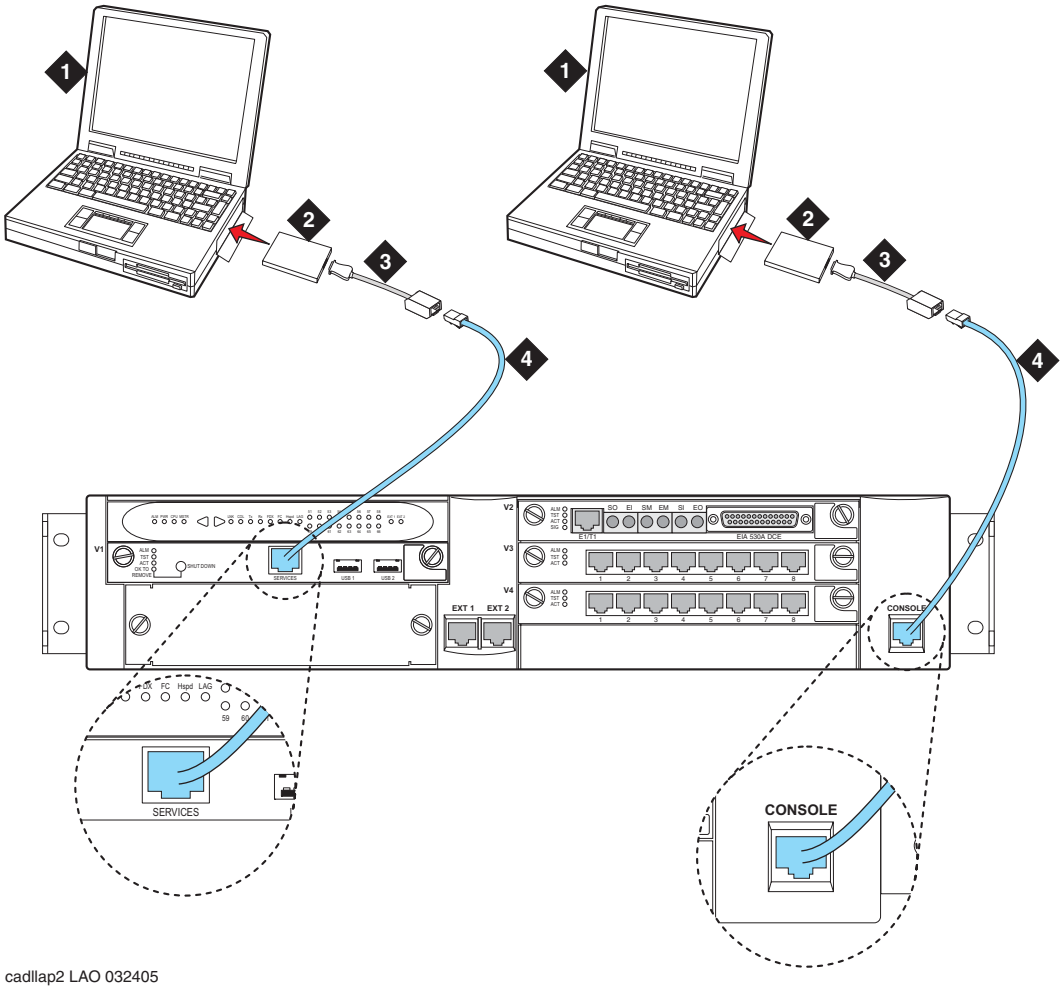


Figure notes:

1. Services laptop
2. Network interface card (NIC)
3. NIC adapter cable (if necessary)
4. Black CAT5 cross-connect cable

Figure 52: A services laptop computer that is connected directly to the S8500 Server

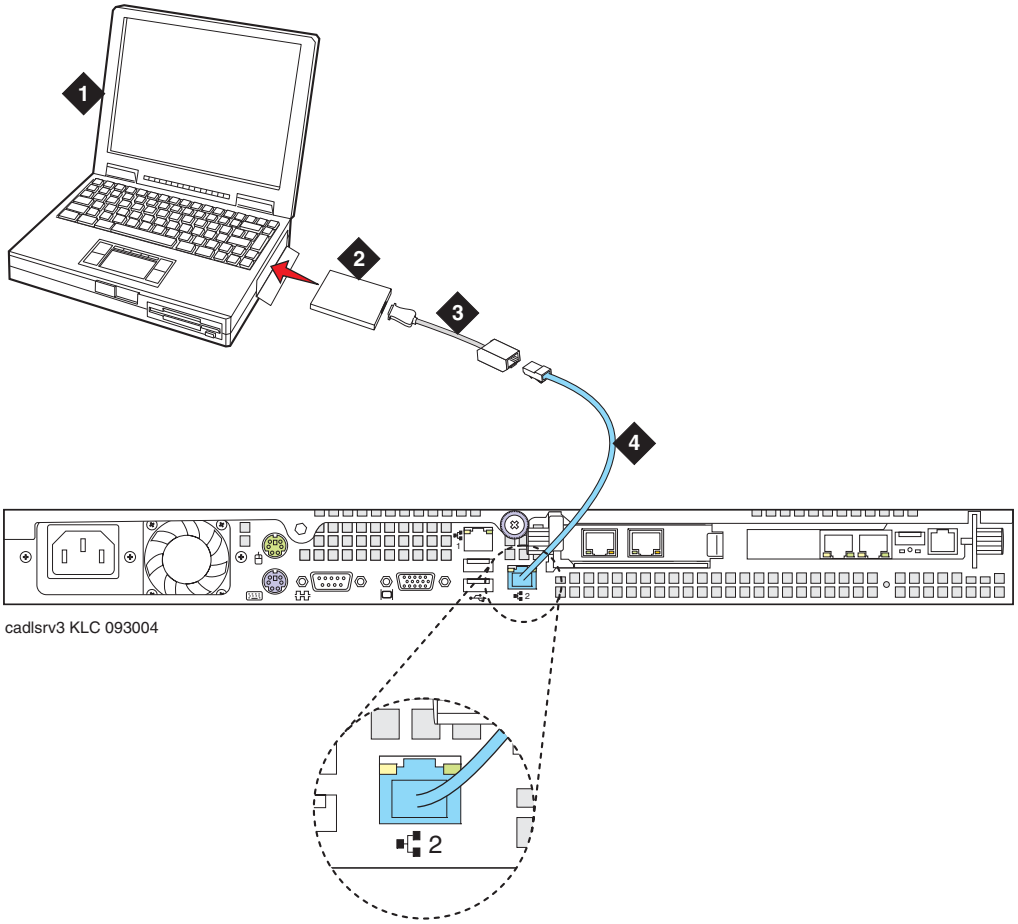


Figure notes:

1. Services laptop
2. Network interface card (NIC)
3. NIC adapter cable (if necessary)
4. Black CAT5 cross-connect cable

Figure 53: A services laptop computer that is connected directly to the S8700 Server

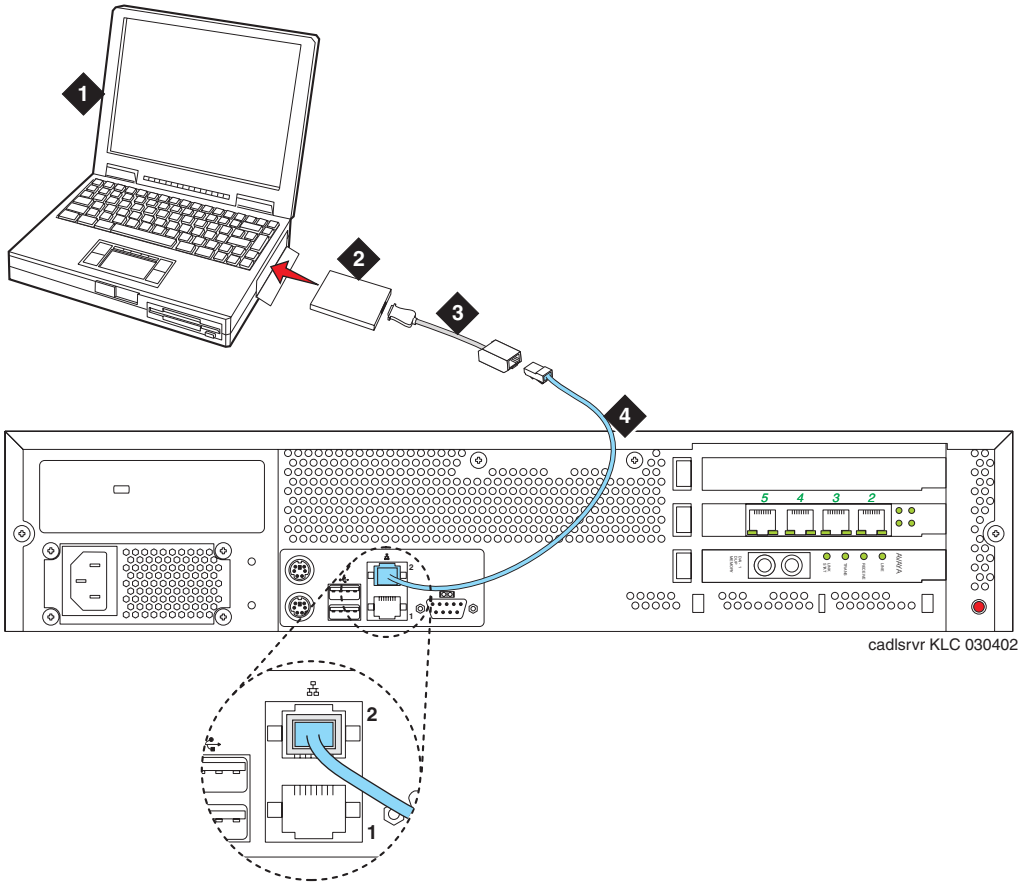


Figure notes:

1. Services laptop
2. Network Interface Card (NIC)
3. NIC adapter cable (if necessary)
4. Black CAT5 crossconnect cable

Figure 54: A services laptop computer that is connected directly to the S8710 Server or S8720 Server (S8710 Server shown)

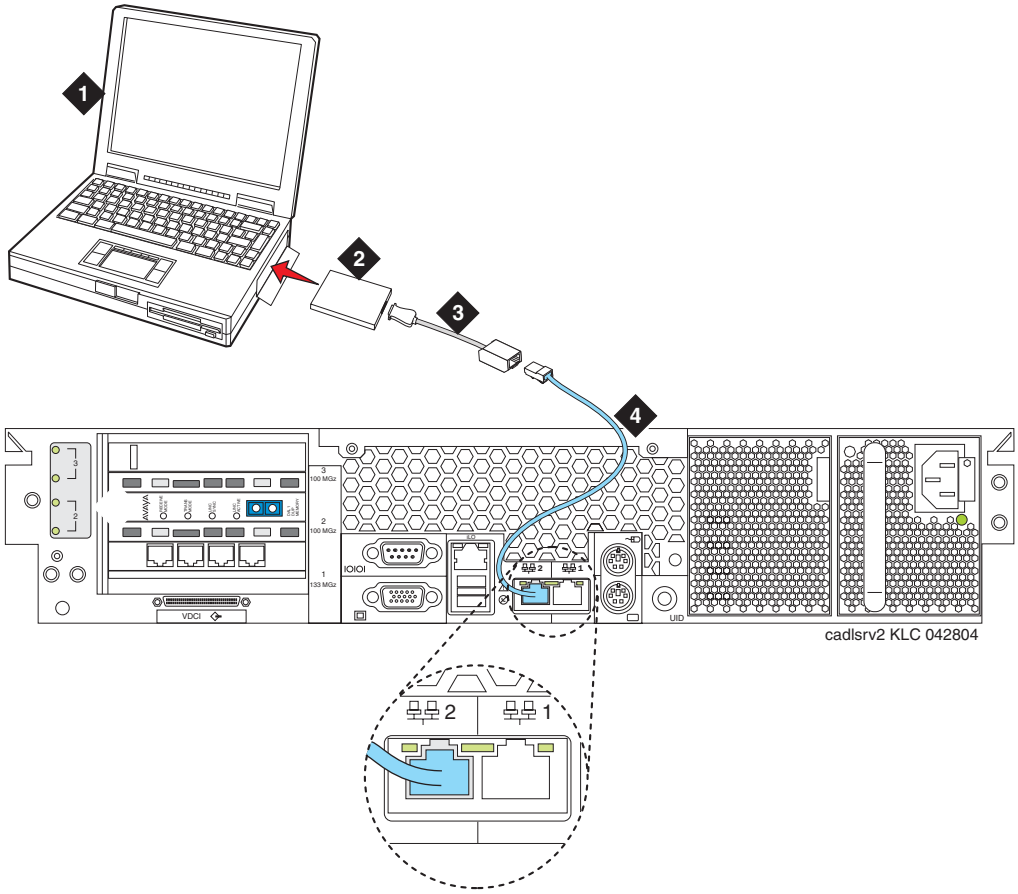


Figure notes:

1. Services laptop
2. Network Interface Card (NIC)
3. NIC adapter cable (if necessary)
4. Black CAT5 crossconnect cable

Figure 55: A services laptop computer that is connected directly to the S8730 Server

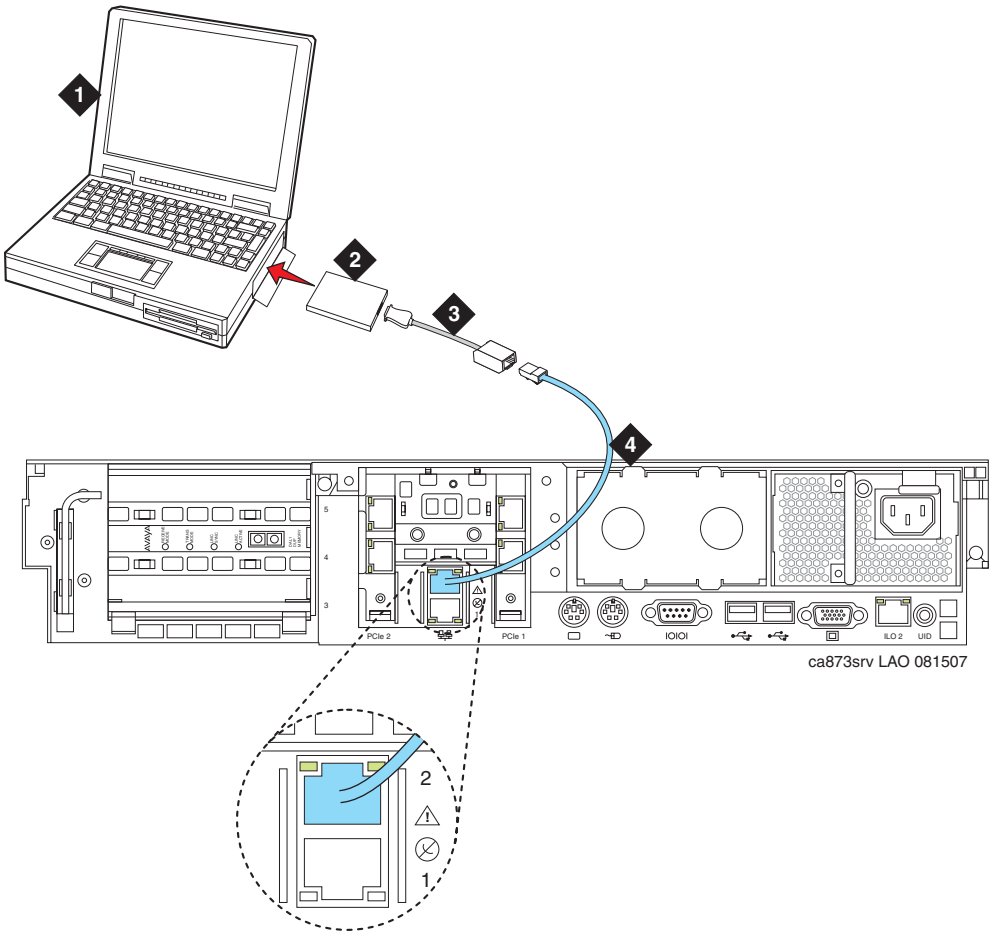


Figure notes:

1. Services laptop
2. Network Interface Card (NIC)
3. NIC adapter cable (if necessary)
4. Black CAT5 crossconnect cable

Connecting the G700 Media Gateway directly

To access the G700 Media Gateway directly, you plug a laptop computer into the Console port on the media gateway. Plug one end of the CAT5 cable into the services port on the front of the media gateway. Plug the other end into the NIC on your computer. For more information about connectivity for your server, see Figure 51: A services laptop computer that is connected directly to the S8300 Server on page 612.

Computer specifications

The computer that you use to access the server must have the following minimum specifications:

- Windows 2000 or Windows XP operating system
- 32-MB of RAM
- 40-MB of available disk space
- An RS-232 port connector
- A Network interface card (NIC) with a 10/100BaseT Ethernet interface
- A 10/100 BaseT Ethernet, CAT5 or better, cross-connect cable with an RJ45 connector on each end (MDI to MDI-X)
- CD-ROM drive

Network configuration

You also must configure your network connection. For more information, see Network configuration on page 623.

The network connection for the computer has the following TCP/IP properties:

- IP address: 192.11.13.5
- Subnet mask: 255.255.255.252

After you connect the computer to the network, you can administer the server through these interfaces:

- The System Management Interface (SMI) for server-specific administration.
- A command line interface in a Telnet or terminal emulation application for Linux and SAT commands, respectively. For duplicated servers, you can use the SAT commands on the active server only.

For more information, see Accessing the System Management Interface (SMI) on page 619.

Connecting to the server remotely over the network

You can access the server from any computer that is connected through the LAN. However, the LAN security settings must allow remote access.

To access the server, open a Web browser or a terminal emulation application. In the address field, type the IP address or the DNS host name that is assigned to the server you want to access.

For duplicated servers, you can use the **active (alias)** server address to connect automatically to the server that is active.

Connecting to the server remotely over a modem

Note:

Remote access over a modem is for Avaya services support access only and not for routine administration. Because the server uses the same line to report alarms, the server cannot report new alarms while the line is in use.

You can access the server through an analog modem. The remote connection requires a data speed of at least 33.5 kilobits per second.

On the S8500-Series Server, you access the server through the remote maintenance board that is installed in the server. For more information about how to access the SAMP, see the *Using the Avaya Server Availability Management Processor (SAMP)* (03-300322).

Setting up a dial-up connection

To use a computer modem, you first must set up your dial-up connection.

1. Start the dial-up connection program, which varies depending on your operating system. Usually, you can access a dial-up connection program from the My Computer or the Control Panel folders. For more information, see the Help system on your computer.
2. To open the New Connection wizard, double-click **Make New Connection**.
3. Within the wizard, and depending on your operating system, you might be asked to:
   - Assign a name to the connection.
   - Select dial-up to the network for the network connection type.
   - Select the modem that you use for a dial-up connection.

- Type the appropriate telephone number to access the active server. For more information about the customer-supplied telephone numbers, see the completed *Electronic Preinstallation Worksheet*.
- Under Advanced, select **PPP** and log on manually. You might have to type a user name and a password. This entry depends on whether the server you are dialing into has a non-null CHAP secret key. If you must type a user name and a password, use **craft** as the user name and ignore the Password field.

Dialing up to the server

To dial up, click the connection name or the icon, if you created an icon when you set up the connection. Once you are connected:

1. When prompted, enter your remote access login name and password.
2. When you see the **Start PPP now!** message, click **Done**. When you see the Connection Complete dialog box, your computer is connected to the server.
3. To open an SSH session, see Using the command line interface on page 620.

Finding the IP address of the active server (duplicated servers)

To find the IP address of the active server in a configuration with duplicated servers:

1. Go to the task bar at the bottom right of your PC screen.

2. Right-click the Network Status icon. Click **Status**, and then click the **Details** tab.
3. Scroll down until you see the Server IP address. This IP address is for the server to which you are connected.

Accessing the System Management Interface (SMI)

To access the System Management Interface. You can either connect:

- Directly to the services port on the server. For more information, see Connecting to the server directly on page 611.
- Over the customer network.

MS Internet Explorer 5.0 or 6.0 is the only browser that is supported.

When you connect *directly* to the server, you must disable all proxy servers. For more information and instructions, see Browser settings on page 624.

To access the System Management Interface (SMI):

1. Open the MS Internet Explorer Web browser.
2. Perform one of the following actions:
   - If you want to connect directly, in the **Address** field, type **`192.11.13.6`**.
   - If you want to connect remotely, in the **Address** field, type the IP address or the DNS host name of the server.
3. When prompted, log in.

Using the command line interface

Accessing the server command line interface with ssh protocol

Note:

Using the ssh protocol to access the server is applicable to Communication Manager Release 3.0 and later.

To use this procedure with a laptop cable connection to the services port, you must configure your laptop for the network connection. In addition, a third-party ssh client must already be installed on your computer.

For more information on Network Configuration, see *Converting Avaya Servers and Media Gateways*, 03-602884.

PuTTY is one such client available for download from http://www.putty.nl/download.html. The following procedure describes, as an example of ssh access, how to log into the server command line with PuTTY.

Note:

A version of PuTTY that is defaulted for ssh server access is available for Avaya services personnel only. In this version, some values below have already been pre-selected.

CAUTION:

While a variety of Avaya products support access using ssh, Avaya does not provide support for third-party clients used for ssh access. Any problems with an ssh client, including PuTTY, are the responsibility of the user or the ssh client vendor.

To access the command line interface using PuTTY with ssh:

1. On your computer, click on the **PuTTY** desktop link or select **Start** > **Programs** > **PuTTY** > **PuTTY**.
2. In the **Host Name (or IP address)** field, type **`192.11.13.6`** if connecting to the services port. Otherwise, for access over the LAN/WAN, type the IP address or the host name of the server.
3. In the **Port** field, type **22** (the SAT is **5022**).
4. Under Protocol, select **SSH**.
5. In the PuTTY menu on the left, click **Connection** > **SSH**.

   The Options controlling SSH connections dialog box opens.
6. In the **Preferred SSH protocol version** field, select **2**.
7. In the **Encryption options** window, use the up and down arrows to set **AES (SSH-2)** as the top option and **3DES** as the second option.

   Note:

   You can save the PuTTY settings and customize the PuTTY tool with other settings, such as for color. For documentation on PuTTY, see http://www.putty.nl/docs.html.
8. In the PuTTY menu on the left, click **Terminal** > **Keyboard**.

   The **Options controlling the effects of keys** dialog box opens.
9. In the **Backspace key** area, select **Control-H**.

   This activates the backspace key while you are using the SAT.
10. Click **Open**.

    Note:

    If you have not connected to this particular server before, ssh prompts you to accept the server host key. If you save this key when prompted, you will not be prompted if you connect again later. If you do not save the key, PuTTY prompts you the next time you connect to this server.

    When connecting through the Services laptop interface on the server, if you save the host key, the host will be identified as 192.11.13.6. If you later connect to a different server through its laptop interface, this new host also appears as 192.11.13.6, but it will have a different key. You get a prompt in this case because it appears that the host key has changed.

11. If necessary, click **Yes** to accept the server's host key.
12. Log in to the server.

Accessing the command line interface with terminal emulation

To use a command line interface in a terminal emulation window:

Note:
Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are the only supported terminal emulation programs.

1. Open your terminal emulation application.
2. Ensure that the port settings of the terminal emulation program are configured as follows:
   - 115200 baud
   - No parity
   - 8 data bits
   - 1 stop bit
   - No flow control
3. Establish a network connection to the server with either the IP address or the DNS host name. Use port **5023** for this connection.
4. When prompted, log in.

Logins

Initial configuration and upgrades by an Avaya technical support representative or an Avaya Business Partner requires a services login, such as craft or dadmin. Avaya technical support representatives can also use a unique password that is assigned to that customer system.

When you finish installing the Avaya authentication file, Communication Manager has a password for the craft login. This password is unique to the server of the customer. You can use the password the next time that you log in as craft, if you access the server through the Services port. Every other means of craft access still requires an ASG challenge/response. RFA records the revised password. ASG Interactive Response provides this password at 1-800-248-1234 or 1-720-444-5557.

Customers can set up their own logins to access Avaya servers. For more information, see the *Administering Avaya Aura™ Communication Manager* (03-300509). You must have superuser permission to create or change logins and passwords.

Important:
When you assign login IDs, do not start the logins with a number.

Network configuration

Important:
Record any IP addresses, DNS servers, or WINS entries that you change when you configure your services computer. You must restore these entries to connect to other networks.

To configure a new network connection:

Note:
These instructions are for Windows 2000 and Windows XP only.

1. On your computer desktop, right-click **My Network Places** and left-click **Properties** to display the **Network Connections** window.

   Windows 2000 and Windows XP automatically detects the Ethernet card in your system and creates a LAN connection for you. More than one connection might occur.

2. Right-click the correct **Local Area Connection** and left-click **Properties** to display the **Local Area Connection Properties** dialog box.
3. Select **Internet Protocol (TCP/IP)**.
4. Click **Properties** to display the **Internet Protocol (TCP/IP) Properties** dialog box.
5. On the **General** tab, select **Use the following IP address**. Enter the following addresses:
   - IP address: **`192.11.13.5`**
   - Subnet mask: **`255.255.255.252`**
6. Record any IP addresses or other entries that you must clear. You might need to restore these later to connect to another network.
7. Select **Use the following DNS server addresses**. Leave the entries for Preferred DNS server and Alternate DNS server blank.
8. At the bottom of the dialog box, click **Advanced** to display the Advanced TCP/IP Settings dialog box.
9. Click the **DNS** tab. Ensure that no DNS server is administered. The address field is blank.
10. Click **OK** > **OK** > **Close** to close all the windows.

11. Reboot the system if directed to do so.

    After you make these changes to the network configuration for your computer, the **Network and Dial-up Connections** window shows the status of the **Local Area Connection.** The system displays:

    - **`Enabled`** when the Ethernet cable from the laptop is connected to the server.
    - **`Disabled`** or **`unplugged`** when the NIC is not connected to any other equipment.

Browser settings

Connecting directly to the server

To set the browser for a direct connection to the server:

Note:
Instructions are for Internet Explorer 6.0 only.

1. Click **Tools** > **Internet Options**.
2. Click the **Connection** tab.
3. In the **LAN Settings** box in the lower righthand of the page, click **Advanced**.
4. In the Exceptions box after the last entry, type **192.11.13.6**
5. Click **OK** > **OK** > **OK** again to close all the dialog boxes.

Connecting remotely through the network

When you connect through a proxy server, a connection session to a server can time out. To avoid a server time out during a session, add the host names or the IP addresses of the servers to the list of host names and IP addresses.

To add the host names or the IP addresses of the servers to the list of host names and IP addresses:

Note:
The following instructions are for Internet Explorer 6.0 only.

1. Click **Tools** > **Internet Options**.
2. Click the **Connection** tab.
3. Click **LAN settings** > **Advanced**.

4. In the **`Do not use proxy server for addresses beginning with`** field, type the IP address for each server that you want to access remotely. If the first or the first and second octets are the same, you can shorten the address to xxx.xxx.* For example, if you have the IP addresses 135.9.42.75 and 135.9.113.113, then you can type **135.9.***).
5. Click **OK** > **OK** > **OK** again to close all the dialog boxes.

Index

A

administering
IPSI on CSI in a CMC to S8500 . . . . 201, 233, 263
ARP cache, clearing on the laptop230, 261, 326, 330, 458, 463
Audix
on S8100 . . . . . 235, 265, 396
slim board 204, 235, 265, 362, 396, 427

B

backing up
recovery system files 319, 451
S8500 translations 203, 234, 264
S8700-Series translations 361, 395, 426
system files, Linux migration for S8500 to S8710 . 480
busying out MMI circuit packs. 541
busying-out
previously busied-out trunks88, 123, 152, 188, 215, 246, 279, 335, 374, 408, 441, 468
busyouts, recording69, 103, 134, 168, 199, 318, 355, 450, 540

C

cabinets
turning off 71, 171
turning off S8100 106
cables
replacing I/O cables. 267, 429
circuit pack
verifying locations, S8700-Series 439
circuit packs
inserting 72, 107, 136, 171
removing for S8400 . . . . . 71, 136, 171
removing from IP600 for S8400 106
verifying insertion86, 121, 150, 186, 213, 244, 277, 334, 372, 406, 439, 466
verifying locations86, 120, 150, 185, 213, 244, 277, 333, 372, 406, 466
clearing
Web browser cache on laptop 230, 261
command line interface. 620
accessing with SSH. 620
Communication Manager
installing 488, 507, 563, 586
connecting
cables 72, 107, 137, 172
to IP600 processor 226, 257, 388, 419
to media servers 330, 463
to processor. 68, 102, 132, 166, 198
to servers 206, 238, 270, 354, 365, 399, 432
control
cabinet, turning off. . . 136, 204, 236, 363, 397, 452
control cabinet, changing
for CSI in a CMC to PN for S8500 204
for DEFINITY ONE/S8100 to PN for S8700-Series 396
for IP600/S8100 to PN for S8500 265
for IP600/S8100 to PN for S8700-Series . . 362, 427
control chassis, turning off 266, 428
control interface, setting82, 116, 146, 181, 208, 240, 273, 327, 368, 401, 435, 459
copy files to media server 296
copying
translation files 200
translations for S8400 78
translations for S8400 using Xmodem 178
translations on CSI in a CMC to S8500 . . . 232, 262
copying files to S8730 . . . . . 491, 565
corruption of translations
checking for. 306
customer data, verifying85, 120, 149, 185, 212, 243, 277, 333, 372, 405, 439, 466

D

data for a migration
restoring for CSI on a CMC to S8710 . .357, 391, 422
direct connection to server 611

E

ESS server
configure for S8720 in XL configuration . . . 497, 574
ESSs
stopping and starting 501, 580

I

I/O cables, replacing 267, 429
IA770
INTUITY AUDIX data that can be reused
IA770 INTUITY AUDIX Messaging
IA770 INTUITY AUDIX data that must be reinput 92
replacing INTUITY AUDIX Messaging 92
IA770 INTUITY AUDIX Messaging. 92, 93
input/output cables, see I/O cables

installing
Communication Manager 507, 563, 586
Communication Manager software 488
license and authentication files . . 77, 113, 142, 177
linear card reader software 58
software load on S8400 . . . . . 74, 109, 138, 173
TN771 . . . . . 206, 237, 270, 365, 399, 432
TN771 for S8400 . . . . . 73, 108, 138, 173
IP addresses, verifying 86, 121, 150, 186, 213, 244, 278, 334, 373, 406, 439, 467
IP settings
recording 227, 258
recording for S8700-Series 389
IPSI
adding IPSI information for CSI in a CMC to S8700-Series 360, 394, 425
administering and enabling on CSI in a CMC to S8500 201, 233, 263
assigning IP addresses 207, 238, 271, 325, 366, 399, 433, 457
enabling control 212, 276, 371, 405, 438
enabling system for translations 359, 393, 425
installing in CSI in a CMC 205, 363
installing in DEFINITY ONE/S8100 to S8500 236, 398
installing in IP600/S8100 to S8500 . . . . . 269, 431
logging in to .208, 239, 272, 326, 367, 401, 434, 459
resetting . . .210, 241, 274, 328, 369, 403, 436, 461
setting alarm activation level. 202, 234, 264, 361, 395, 426
setting IPSI duplication (high/critical reliability) for CSI in a CMC to S8700-Series 360, 394, 426
setting static IP address for CSI in a CMC to S8700-Series 366
verifying circuit pack version . 214, 245, 278, 335, 373, 407, 440, 467, 474
verifying connectivity211, 243, 276, 333, 371, 404, 438, 465
verifying translations211, 242, 275, 332, 370, 404, 437, 465
IPSI connectivity, verifying 211, 243, 276, 333, 371, 404, 438, 465
IPSI translations
adding for CSI in a CMC to S8500 . . . 202, 233, 264

L

laptop connection to server 611
license and authentication files
generating and retrieving 48
installing on media server 77, 113, 142, 177
license file
installing new 131, 197, 203, 226, 234, 256, 266, 320, 362, 388, 396, 419, 428
installing new on S8400 65, 71, 101, 104, 135, 166, 169
RFA process 48
verifying 243, 277, 357, 391, 422
linear card reader, installing software 58
link status, checking87, 121, 151, 186, 214, 245, 278, 334, 373, 407, 440, 467
Linux migration
backing up system files for S8500 to S8710 . . . 480
local survivable processor, see LSP
login
obtaining password for 48
login, super-user 500, 578
LSP
upgrading 475, 534
LSP media server
configure for S8720 in extra large (XL) configuration497, 574
LSP or ESS server type information 41
LSPs
stopping and starting 501, 580

M

Maintenance Web Interface
starting 619
media server
copying files to 296
media servers
connecting to 330, 463
Migrating
S8700, S8710, S8720 to S8730 535
migrating
DEFINITY CSI in a CMC to S8500 . . . 44, 155, 189
DEFINITY CSI in a CMC to S8700-Series47, 341, 343
DEFINITY ONE/S8100 in a CMC to S8500 . .44, 155
DEFINITY ONE/S8100 in a CMC to S8700-Series . 47, 341
DEFINITY ONE/S8100 to an S8700-Series IP-PNC377
DEFINITY ONE/S8100 to S8500 IP-PNC 217
DEFINITY R in an MCC to S8700-Series 340
DEFINITY SI in an MCC to S8500 . . . . . .44, 154
DEFINITY SI in an MCC to S8700-Series . . .46, 340
DEFINITY SI in an SCC to S8500 . . . . . .44, 154
DEFINITY SI in an SCC to S8700-Series . . .46, 341
from existing DEFINITY and Linux platforms .54, 153
from existing DEFINITY and Linux platforms to S8400 54
from existing DEFINITY and Linux platforms to S8500 153
from existing DEFINITY and Linux platforms to S8700-Series 339
IP600 to S8700-Series IP-PNC 409
IP600/S8100 in a G600 to S8400 42
IP600/S8100 in a G600 to S8500 . . . . . .45, 155
IP600/S8100 in a G600 to S8700-Series . . .47, 341
IP600/S8100 to S8500 IP-PNC 247
S8400 to S8500 309
S8400 to S8700-Series 443
S8500 to S8730 471
S8700-Series to S8730 525
to an S8400 53

to an S8500 153
to an S8700-Series 339
migration
path, definition 31, 53, 153, 339
paths to S8400 53
to S8400 . . . . . .53, 55
to S8500 155
to S8700-Series 342
MMI circuit packs
busying out. 541
modem
access to server 618

N

netcon data modules
removing for S8400 . . . . . 68, 132, 167
node name and IP addresses, recording70, 103, 134, 169, 199, 227, 257, 318, 355, 389, 420, 450

P

password
after installation. 48
premigration administration . 66, 166, 198, 226, 317, 354, 388, 449
premigration administration for IP600 101
premigration setup
downloading authentication file192, 220, 250, 312, 346, 380, 412, 446
downloading license file 192, 220, 250, 312, 346, 380, 412, 446
freezing translations192, 220, 250, 312, 346, 380, 412, 446
processor
connecting to 68, 102, 132, 166, 198
connecting to IP600. . . . . 226, 257, 388, 419

R

recording
IP settings 227, 258
IP settings for S8700-Series 389
node names and IP addresses70, 103, 134, 169, 199, 227, 257, 318, 355, 389, 420, 450
remote access to server
over modem 618
over network 618
Remote Feature Activation
going to the website. 67
starting. 66
removing
circuit packs IP600 to S8400 106
circuit packs S8400 . . . . . 71, 136, 171
netcon data modules S8400 . . . . . 68, 132, 167
removing unused INTUITY AUDIX ports and hunt groups93
replacing
TN2182 with a TN2312BP in CSI 205, 363
TN2182 with a TN2312BP in DEFINITY ONE/S8100 to S8500. . . . . 236, 398
TN2402 with a TN2312BP for CSI in a CMC 205, 363
TN744 397
TN795 . . . . . .235, 266, 428
TN795 with a TN2312BP for CSI in a CMC . 205, 363
TN795 with a TN2312BP in DEFINITY ONE/S8100 to S8500. . . . . 236, 398
TN795 with a TN2312BP in IP600/S8100 to S8500269, 431
TN799 . . . . . 236, 266, 397, 428
TN799C with a TN799DP73, 108, 137, 172, 205, 237, 270, 365, 398, 432
restoring
data for a migration
for CSI on a CMC to S8710 . . . . .357, 391, 422
restoring translations
for CSI in a CMC to S8700-Series . . .358, 392, 423
RFA process 48

S

S8500
disconnecting cables 481
S8720 in extra large (XL) configuration
configuring ESS or LSP media server. . . . 497, 574
configuring LSP media server 497, 574
S8730
configuring ESS/LSP for XL 497, 574
confirming product ID 496, 573
connecting cables 484, 559
copying files. 491, 565
inserting CD. 559
installing in rack 558
performing integrity check 498, 575
restoring backup 571
restoring configuration data and translations . . 569
verifying connectivity 568
verifying server configuration. 495, 571
SAT session, starting 540
saving
translations 199, 227, 318, 355, 451
translations IP600 . . . . . .258, 389, 420
translations with PCMCIA 134
translations with PCMCIA and Xmodem 167
server
command line interface 620
Server type information for LSP or ESS servers . . . 41
servers
access remotely over modem 618
access remotely over network 618
configuring S8400 . . . . . 75, 140, 175
connecting to 206, 238, 270, 354, 365, 399, 432
direct connection 611

starting Maintenance Web pages 200, 231, 262, 390, 421, 490, 565
Services laptop
to S8710, S8720 538
services laptop
to S8730 . . . . . 487, 562
services laptop computer to S8730 Server . . . 487, 562
setting
alarm activation level on TN2312BP202, 234, 264, 361, 395, 426
control interface82, 116, 146, 181, 208, 240, 273, 327, 368, 401, 435, 459
telnet parameters 109
VLAN and diffserv parameters209, 241, 274, 369, 402, 436
SIPI
assigning IP addresses for CSI in a CMC80, 115, 144, 180
static addressing 80, 115, 144, 180
verifying circuit pack version 87, 122, 151, 187
verifying connectivity 85, 120, 149, 185
verifying translations 85, 119, 149, 184
software
installing on S8400 . . . . . 74, 109, 138, 173
starting
Remote Feature Activation 66
SAT session 540
static addressing
for CSI in a CMC to S8700-Series, setting 366
SIPI 80, 115, 144, 180
stopping and starting ESSs and LSPs 501, 580
super-user login 500, 578
system files
backing up 319, 451
system status
verifying 69, 102, 133, 168, 198, 317, 354, 356, 391, 422, 449

T

Tables
LSP or ESS server types 41
telnet parameters
setting 109
terminal emulation 620
TN2182 circuit pack
replacing with a TN2312BP in CSI 205, 363
replacing with a TN2312BP in DEFINITY ONE/S8100 to S8500 . . . . . 236, 398
TN2312BP circuit pack
replacing a TN2182 in CSI 205, 363
replacing a TN2182 in DEFINITY ONE/S8100 to S8500 236, 398
replacing a TN2402 in CSI 205, 363
replacing a TN795 in DEFINITY ONE/S8100 to S8500 236, 398
replacing a TN795 in IP600/S8100 for S8500 269, 431
replacing a TN798 in CSI 205, 363
setting alarm activation level 202, 234, 264, 361, 395, 426
TN2402 circuit pack
replacing with a TN2312BP in CSI 205, 363
TN744 circuit pack
replacing 397
TN771 circuit pack
installing 206, 237, 270, 365, 399, 432
installing for S8400 . . . . . 73, 108, 138, 173
TN795 circuit pack
replacing 235, 266, 428
replacing with a TN2312BP in DEFINITY ONE/S8100 to S8500 . . . . . 236, 398
replacing with a TN2312BP in IP600/S8100 to S8500 269, 431
TN798 circuit pack
replacing with a TN2312BP in CSI 205, 363
TN799 circuit pack
replacing 236, 266, 397, 428
TN799C circuit pack
replacing with a TN799DP73, 108, 137, 172, 205, 237, 270, 365, 398, 432
TN799DP circuit pack
replacing a TN799C 73, 108, 137, 172, 205, 237, 270, 365, 398, 432
translation corruption
checking for 306, 476
translations
backing up S8500 . . . . . 203, 234, 264
backing up S8700-Series 361, 395, 426
copying files 200
copying files on CSI in a CMC to S8500 . . 232, 262
copying files to S8710 . . . . . 358, 392, 423
copying for S8400 78
copying for S8400 using Xmodem 178
migrating 331, 464
restoring 201, 232, 262
restoring for CSI in a CMC to S8700-Series . 358, 392, 423
saving 199, 227, 318, 355, 451
saving IP600 . . . . . 258, 389, 420
saving with PCMCIA 134
saving with PCMCIA and Xmodem 167
verifying IPSI 211, 242, 275, 332, 370, 404, 437, 465
turning off
cabinets 71, 171
control cabinet 136, 204, 236, 363, 397, 452
control chassis 266, 428
S8100 cabinets 106
S8500 481

U

upgrading
G150 Gateway firmware 474

G150 Media Gateway firmware 533
G250 Gateway firmware 474
G350 Gateway firmware 474
G350 Media Gateway firmware 533
G700 Gateway firmware 474
G700 Media Gateway firmware 533
J4350 Gateway firmware 474
J6350 Gateway firmware 474
software on LSP 475, 534

V

verifying
circuit pack locations, S8700-Series 439
VLAN and diffserv parameters, setting209, 241, 274, 369, 402, 436

W

Web browser cache
clearing 329, 462
clearing on laptop. 230, 261
Web pages
starting. 619