Avaya Interaction Center

Release 7.0

Installation Planning and Prerequisites

Document ID 07-300099
Issue 3.0
July 2005

© 2005 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.

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 and 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

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Providing telecommunications security

Telecommunications security (of voice, data, and video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Use (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including, but not limited to, human and data privacy, intellectual property, material assets, financial resources, labor costs, and legal costs).

Your responsibility for your company's telecommunications security

The final responsibility for securing both this system and its networked equipment rests with you, an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources, including, but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Trademarks

Avaya is a trademark of Avaya Inc.

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

Third-party royalty-free license agreements

This product and future updates and service packs to this product may contain third-party royalty-free technology which is provided to you under terms and conditions which are different from your Avaya product license agreement. A file containing these third-party royalty-free licenses, `3plirdme.txt` or a similar name, is in the root directory of the product CD. Your use of this technology described in this file will be subject to the terms and conditions of such other license agreements, and not the Avaya product license agreement.

Document ordering information:
Avaya Publications Center

Voice: +1-207-866-6701
1-800-457-1764 (Toll-free, U.S. and Canada only)

Fax: +1-207-626-7269
1-800-457-1764 (Toll-free, U.S. and Canada only)

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Manager

Web: http://www.avaya.com/support

E-mail: totalware@gwsmail.com

Order: Document No. 07-300099, Issue 3.0
July 2005

For the most current versions of documentation, go to the Avaya support Web site:

http://www.avaya.com/support

COMPAS

This document is also available from the COMPAS database. The COMPAS ID for this document is 107128.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. 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

Avaya Interaction Center
Release 7.0
Installation Planning and Prerequisites

Contents

Before you begin 17

Typographical conventions 17
Notes, tips, and cautions 18
Contacting Technical Support 18
Product documentation 19
Readme file 19
Electronic documentation 19
Printed documentation 20
License to print the electronic documentation 20
Right-to-print license terms 20
Educational services 21

Chapter 1: Introduction 23

Purpose of document 24
Internationalization and localization support 24
Supported languages 24
Limitations on support for Traditional Chinese 25
Limitations on localization and internationalization support with Citrix 25
Avaya IC Readme 25
Avaya IC documentation 26
Avaya Interaction Center CD-ROM 26
Avaya Interaction Center Documentation CD-ROM 26
Documentation directory on an Avaya IC machine 27
Avaya CRM Technical Support Website 27
Avaya IC components 27
Avaya IC core servers 28
Avaya IC Design & Administration Tools 28
IC Manager 28
Avaya Workflow Designer 29
Avaya Database Designer 29
Agent interfaces 29
Avaya Agent 30
Avaya Agent Web Client 30
Avaya Computer Telephony for IC 30
Web Management 31
Avaya Email Management 31
Avaya Outbound Contact Management 31

Avaya Business Advocate for Avaya IC 32
Avaya Content Analyzer 33
Avaya Full Text Search Engine 34
Avaya IC for Siebel 7 34
Avaya Operational Analyst 35
Security for Avaya IC accounts 36
Avaya IC implementation roles 36

Chapter 2: Required software components 41

About the supported versions 42
Exceptions to supported operating systems 42
Required software for Avaya IC servers 43
Required software for Avaya IC databases 45
Required Avaya IC databases 45
Optional Avaya IC databases 45
Prerequisites for the databases 46
Required software for Telephony 47
Telephony servers 47
Prerequisites for Telephony servers 48
Supported Telephony software 48
Supported Avaya switches and software 49
Supported Aspect switches and software 49
Supported Ericsson switches and software 50
Supported Nortel switches and software 50
Required software for Web Management 51
Web Management servers 52
Prerequisites for Web Management servers 53
Required software for Email Management and Content Analyzer 54
Email Management servers and Content Analyzer servers 54
Prerequisites for Email Management servers and Content Analyzer servers 55
Required software for Outbound Contact 56
Support for Outbound Contact 56
Outbound Contact servers 57
Prerequisites for Outbound Contact servers 58
Required software for Business Advocate 60
Business Advocate servers 60
Prerequisites for Business Advocate servers 62
Required software for Avaya IC for Siebel 7 63
Required software for Design & Administration Tools 64
Required software for agent interfaces 65
Prerequisites for Avaya Agent 66
Requirements for Avaya Agent Web Client 66
Required server software 67
Required client software 67
Required client hardware 67
Prerequisites for agent desktop applications on Citrix 68

Required software for customers of Web Management 69
Supported Web browsers 69
Customer HTML Chat Client 70
Known exceptions to Web browser support 71
Exceptions to support of Sun JVM for Website customers 72

Chapter 3: Guidelines for an Avaya IC deployment 75

Performance factors 76
Avaya IC components 76
Volume of contacts 77
Number of concurrent users 77
Network topology and configuration guidelines 78
Network security 78
Avaya IC communication protocol 78
WAN and LAN connections 79
Remote agents for Avaya Agent 79
Connections for remote agents 79
Bandwidth for remote agents 80
Multiple network interface cards 81
Firewall guidelines for Avaya Agent 82
Network and Firewall requirements for Avaya Agent Web Client 83
Database guidelines 83
Avaya IC databases 84
Avaya IC database performance guidelines 85
Database table limitations 86
Time zone handling 86
Methods for time zone handling 87
Time zone methods used by Avaya IC components 88
Avaya IC server guidelines 88
Server naming guidelines 89
Server partitioning guidelines 89
Physical partitioning 90
Logical partitioning 90
Web License Manager guidelines 91
Co-location of client applications with servers 91
Time synchronization for servers 91
Server failure considerations 93
Avaya IC core server guidelines 93
ADU server guidelines 93
Data server guidelines 94
Directory server and Alarm server guidelines 94
EDU server guidelines 95
ORB server guidelines 95
Notification server guidelines 96
Report server guidelines 96
Workflow server guidelines 96
Voice channel server guidelines 98
Telephony server guidelines 98

Telephony Queue Statistics server guidelines . . . 98
DUStore server for voice guidelines . . . 99
Chat channel server guidelines . . . 99
Attribute server guidelines . . . 99
DUStore server for chat guidelines . . . 99
ICM server and CIRS server guidelines . . . 100
Web Management servers guidelines . . . 100
Email channel server guidelines . . . 100
IC Email server guidelines . . . 100
DUStore server for email guidelines . . . 100
Email EDU server guidelines . . . 101
Outbound Contact server guidelines . . . 101
Business Advocate server guidelines . . . 101
Logical Resource Manager guidelines . . . 102
Resource Manager server guidelines . . . 102
Business Advocate databases guidelines . . . 102
Telephony Services Adaptor server guidelines . . . 103
Web Advocate Adaptor server guidelines . . . 104
Workflows for Business Advocate guidelines . . . 104
Avaya OA server guidelines . . . 104
Event Collector server guidelines . . . 105
Location of Event Collector server . . . 105
Event Collector server and Avaya IC domains . . . 105
Event Collector server and Avaya IC sites . . . 105
Event Collector server and ADU servers . . . 105
Event Collector server and Telephony . . . 106
Event Collector server and Business Advocate . . . 106
Limitations on ADU data collection . . . 106
Event Collector Bridge guidelines . . . 107
Minimum deployment . . . 107
Event Collector Bridge and Resource Manager server . . . 107
Event Collector server failover guidelines . . . 107
Avaya OA reporting problems caused by incorrect server deployment . . . 108
Agent fails over to an ADU server that is monitored by a different Event Collector server . . . 109
An agent fails over to an ADU server that is not monitored by an Event Collector server . . . 109
Two Event Collector servers monitor the same agent domains . . . 109

Chapter 4: Avaya IC single site deployment scenarios . . . 111

Adapting deployment scenarios . . . 111
Adding more servers and domains . . . 112
Deploying servers on multi-processor machines . . . 112
Including additional server machines in a deployment . . . 113
Co-locating servers on one machine . . . 113
Rules for items not shown in the deployment scenarios . . . 114
Scenario 1: Single site, voice only . . . 114
Scenario 1: Deployment overview . . . 114
Scenario 1: Avaya IC domain overview . . . 115
Scenario 1: Partitioning of servers . . . 115

Scenario 1: Failover strategy 117
Scenario 2: Business Advocate for single site, voice only 118
Scenario 2: Deployment overview 119
Scenario 2: Avaya IC domain overview 119
Scenario 2: Partitioning of Business Advocate servers 120
Scenario 2: Failover strategy 121
Scenario 3: Business Advocate for single site, high volume voice 121
Scenario 3: Deployment overview 122
Scenario 3: Avaya IC domain overview 122
Scenario 3: Partitioning of Business Advocate servers 123
Scenario 3: Failover strategy 124
Scenario 4: Single site, multi-channel 125
Scenario 4: Deployment overview 125
Scenario 4: Avaya IC domain overview 126
Scenario 4: Partitioning of servers 127
Scenario 4: Failover strategy 128
Scenario 5: Single site, multi-channel with high volume voice 130
Scenario 5: Deployment overview 130
Scenario 5: Avaya IC domain overview 131
Scenario 5: Partitioning of servers 131
Scenario 5: Failover strategy 133
Scenario 6: Business Advocate for single site, multi-channel 135
Scenario 6: Deployment overview 136
Scenario 6: Avaya IC domain overview 136
Scenario 6: Partitioning of Business Advocate servers 137
Scenario 6: Failover strategy 138
Scenario 7: Single site, chat and email only 138
Scenario 7: Deployment overview 139
Scenario 7: Avaya IC domain overview 139
Scenario 7: Partitioning of servers 140
Scenario 7: Failover strategy 141

Chapter 5: Avaya IC multi-site deployment scenarios 143

Scenario 8: Two sites, voice only 144
Scenario 8: Deployment overview 144
Scenario 8: Avaya IC domain overview 145
Scenario 8: Partitioning of Avaya IC servers 145
Partitioning at London site 146
Partitioning at Chicago site 147
Scenario 8: Failover strategy 147
Failover strategy at London site 148
Failover strategy at Chicago site 150
Scenario 9: Two sites, multi-channel 152
Scenario 9: Deployment overview 152
Scenario 9: Avaya IC domain overview 153
Scenario 9: Partitioning of servers 153
Partitioning at York site 154

Partitioning at Paris site . . . 155
Scenario 9: Failover strategy . . . 155
Failover strategy at York site . . . 156
Failover strategy at Paris site . . . 158
Scenario 10: Single instance Business Advocate for two sites, multi-channel . . . 160
Scenario 10: Deployment overview . . . 160
Scenario 10: Avaya IC domain overview . . . 161
Scenario 10: Partitioning of Business Advocate servers . . . 161
Partitioning of Business Advocate servers at Paris site . . . 162
Partitioning of Business Advocate servers at York site . . . 163
Scenario 10: Failover strategy for Business Advocate domains . . . 163
Scenario 11: Multi-instance Business Advocate for two sites, multi-channel . . . 164
Scenario 11: Deployment overview . . . 165
Scenario 11: Avaya IC domain overview . . . 166
Scenario 11: Partitioning of Business Advocate servers . . . 167
Partitioning of Business Advocate servers at York site . . . 167
Partitioning of Business Advocate servers at Paris site . . . 168
Scenario 11: Failover strategy for Business Advocate domains . . . 169
Failover strategy at York site . . . 169
Failover strategy at Paris site . . . 170
Scenario 12: Two sites, chat and email only . . . 170
Scenario 12: Deployment overview . . . 171
Scenario 12: Avaya IC domain overview . . . 171
Scenario 12: Partitioning of Avaya IC servers . . . 172
Scenario 12: Failover strategy . . . 173
Scenario 13: Two sites, multi-channel, data center . . . 174
Scenario 13: Deployment overview . . . 175
Scenario 13: Avaya IC domain overview . . . 175
Scenario 13: Partitioning of servers . . . 176
Partitioning at Paris site . . . 176
Partitioning at York site . . . 177
Scenario 13: Failover strategy . . . 177
Failover strategy at Paris site . . . 178
Failover strategy at York site . . . 179
Scenario 14: Business Advocate for two sites, multi-channel, data center . . . 181
Scenario 14: Deployment overview . . . 182
Scenario 14: Avaya IC domain overview . . . 183
Scenario 14: Partitioning of servers . . . 183
Partitioning at Paris site . . . 184
Partitioning at York site . . . 185
Scenario 14: Failover strategy . . . 185

Chapter 6: Avaya Agent Web Client server deployment scenarios . . . 187

Avaya Agent Web Client deployment guidelines . . . 188
Deployment summary . . . 189
Basic deployment . . . 191
Clustered deployment . . . 192

Load balancing deployment . . . 194
Multiple cell deployment . . . 196

Chapter 7: Avaya IC hardware requirements . . . 199

Hardware requirements for deploying Avaya IC . . . 199
Hardware guidelines for Avaya IC servers . . . 200
Hardware requirements . . . 201
Server distribution . . . 201
Server failover . . . 201
Server machine speed . . . 201
Server configuration impact . . . 202
Disk space for Avaya IC servers . . . 202
Disk space for server log files . . . 202
Validation of Avaya IC configuration . . . 202
IBM Logical Partition (LPAR) technology . . . 202
Hardware requirements for Design & Administration Tools . . . 203
Required hardware for agent workstations . . . 204
Required hardware for the Avaya Agent interface . . . 204
Required hardware for the Avaya Agent Web Client interface . . . 205

Chapter 8: Avaya IC licensing . . . 207

Prerequisites for license files . . . 207
Identifying a physical address . . . 208
Requesting a license file . . . 209
Updating a license file . . . 210
Requesting a replacement license file . . . 211
Troubleshooting for license files . . . 213
Identifying a physical address in Windows . . . 213
Identifying a physical address on Solaris . . . 213
Identifying a physical address on AIX . . . 213

Chapter 9: Supported operating systems . . . 215

Regional settings . . . 215
Microsoft Windows . . . 215
Setting up Windows 2000 Server . . . 216
Installing required service packs for Windows 2000 Server . . . 216
Setting up Windows Server 2003 . . . 217
Setting up Windows XP Professional . . . 217
Installing required service packs for Windows XP Professional . . . 217
Setting up Microsoft Internet Explorer . . . 217
Downloading Internet Explorer . . . 218
Installing a Java Virtual Machine plugin for Internet Explorer . . . 218
Activating the Microsoft JVM . . . 219
Configuring the Sun JVM . . . 219
Configuring encoding for localized releases . . . 220
Security for Unix platforms . . . 220

Sun Solaris 220
Browser requirements for Solaris 221
Disk space requirements for Solaris 221
Installing required patches for Solaris 222
Recommended patch cluster 222
Additional required patches for Solaris 8 222
Additional required patches for Solaris 9 222
Installing Solaris patches 223
Configuration requirements for Solaris 223
Configuration settings for Solaris 223
ULIMIT parameters 224
User accounts for Solaris 225
Root user 225
Installation user 225
IBM AIX 226
Supported versions of AIX 226
C++ runtime library updates 227
Browser requirements for AIX 227
Disk space requirements for AIX 227
Installing required locales 228
Configuration requirements for AIX 229
User accounts for AIX 230
Root user 230
Installation user 230
Citrix 231
Deployment of Avaya IC components in a Citrix environment 231
Location of Avaya IC components 232
Multiple configurations of agent desktop applications 232
Supported versions of Citrix 233
Avaya IC components supported in Citrix 233
Avaya IC support for publishing applications in Citrix 233
Limitations on support for Citrix 234
Licensing for Avaya IC in Citrix 234
Citrix Web interface 235
Citrix client interface 235
Configuring Citrix 236
Configuring Citrix integration for seamless window applications 236
Web browser tool for the client interface 236
Executable tool for the client interface 236
Limitations of integration with Citrix 237

Chapter 10: Network configuration 239

Enabling TCP/IP networking 239
Verifying DNS resolution 240
Verifying DNS resolution in Windows 240
Verifying DNS resolution on Solaris and AIX 241
Troubleshooting an unresolved DNS entry 242

Chapter 11: Supported database management systems 245
About Avaya IC databases 246
Supported database management systems 246
Supported mixed operating system combinations 247
Mixing operating systems 247
Examples of mixed operating system combinations 247
Supported combination 247
Unsupported combination 248
Mixed operating system combinations 248
Exceptions to supported database management systems 249
Requirements for database login 249
Installing database servers 249
Installing database client software 250
Location for database clients 251
Requirements for database clients 251
Configuring binary sort order for Web Management 252
SQL Server 252
Installing SQL Server 253
Installing required service packs for SQL Server 254
Installing the SQL Server 2000 client 254
Recommended configuration for SQL Server 255
Oracle 255
Required version mode for an Oracle 9.2.0 database 255
Required patches for an Oracle database 256
Installing Oracle Server 256
Location of Oracle server 256
Recommended values for installing Oracle server 257
Configuration settings for Oracle server 259
Character set configuration for Oracle server 260
Installing Oracle Client 261
IBM DB2 261
Supported versions of DB2 262
Location of IBM DB2 Server 262
Configuring IBM DB2 server for Avaya IC 262
DB2 registry variables 263
Manual configuration parameters 263
Automatic configuration parameters 263
Installing IBM DB2 Client 264
Configuring IBM DB2 client for Avaya IC 264

Chapter 12: Supported Telephony switches and software 265
Exceptions for Telephony software and switches 266
Avaya Definity and Communication Manager products 267
Supported components 268
Requirements for Avaya Definity and Communication Manager products 268
Downloading the CVLAN client 270

Aspect CallCenter switches . . . 271
Supported components . . . 271
Requirements for Aspect CallCenter switches . . . 271
Nortel Meridian switches and middleware . . . 272
Limitations on support for Nortel Meridian switches . . . 272
Supported links . . . 273
Supported packages . . . 273
Supported components . . . 274
Requirements for Nortel Meridian switches . . . 274
Ericsson MD110 switches . . . 276
Supported components . . . 276
Requirements for Ericsson MD110 switches . . . 276
Intel NetMerge Call Processing Software . . . 277
Interactive Voice Response systems . . . 279

Chapter 13: Supported Web servers . . . 281

Components that require a Web server . . . 281
Supported Web server versions . . . 282
Microsoft Internet Information Server . . . 283
Supported versions of Microsoft IIS . . . 283
Security patches and hot fixes for Microsoft IIS . . . 283
Security considerations for Microsoft IIS 5.0 . . . 284
Security considerations for Microsoft IIS 6.0 . . . 284
Configuring IIS 6.0 for Avaya IC . . . 284
Configuring IIS 6.0 for Avaya IC plugin and Tomcat ISAPI extensions . . . 285
Configuring MIME types for IIS 6.0 . . . 286
Sun Java System Web Server . . . 286
Supported versions of Sun Java System Web server . . . 287
Limitations on Sun Java System Web Server support . . . 287
Sun Java System Web Server 6.0 configuration parameters . . . 287
Sun Java System Web Server configuration parameters . . . 288
IBM HTTP Server . . . 290
Supported version of IBM HTTP server . . . 290
Restriction on the deployment of IBM HTTP Server . . . 290
IBM HTTP Server configuration parameters . . . 291
Java SDK . . . 291
Supported versions of the Java SDK . . . 292
Components that require the Java SDK . . . 292
Installing the JDK for Windows and Solaris . . . 292
Installing the JDK for AIX . . . 293
IBM Websphere Application server . . . 293
Supported version of IBM WAS . . . 293
Installing IBM WAS . . . 294
Configuring IBM WAS for Avaya Agent Web Client . . . 294
Changing the JVM heap size . . . 295
Changing Web Container thread pool size . . . 295
Disabling the Dynamic Cache Service . . . 296

Chapter 14: Supported email servers 297
Configuring SMTP and POP3 servers 297

Chapter 15: Supported third party applications 301
Adobe Acrobat Reader 302
Compilers for Avaya IC Server SDK 302
Lotus Sametime 303
Tomcat 303
IBM WebSphere 303

Chapter 16: Business Advocate 305
Exceptions to platform support for Business Advocate 305
Configuring Windows for Business Advocate 306
Configuring Windows Server 2003 for Business Advocate 306
Configuring the Windows Server 2003 application server role 306
Setting up the Active Directory domain for Windows Server 2003 307
Installing the MSMQ service for Windows Server 2003 308
Configuring Windows 2000 Server for Business Advocate 309
Setting up the Active Directory domain for Windows 2000 Server 310
Installing the MSMQ service for Windows 2000 Server 310
Configuring Windows for Thai (optional) 311
Troubleshooting the installation of MSMQ 311
Configuring SQL Server for Business Advocate 312
Creating a database for Business Advocate 313
Creating the Nethome directory 313
Configuring the SQL Server client 313
Configuring a user to run Business Advocate services 314
Configuring SQL Server for Thai (optional) 315
Configuring Oracle for Business Advocate 315
Location of Oracle components for Business Advocate 316
Creating tablespaces for the Business Advocate database 316
Creating Oracle users for Business Advocate 317
Disabling NTS authentication 318
Installing the Oracle Client 319
Completing the Net8 configuration 319

Appendix A: Switch administration 321
Avaya Communication Manager administration 322
Configuration for IC 7.0 322
Best Services Routing (BSR) option 323
Timed ACW 323
Support Limitations 324
Call vectoring adjunct routing request 325
Defining Vector Directory Numbers (VDNs) 325
Defining vectors 326
Blind transfer 327
Defining ASAI link station extensions (before 1.1) 327

Defining link numbers (on 1.1 or later) . . . 328
Involvement of the telephony server . . . 331
Defining hunt and skill groups . . . 331
Summary of adjunct routing requirements . . . 332
Configuring MAPD CVLAN server software . . . 333
Configuring redundant CTI links . . . 334
Avaya DEFINITY/Communication Manager setup . . . 334
Configuring the switch in an ACD environment . . . 336
Service Observing . . . 337
Predictive call properties . . . 338
Call Coverage . . . 339
Coverage Path . . . 339
Call Forwarding . . . 340
VoIP configuration . . . 342
Define Codec Set . . . 342
Assign node name . . . 343
Define the IP interface . . . 344
Assign a link to the LAN . . . 345
Create an IP signaling group . . . 346
Create IP trunk group . . . 347
Create a DS1 . . . 350
Create a PRI signaling group . . . 351
Create a PRI trunk group . . . 352
Define the class of restriction . . . 354
Define the AAR analysis . . . 355
Define the routing pattern . . . 356
Universal Call ID (UCID) . . . 356
Aspect CallCenter administration . . . 357
Aspect server topology . . . 357
Configure Aspect CallCenter for the TS . . . 358
General tab . . . 358
Settings tab . . . 358
Message Format tab . . . 359
Monitoring & Timeout tab . . . 360
Configure the Aspect CMI server . . . 361
Call control tables configuration . . . 362
MakeCallCCT . . . 362
TransferInitCCT . . . 364
ExternalCCT . . . 366
RouteCCT . . . 367
BlindCCT . . . 368
AgentGroupCCT . . . 370
TS mechanisms . . . 371
Route points . . . 371
Agent configuration . . . 371
Predictive call properties . . . 375
Predictive dialing considerations . . . 377
Fax / modem detection . . . 377
mcscon.ini . . . 377
Multiple CMI server clients . . . 378

Configure Aspect CallCenter for the TSQS 378
Set up the Aspect RealTime configuration file 378
Set up the Aspect RealTime Data Server 380
Aspect Reserved Subtypes 381
destbusy Destination Busy 383
gvxxxxxxxxxx Get One VDU Value 384
newtrans New Transaction 385
preptrans Prep Transaction 386
svxxxxxxxxxx Set One VDU Value 387
timeout Timeout 388
Meridian-1 administration: Symposium Server 389
ELAN and VSID Configuration 389
Value-added server (VAS) print out 390
Symposium Call Center Server link start up 391
Control DN (CDN) configuration 392
ACD-DN configuration 393
Phone set and ACD agent configuration 394
TSQS Configuration 397
Meridian-1 administration: Meridian Link 398
AML configuration 398
Meridian Link Module configuration 400
Link 0: Application Module Link 400
Link 1: TCP/IP host link protocol (Meridian Link) 400
Meridian Link start up 401
Control DN (CDN) configuration 402
ACD-DN configuration 403
Phone set and ACD agent configuration 404
Ericsson MD110 Administration 405
Software requirements 405
Configuring the Application Link 406
Timed ACW 409
ACD and CTI groups 409

Appendix B: IIS Lockdown Tool 411

Prerequisites for the IIS Lockdown Tool 411
Downloading the IIS Lockdown Tool 412
Configuring security with the IIS Lockdown Tool 412
Testing the security settings 415
Troubleshooting the security settings 415

Index 417

Before you begin

This section includes the following topics:

- Typographical conventions on page 17.
- Notes, tips, and cautions on page 18.
- Contacting Technical Support on page 18.
- Product documentation on page 19.
- Educational services on page 21.

Typographical conventions

This guide uses the following font conventions:

Font Type	Meaning
`command`	This font signifies commands, information that you enter into the computer, or information contained in a file on your computer.
`commandvariable`	This font indicates variables in a command string.
italics	This font is used to add emphasis to important words and for references to other chapter names and manual titles.
link	Blue underlined text in online documents indicates a hypertext jump to related information. To view the related material, click the blue underlined text.

Notes, tips, and cautions

Note:
A note calls attention to important information.

Important:
An important note calls attention to a situation that has the potential to cause serious inconvenience or other similar repercussions.

Tip:
A tip offers additional how-to advice.

CAUTION:
A caution points out actions that may lead to data loss or other serious problems.

Contacting Technical Support

If you are having trouble using Avaya software, you should:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related issues.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by:
   - Logging in to the Avaya Technical Support Web site http://www.avaya.com/support
   - Calling or faxing one of the following numbers from 8:30 a.m. to 8:30 p.m. (Eastern Standard Time), Monday through Friday (excluding holidays):
     - Toll free in the U.S. and Canada: 1-888-TECH-SPT (1-888-832-4778)
     - Direct line for international and domestic calls: 1-512-425-2201
     - Direct line for faxes: 1-512-997-4330
   - Sending email with your question or problem to crmsupport@avaya.com. You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

Note:

If you have difficulty reaching Avaya Technical Support through the above URL or email address, please go to http://www.avaya.com for further information.

Product documentation

Most Avaya product documentation is available in both printed and online form. However, some reference material is available only online, and certain information is available only in printed form. A PDF document with detailed information about all of the documentation for the Avaya Interaction Center is included in the `Doc` directory on the product CD-ROM. This PDF document is also included on the separate documentation CD-ROM.

Readme file

The Readme file is a PDF file included on the Avaya Interaction Center software CD-ROM. This file contains important information that was collected too late for inclusion in the printed documentation. The Readme file can include installation instructions, system requirements, information on new product features and enhancements, suggested work-arounds to known problems, and other information critical to successfully installing and using your Avaya software. Avaya may also deliver an Addendum to the Readme, which will be posted on the Avaya Technical Support Website. The Readme Addendum will contain similar information uncovered after the manufacture of the product CD-ROM. Review the Readme file and the Readme Addendum before you install your new Avaya software.

Electronic documentation

The electronic documentation (in PDF or HTML format) for each Avaya Interaction Center product is installed automatically with the program. Electronic documentation for the entire Avaya product suite is included on the product CD-ROM and the documentation CD-ROM.

You can also view the documentation set online at http://www.avayadocs.com.

Printed documentation

You can purchase printed copies of these manuals separately. For details, see the back of this manual’s title page.

License to print the electronic documentation

Online copies of documentation are included on the CD-ROM that accompanies every software release. An Avaya customer who has licensed software (a “Licensee”) is entitled to make this online documentation available on an internal network or “intranet” solely for the Licensee's use for internal business purposes. Licensees are granted the right to print the documentation corresponding to the software they have purchased solely for such purposes.

Right-to-print license terms

Documents must be printed “as-is” from the provided online versions. Making changes to documents is not permitted. Documents may be printed only by any employee or contractor of Licensee that has been given access to the online documentation versions solely for Licensee's internal business purposes and subject to all applicable license agreements with Avaya. Both online and printed versions of the documents may not be distributed outside of Licensee enterprise or used as part of commercial time-sharing, rental, outsourcing, or service bureau use, or to train persons other than Licensee's employees and contractors for Licensee's internal business purposes, unless previously agreed to in writing by Avaya. If Licensee reproduces copies of printed documents for Licensee's internal business purposes, then these copies should be marked “For internal use only within <Licensee> only.” on the first page or cover (where <Licensee> is the name of Licensee). Licensee must fully and faithfully reproduce any proprietary notices contained in the documentation. The copyrights to all documentation provided by Avaya are owned by Avaya and its licensors. By printing any copy of online documentation Licensee indicates its acceptance of these terms and conditions. This license only governs terms and conditions of printing online documentation. Please reference the appropriate license agreement for terms and conditions applicable to any other use, reproduction, modification, distribution or display of Avaya software and documentation.

Educational services

Avaya University provides excellent training courses on a variety of topics. For the latest course descriptions, schedules, and online registration, you can get in touch with us:

- Through the web at http://www.avaya-learning.com/logon_form.asp
- Over the telephone at 800-288-5327 (within the U.S.) +001 303-406-6089 (outside of the U.S.)
- Through email at Avaya.U.Helpdesk@accenture.com

Chapter 1: Introduction

Avaya Interaction Center (Avaya IC) is a multimedia contact center solution that provides a blended channel management solution for voice, web, and email contacts.

Avaya IC combines server and client applications to allow enterprises and other organizations to manage information. Avaya IC provides a single view of the customer, a single set of business rules and workflows, and a single agent interface across all media.

Avaya IC can:

- Manage high volumes of customer contacts
- Support a broad range of communication channels
- Deliver consistent and integrated customer service
- Capture, manage, and derive business value from all relevant customer information

This section provides an overview of Avaya IC. This section includes the following topics:

- Purpose of document on page 24
- Internationalization and localization support on page 24
- Avaya IC Readme on page 25
- Avaya IC documentation on page 26
- Avaya IC components on page 27
- Avaya Operational Analyst on page 35
- Security for Avaya IC accounts on page 36
- Avaya IC implementation roles on page 36

Purpose of document

Deployment of an Avaya IC system is a complex task that requires careful planning. Before you can install and configure your Avaya IC system, review the information in this manual to ensure that your system includes all necessary prerequisites.

This manual includes the following information to help you plan, install and configure an Avaya IC system:

- Deployment planning information, including sample deployment scenarios
- Minimum system requirements to install and run Avaya IC on the supported Windows operating systems
- Minimum system requirements to install and run Avaya IC servers on the supported Solaris operating systems
- Minimum system requirements to install and run Avaya IC servers on the supported AIX operating systems
- Network configuration requirements for Avaya IC
- Supported hardware and software platforms for required third party applications
- Information on how to install and configure third party applications required by Avaya IC

Internationalization and localization support

This section describes the languages for which Avaya IC provides internationalization and localization support and any limitations on that support. This section includes the following topics:

- Supported languages on page 24.
- Limitations on support for Traditional Chinese on page 25.
- Limitations on localization and internationalization support with Citrix on page 25.

Supported languages

Internationalization and localization support includes localized interfaces and localized online help systems for agent desktop applications. Avaya IC will support the following languages with the localization release of Avaya IC:

- English

- German
- French
- Italian
- Spanish
- Portuguese
- Japanese
- Korean
- Simplified Chinese
- Thai
- Traditional Chinese
- Russian

Limitations on support for Traditional Chinese

Avaya IC supports Traditional Chinese only on Windows Server 2003 with a supported Oracle database.

Avaya IC does not include support for Traditional Chinese internationalization and localization in the following components:

- Avaya Content Analyzer
- Outbound Contact Management
- Business Advocate
- Avaya IC for Siebel 7 Integration
- IC Script Debugger
- Spell Checker

Limitations on localization and internationalization support with Citrix

Citrix is responsible for all localization and internationalization support within the Citrix MetaFrame environment. Avaya has not tested localized versions of Avaya IC in a localized Citrix MetaFrame environment.

Avaya IC Readme

You must carefully review the *Avaya Interaction Center 7.0 Readme* file and the *Avaya Interaction Center 7.0 Readme Addendum* before you plan your Avaya IC deployment, or

install and configure your Avaya IC system. You can print the Readme file and Readme Addendum or view them online.

The Readme file contains last-minute information about Avaya IC 7.0 that was not available for the publication of this documentation. The Readme file is available on the Avaya Interaction Center CD-ROM and on the Avaya CRM Technical Support Website at http://www.avaya.com/support/qq.

The Readme Addendum contains information that became available after the publication of the Readme file, if any. The Readme Addendum is available on the Avaya CRM Technical Support Website at http://www.avaya.com/support/qq.

To access the Readme file:

- If your Avaya Interaction Center CD-ROM automatically opens the installation application when you put the CD-ROM in your drive, click **Readme** in the Avaya Interaction Center Installation.
- If your Avaya Interaction Center CD-ROM does not automatically open the installation application, navigate to the Readme file in the root directory of the Avaya Interaction Center CD-ROM: **<*cd-rom_drive*>:\README.htm**

Avaya IC documentation

The following topics describe the locations where you can access Avaya IC documentation in PDF format:

- Avaya Interaction Center CD-ROM on page 26.
- Avaya Interaction Center Documentation CD-ROM on page 26.
- Documentation directory on an Avaya IC machine on page 27.
- Avaya CRM Technical Support Website on page 27.

Avaya Interaction Center CD-ROM

PDF files for all documentation are in the Doc directory on the Avaya IC CD-ROM for Windows.

Avaya Interaction Center Documentation CD-ROM

The PDF files on this CD-ROM also include the *Avaya IC Product Documentation Guide*.

Documentation directory on an Avaya IC machine

This directory includes all documentation that relates to the Avaya IC components on the machine. To access the documentation on an Avaya IC machine, perform one of the following tasks:

- Navigate to the default documentation directory at: *IC_INSTALL_DIR*\IC70\doc
- For Windows only, perform the following steps:
  1. Select **Start** > **Programs** > **Avaya Interaction Center 7.0** > **Online Documentation**
  2. Select the Documentation Index file for the desired component type.
  3. In the Documentation Index file, click the link for the document that you want to view.

Avaya CRM Technical Support Website

All Avaya IC 7.0 documentation is available on the Avaya CRM Technical Support Website at http://www.avaya.com/support.

Avaya IC components

You can deploy Avaya IC in a variety of configurations. A typical configuration includes several Avaya IC components.

Every Avaya IC system requires the mandatory components described in the following sections:

- Avaya IC core servers on page 28.
- Avaya IC Design & Administration Tools on page 28.
- Agent interfaces on page 29.

Each Avaya IC system can integrate all available media channels, or can include only one media channel. An Avaya IC system can also include a combination of other optional components. The following sections describe the optional components of Avaya IC:

- Avaya Computer Telephony for IC on page 30.
- Web Management on page 31.
- Avaya Email Management on page 31.
- Avaya Outbound Contact Management on page 31.

- Avaya Business Advocate for Avaya IC on page 32.
- Avaya Content Analyzer on page 33.
- Avaya Full Text Search Engine on page 34.
- Avaya IC for Siebel 7 on page 34.

Avaya IC core servers

The Avaya IC core servers are the core of the Avaya IC architecture. These servers manage communication between internal and external components, and to control the routing of contacts.

The Avaya IC core servers manage communication between the following components:

- Telephony equipment, such as ACDs, PBXs, and IVRs
- Internet applications, such as Web, Email, and VOIP applications
- Databases
- Avaya IC administrative tools
- Avaya IC client applications

Avaya IC Design & Administration Tools

The Avaya IC Design & Administration tools include:

- IC Manager
- Avaya Workflow Designer
- Avaya Database Designer

IC Manager

IC Manager is an administrative application that monitors, manages, and configures Avaya IC. With IC Manager, contact center supervisors and system administrators can:

- Add, delete, and modify information for agents, servers, and devices
- Start, stop, and configure Avaya IC servers
- Monitor server, agent, and device activities

Avaya Workflow Designer

Avaya Workflow Designer is a customization tool for workflows. Workflow Designer includes sample workflows and pre-defined blocks. You can use Workflow Designer to design, create, and compile:

- Routing workflows that control the routing of contacts through all media channels, and manage the related data during the initial stages of a contact
- Blending workflows that implement business rules to define how agents handle contacts across multiple media
- Email analysis workflows that analyze and process inbound and outbound email contacts
- Agent scripts that can be stored and run in the application
- Business Advocate workflows that qualify contacts for Business Advocate routing

You can also use Workflow Designer to create and compile custom flows to meet the specific needs of your enterprise and your contact center.

Avaya Database Designer

Avaya Database Designer is a customization tool that lets you customize Avaya applications and configure Avaya IC databases. With Database Designer, you can:

- Set database connections
- Configure databases and database connections for Avaya IC, Business Advocate, and Outbound Contact
- Create data sources for servers to access the database
- Upload the application interface, help files, data model, and IC Scripts to the database when you implement:
  - Avaya Agent
  - Avaya Agent Web Client

Agent interfaces

The Avaya Agent interfaces can include one or more of the following applications:

- Avaya Agent
- Avaya Agent Web Client

This section includes the following topics that describe the primary agent interfaces:

- Avaya Agent on page 30
- Avaya Agent Web Client on page 30

Avaya Agent

Avaya Agent is an agent desktop application that integrates multiple media channels and agent applications. With Avaya Agent, an agent can:

- Handle inbound contacts from customers and others in multiple media, such as voice, email, chat, and voice chat
- Handle outbound voice contacts to customers and others
- Access and review information about a customer from the Avaya IC database

Avaya Agent can include media channels from the following applications:

- Avaya Computer Telephony for IC on page 30
- Web Management on page 31
- Avaya Email Management on page 31
- Avaya Outbound Contact Management on page 31

Avaya Agent Web Client

Avaya Agent Web Client is an additional application you can add to your Avaya Interaction Center (IC) contact management solution. Avaya Agent Web Client provides a browser based application interface for the agents in your contact center. Agents do not need to have the Avaya Agent Web Client software installed on their desktops.

The Avaya Agent Web Client interface provides functionality that is similar to the Avaya Agent interface. Agents access the interface by connecting to the Avaya Agent Web Client server through a Web browser. Avaya Agent Web Client supports agent tasks. It does not support supervisor tasks. For example, a supervisor cannot monitor chat sessions or create global resources in Avaya Agent Web Client. You must install Avaya Agent on a separate agent workstation if you want supervisors to perform these tasks. You can run Avaya Agent Web Client or Avaya Agent. You cannot log in to both applications from the same machine.

Note:

Outbound Contact is not supported with Avaya Agent Web Client.

The Avaya Agent Web Client server requires IBM WebSphere Application Server (WAS) and IBM WAS Application Server Kit (AST). For more information about the IBM WebSphere, see IBM WebSphere on page 303.

Avaya Computer Telephony for IC

Avaya Computer Telephony for IC (Telephony) is a computer telephony integration solution that seamlessly links computers, telephones, voice, and data to provide intelligent call qualification and routing in conjunction with voice and data collection. This solution has an

open, scalable architecture that integrates with the most popular PBXs, ACDs, and IVRs to maximize a company's investment in its telephony infrastructure.

Web Management

Avaya Web Management (Web Management) is a Web-based marketing, sales, and service application that personalizes and manages Web transactions across the enterprise. Web Management includes integrated functionality for:

- Web self-service
- Live customer interaction through chat contacts and voice chat contacts
- Email functionality in your customer Web site

Web Management provides access to these features through multiple Web channels, including Web chat, Web-driven customer callback, and real-time, browser-based collaboration and navigation.

By providing customers with direct Web-based service, Web Management can:

- Increase buy-to-browse ratios
- Let your customers handle multiple tasks during a single Web visit
- Reduce the costs associated with telephone-based service, because customers can get more done on the Web

Avaya Email Management

Avaya Email Management (Email Management) is an application that helps contact centers effectively manage the increasing volume of customer email with intelligent email routing and automated response capabilities.

Email Management uses rules-based email management technology to analyze incoming messages and compose personalized answers that can be automatically sent to a customer or queued for review by an agent. Email Management uses data from the IC database and from external sources to help develop highly personalized responses.

Avaya Outbound Contact Management

Avaya Outbound Contact Management (Outbound Contact) works with your telephony switch to provide outbound calling features.

Important:
In Avaya IC 7.0, Outbound Contact is only supported with Avaya Agent. Outbound Contact is not supported with Avaya Agent Web Client.

With Outbound Contact, agents can handle predictive, preview, and automatic outbound calling. Outbound Contact includes “agent blending” for media channels. With agent blending, agents can switch to other media channels when needed, including inbound telephone calls, email, and Web contacts.

With Outbound Contact, managers and supervisors in contact centers can associate a list of customer telephone numbers with specific goals and calling activities.

Managers and supervisors use Outbound Contact to perform the following tasks:

- Define the enterprise settings for the dialers installed across the enterprise.
- Specify the region for each enterprise dialer.
- Create one or more outbound jobs for an outbound calling campaign.
- Import customer telephone numbers into the database.
- Set up calling lists.
- Load one or more outbound jobs into a dialer.
- Disconnect from the current dialer and connect a different dialer, and load one or more jobs into the dialer.
- Monitor calling activities on the dialers, one at a time.
- Manage jobs on individual dialers.

Outbound Contact works with the following reports to help you monitor the outbound calling activities in your contact center:

- Operational Analyst provides real-time monitoring for agent and job information.
- Outbound Contact Reports generates Scheduled Calls Reports and Call Activity Reports.

For more information about Outbound Contact, see *IC Administration Volume 2: Agents, Customers, & Queues* and *Avaya Agent User’s Guide*.

Avaya Business Advocate for Avaya IC

Avaya Business Advocate is an application that manages email, web chat, and voice contacts. Business Advocate understands the needs of each service that you offer to your customers. With that understanding, Business Advocate allocates agent resources to those services to meet the service levels set by you and expected by your customers.

Business Advocate provides fully integrated multimedia, multi-site management of all your contacts.

Business Advocate integrates the following Avaya IC components:

- Avaya Computer Telephony for IC
- Web Management
- Avaya Email Management

With Business Advocate, you can dynamically increase and decrease your agent resource pool. Business Advocate monitors contacts, service classes, and agents in real time. Business Advocate uses the information from the real-time monitoring to apply your agent resources where they are most needed.

You can use Business Advocate Supervisor to administer Business Advocate, including:

- Specify the service classes for your contacts.
- Assign agents to handle contacts in those service classes.

Avaya Content Analyzer

Avaya Content Analyzer (Content Analyzer) is an optional Avaya IC component that performs content analysis on incoming and outgoing email. Content Analyzer applies complex, natural language algorithms to the content of email contacts, and derives a statistically-based match between the intention of that text and a list of pre-applied topics.

With Content Analyzer, you can automatically:

- Identify the language that a customer uses in an email contact
- Route email contacts to agents, according to topic and agent skills
- Screen out email to which the contact center does not want to respond
- Suggest responses for agents to use when an agent responds to an email contact
- Respond to email contacts automatically without agent intervention

Content Analyzer can identify sixteen languages. Content Analyzer can also identify the primary language in an email contact that contains text in more than one language.

However, Content Analyzer cannot analyze the text of email contacts in all languages that it can identify. Content Analyzer can analyze and classify text in the following languages:

- English (US)
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Simplified Chinese
- Spanish

Content Analyzer can identify additional languages in the text of an email contact, although it cannot analyze those languages. For more information, see *IC Administration Volume 1: Servers & Domains*.

Avaya Full Text Search Engine

Avaya Full Text Search Engine (Avaya FTSE) is the full text search engine for Avaya Interaction Center (Avaya IC). Avaya IC requires Avaya FTSE to function correctly. For more information about Avaya FTSE, see *IC Installation and Configuration* and *IC Administration Volume 2: Agents, Customers, & Queues*.

The following Avaya IC components use Avaya FTSE:

Web Self-Service - Web Self-Service is a component of Web Management. Web Self-Service uses Avaya FTSE to search the Frequently Asked Questions (FAQ) database.

The FAQ is an online database of question and answer pairs. Each pair is called a document. The documents are grouped together under topics. In this tree-like hierarchy, the topics are the branches and the documents are the leaves. Agents and customers can search this database using the HTML interface for Web Self-Service.

The Web Self-Service FAQ database can also store suggested responses for agents handling email contacts. The Avaya IC email analysis workflow can be configured to automatically search the Web Self-Service FAQ database for suggested responses using specific keywords found in the customer email or using the email topic as determined by Avaya Content Analyzer. Avaya Content Analyzer is an optional component. These suggested responses will be delivered to agents with the customer emails to enhance email processing efficiency.

Avaya IC for Siebel 7

Avaya Interaction Center for Siebel 7 supports integration with the following:

- Siebel 7.0.4
- Siebel 7.5.2
- Siebel 7.5.3
- Siebel 7.7

The Avaya Interaction Center for Siebel 7 integration combines Avaya IC with the Siebel 7 application. Avaya IC for Siebel 7 provides the customer management features of the

supported versions of Siebel 7 with the contact management and routing features of Avaya IC.

With this integration, the agents in your contact center can provide a unique and customized interaction with each customer. Each agent will:

- Receive work items that are appropriate for the set of skills of that agent
- Perform contact work in multiple media channels
- Access any historical data about work previously performed for a specific customer

In Avaya IC for Siebel 7, all agent interactions occur through the Siebel Communications Toolbar.

For detailed information about the planning and prerequisites that are required for Avaya IC for Siebel 7, see *Avaya IC for Siebel 7 Integration*, which is available on the Avaya IC for Siebel 7 installation CD-ROM.

Avaya Operational Analyst

Avaya Operational Analyst (Avaya OA) is a required component of Avaya IC. Avaya OA performs operational reporting for a multimedia contact center, smoothly growing from single channel analysis, to full interaction, multi-channel analysis with a common data model and user interfaces across these systems.

Avaya OA provides reporting tools that show you summary and detail information about the contact activity at your contact center.

With Avaya OA, you can:

- Create and maintain customized reports that enable managers to monitor contact center, marketing, and service activities
- Build PowerPlay data cubes, then view the summary information in the cube and drill through to more detailed information in the CCQ database, and IC Repository database
- Use business reporting features to distinguish and detail contacts leading to sales, fulfillment requests, or customer service requests

For more information about Avaya OA and its prerequisites, see *Avaya OA Installation Planning and Prerequisites*.

Security for Avaya IC accounts

Avaya IC has security for agent and administrator accounts and passwords. The security includes configurable parameters for Avaya IC accounts, such as:

- Maximum log-in attempts before account is disabled
- Rules for password change intervals
- Rules for password validity, such as minimum and maximum number of alphabetic and numeric characters
- Records of the creation and changes to all login accounts

These security features help defend the Avaya IC system against unauthorized users and malicious use.

For more information about how to configure these parameters, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Avaya IC implementation roles

Implementation of an Avaya IC system requires knowledgeable resources. The amount of resources you need will depend on your environment, and the complexity of the installation.

An implementation team can include representatives from Avaya, an Avaya Business Partner, and the customer. Members of an implementation team can perform more than one role.

The complexity of your Avaya IC installation depends on many factors, such as:

- How many media channels are in your Avaya IC system
- Which third party systems you need to integrate with your Avaya IC system
- What business processes you want to implement in your Avaya IC system

The following table lists the different roles that Avaya IC projects may require. This table does not include the roles that Avaya OA may require. For information about the requirements of Avaya OA, see *Avaya OA Installation and Configuration*.

Role	Responsibility
Project manager	Coordinates developer tasks, manages the project plan, and provides status to management and project sponsors.
Architect	Designs the physical and logical system architecture. Provides designs for complex integrations and logic. Assists other developers with designs and issues. Designs the physical and logical server architecture.
Network administrator	Establishes user network accounts. Monitors the network using network operating system tools or network hardware tools to ensure adequate performance and to diagnose network related issues.
Application and workflow designer	Determines requirements for application and workflow customizations. Works with the Project Manager to determine estimates for requirement implementation.
Database administrator	Works with the database operating system tools. Installs the database server and required client components. Establishes required database accounts. Tunes the database for optimal performance. Ensures security and database integrity. Ensures standards for data normalization and data attributes. Can diagnose database connectivity and performance issues.
Data modeler	Uses Database Designer to modify database tables and data definitions to meet customer requirements. Assists interface designers by adding table fields, table sets, browsers, and table relations to enable customer required functionality.
Interface designer	For Avaya Agent, use XML to modify the layout of the interface. For Avaya Agent Web Client, use XML, JSP, and JavaScript to modify the layout of the interface.
Business logic developer	Uses scripting language to ensure that business logic and IC Scripts perform to requirements. Business logic includes checking and verifying program flow, logic, and data entered by users.
Media routing workflow developer	Uses Workflow Designer to modify or create routing workflows for media contacts, including phone contacts, Web contacts, email contacts, and voice chat contacts. Tests flows with the Workflow servers to make sure they perform correctly and meet performance needs.

Role	Responsibility
Prompter workflow developer	Uses Workflow Designer to modify or create prompting flows as required by the needs of your contact center. Prompter flows can assist agents with typical tasks and provide the scripts for agents to following during contacts with customers.
Integration test analyst	Designs and runs tests that exercise the developed system. Verifies that the configuration and customization do not cause the Avaya IC system to fail. Can use tools such as WinRunner to automate testing processes.
System test analyst	Designs and runs tests that exercise the developed system in accordance with the business processes of your contact center. Can use tools such as WinRunner to automate testing processes.
Server and Workstation software specialist	Installs software on servers and client machines. Configures the software to operate to the specifications for failover and redundancy. Creates installation procedures or workstation images to enable rapid deployment of agent workstations.
Project librarian	Establishes source code management system and implements rules for developers to check out and check in their source code. Merges changes from multiple developers, if required. Creates software builds for integration tests, system tests, and production environments.
Data migration specialist	Analyzes existing data in legacy systems and creates programs or manual procedures to populate data fields in the new system.
Telephony specialist	Uses Telephony tools to establish agent accounts. Creates or modifies telephony vectors or similar components to enable communication with the Avaya IC Telephony server. Configures the Avaya IC Telephony server for optimal performance.
Email specialist	Uses email server tools to establish mail boxes and accounts required for the Avaya IC system. Configures and uses existing email tools to optimize flow of email data. Configures or creates Content Analyzer rules for auto response and auto reply functionality.
Web specialist	Customizes customer-facing Web pages to insert links for Avaya Web Management. Enables, configures, and customizes Web options and Web pages to meet the requirements of your contact center.

Role	Responsibility
Reporting specialist	Uses Avaya OA to create or customize reports to meet the needs of your contact center.
Business Advocate specialist	Understands, implements, and tunes routing and configuration in Business Advocate for maximum performance.

Chapter 2: Required software components

Before you plan or install an Avaya Interaction Center (Avaya IC) system, you need to know the following:

- Which servers are required by the components in the Avaya IC system?
- Which third party software is required for the components in the Avaya IC system?

This section includes the following topics to help you answer these questions for the different components of Avaya IC:

- About the supported versions on page 42
- Exceptions to supported operating systems on page 42
- Required software for Avaya IC servers on page 43
- Required software for Avaya IC databases on page 45
- Required software for Telephony on page 47
- Required software for Web Management on page 51
- Required software for Email Management and Content Analyzer on page 54
- Required software for Outbound Contact on page 56
- Required software for Business Advocate on page 60
- Required software for Avaya IC for Siebel 7 on page 63
- Required software for Design & Administration Tools on page 64
- Required software for agent interfaces on page 65
- Required software for customers of Web Management on page 69

Tip:

This section provides a summary of the prerequisites for the Avaya IC components. Further details about service packs, fix packs, maintenance levels, and patches are available in the appropriate chapters of this document.

These topics do not include information about required software for Avaya OA. For more information about Avaya OA and its prerequisites, see *Avaya OA Planning and Prerequisites*.

About the supported versions

Avaya supports use of the software versions documented in this manual with release 7.0 of Avaya OA and Avaya IC. These software versions are the minimum versions required by Avaya.

Release 7.0 does not support operating systems, databases, Web servers, switches, or other software platforms that are not documented in this manual.

Avaya will support subsequent updates and service packs that are released to provide corrections to a bug, defect, or problem for the software versions documented in this manual, so long as those updates and service packs:

- Are guaranteed by the manufacturer to be backwards compatible with the supported version.
- Do not include changes to core functionality or new features.

Avaya recommends that you test all updates and service packs subsequent to the supported versions in a development environment before applying them to a production environment.

Exceptions to supported operating systems

The following table describes the exceptions to operating system support for Avaya IC. For information about limitations to support for Citrix, see Limitations on support for Citrix on page 234.

Avaya IC component	Exception to supported operating systems
Voice Chat	No AIX support for the Voice Media Manager (VMM) service. Voice Chat does not function with the VMM on AIX. Host the VMM on a Windows or Solaris machine.
Business Advocate	No AIX or Solaris support for Resource Manager servers. Business Advocate does not function with the Resource Manager servers on AIX or Solaris. Host the Resource Manager servers on Windows machines. For more information, see Exceptions to platform support for Business Advocate on page 305.

Avaya IC component	Exception to supported operating systems
Outbound Contact	No AIX or Solaris support for Outbound Contact. Outbound Contact does not function with the Dialing Kernel server or Softdialer server on AIX or Solaris. Host the Outbound Contact servers and other components on Windows machines.
Telephony	No Solaris 9 or AIX support for Telephony server and Nortel Meridian or Nortel Symposium. This exception occurs because NetMerge is not available for Solaris 9. If the Avaya IC system requires a Nortel or Meridian switch, use another supported operating system, such as Solaris 8.

Required software for Avaya IC servers

The Avaya IC servers manage communication between internal and external components, and control the routing of contacts. Some servers are required by all Avaya IC systems. However, some servers, such as the DUStore server, are not required in all Avaya IC systems. To determine which core servers your Avaya IC system requires, see the appropriate deployment scenario in one of the following chapters:

- Chapter 4: Avaya IC single site deployment scenarios on page 111.
- Chapter 5: Avaya IC multi-site deployment scenarios on page 143.

The following table shows the software that you must install on machines that host one or more Avaya IC servers or on a machine that communicates with a server machine. For

more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Required software	Location	Supported versions[1]					
		Windows		Solaris		AIX	
Operating systems	All core server machines	Windows 2000 Server SP4	Windows Server 2003	Solaris 8	Solaris 9	AIX 5.1L ML3	AIX 5.2 ML2
Web server	Machine that communicates with WebLM application **Note:** You can host the server and the application on the same machine.	Microsoft IIS 5.0	Microsoft IIS 6.0	Sun ONE Web Server 7.0	Sun Java System Web Server 6.1 SP1	IBM HTTP Server 1.3.28	
Time synchronization utility	All core server machines	Third party NTP application		NTP application		NTP application	
PDF reader for documentation	All server machines	Adobe Acrobat Reader		Adobe Acrobat Reader		Adobe Acrobat Reader	
Java SDK	Machine that hosts WebLM	Sun JDK 1.3.1_15		Sun JDK 1.3.1_15		IBM JDK 1.3.1 32 bit build ca131-20030329	
Email servers	Machine that communicates with Notification server	SMTP and POP3 compliant email servers		SMTP and POP3 compliant email servers		SMTP and POP3 compliant email servers	
Web browser	Machine that hosts WebLM	Internet Explorer 6.0 SP1		Through Admin machine: Internet Explorer 6.0 SP1		Through Admin machine: Internet Explorer 6.0 SP1	

1. 64 bit versions of the Solaris and AIX Operating Systems are not supported. Virtualization technologies like VMWare are not supported. For information about IBM LPAR support, see IBM Logical Partition (LPAR) technology on page 202.

Required software for Avaya IC databases

Avaya IC servers and client applications require access to the Avaya IC databases. These databases store system level data, including information about customers and agents, and application level data, including information about contacts with customers.

Avaya OA reports on information that Avaya IC stores in its databases.

This section lists the prerequisite software required to support the Avaya IC databases. This section includes the following topics:

- Required Avaya IC databases on page 45.
- Optional Avaya IC databases on page 45.
- Prerequisites for the databases on page 46.

Required Avaya IC databases

The following Avaya IC databases are required for all Avaya IC systems. For a brief description of these databases, see Avaya IC databases on page 84.

- Repository
- CCQ

Important:
The CCQ database is required for all systems.

Optional Avaya IC databases

The following table shows the Avaya IC databases that are only required for Avaya IC systems that include specific components. For a brief description of these databases, see Avaya IC databases on page 84.

Component	Databases
Outbound Contact	• Dialer
Business Advocate	• Business Advocate System Store • Business Advocate Resource Store
Avaya IC for Siebel	• Siebel 7

Prerequisites for the databases

All Avaya IC systems require a relational database management system (RBDMS). Avaya IC provides support for each RDBMS only on certain supported operating systems. The following table lists the required operating system for each supported RDBMS.

For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Note:

Avaya IC provides limited support for databases that run on a different operating system than the Avaya IC servers. For more information, see Chapter 11: Supported database management systems on page 245.
For information about exceptions to this RDBMS support for certain optional databases, such as Business Advocate databases, see Exceptions to supported database management systems on page 249.

Database operating system	SQL Server 2000 SP3a	Oracle 8.1.7	Oracle 9.2.0	DB2 UDB 8.1 FP5
Windows 2000 Server SP4	✔	✔	✔	-
Windows Server 2003	✔	✔	✔	-
Solaris 8	-	✔	-	-
Solaris 9	-	✔	✔	-
AIX 5.1L ML3	-	-	-	-
AIX 5.2 ML2	-	-	-	✔

Required software for Telephony

Telephony components provide services that manage communication between switches and Avaya IC, and control the routing of voice contacts.

This section lists the servers that support Telephony for Avaya IC and the prerequisite software for those servers. This section includes the following topics:

- Telephony servers on page 47.
- Prerequisites for Telephony servers on page 48.

Telephony servers

The following table shows the servers that support Telephony.

Component	Servers
Required servers for Telephony	• Telephony server
Optional servers for Telephony	• Telephony Queue Statistics server • VOX server
Required core servers for Telephony	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server
Optional core servers for Telephony	For systems with multiple server machines, install additional core servers as described in the following sections: • Chapter 4: Avaya IC single site deployment scenarios on page 111 • Chapter 5: Avaya IC multi-site deployment scenarios on page 143

Prerequisites for Telephony servers

The following table shows the software that you must install on machines that host one or more servers for Telephony.

For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Certain switches and software support only certain functions and components of Avaya IC. For more detailed information, see Chapter 12: Supported Telephony switches and software on page 265.

Supported Telephony software

Required software	Location	Supported operating system versions		
		Windows	Solaris	AIX
Operating systems	All core server machines	• Windows 2000 Server SP4 • Windows Server 2003	• Solaris 8 • Solaris 9	• AIX 5.1L ML3 • AIX 5.2 ML2
Time synchronization utility	All core server machines	Third party NTP application	NTP application	NTP application
Avaya switches and software	As required by switch or software	For more information about supported switches and switch software, see: • Supported Avaya switches and software on page 49 • Supported Aspect switches and software on page 49 • Supported Ericsson switches and software on page 50 • Supported Nortel switches and software on page 50		

Supported Avaya switches and software

Switch releases	Required software	Operating system support
Definity G3 R8.3, R9, R10	• CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 9 or 8.2.5 or later. • ADJLK Adjunct Link (not asai link) on the switch • Call Center Elite with EAS for ASAI Agent States	• Windows 2000 Server SP4 • Windows Server 2003 • Solaris 8 • Solaris 9 • AIX 5.1L ML3 • AIX 5.2 ML2
Communication Manager 1.1, 1.2, 1.3, 2.x	• CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 8.2.5 or later. • ADJLK Adjunct Link (not asai link) on the switch • Call Center Elite with EAS for ASAI Agent States	• Windows 2000 Server SP4 • Windows Server 2003 • Solaris 8 • Solaris 9 • AIX 5.1L ML3 • AIX 5.2 ML2
Communication Manager 3.x	• AE Services 3.0 CVLAN Service (new implementations) • MAPD based CVLAN Server (existing implementations upgrading to 3.x). • CVLAN Client 8.2.5 or later. • ADJ-IP Adjunct Link (not asai link) configured on the switch. Order of an Avaya IC ACD connector configures the RFA file on the switch appropriately. • Call Center Elite with EAS for ASAI Agent States For Business Advocate only: • Increased Adjunct Route Capacity	• Windows 2000 Server SP4 • Windows Server 2003 • Solaris 8 • Solaris 9 • AIX 5.1L ML3 • AIX 5.2 ML2

Supported Aspect switches and software

Switch releases	Required software	Operating system support
Aspect 8.3	• Aspect Contact Server (Portal) • Aspect CMI server version 4.X • Aspect Real-time Receiver Custom Control runtime version • Aspect App Bridge Admin tool	• Windows 2000 Server SP4 • Windows Server 2003

Supported Ericsson switches and software

Switch releases	Required software	Operating system support
Ericsson MD110 release BC11	• Ericsson ApplicationLink 4.0 • Intel NetMerge Call Processing 6.0	• Windows 2000 Server SP4 • Windows Server 2003 • Solaris 8 • Solaris 9

Supported Nortel switches and software

Switch releases	Required software	Operating system support
Nortel Meridian-1: • Meridian Link • Option 11, 61, and 81 switches • X11 Release with V2111 patch (core patch 9MP05182) Version 5.42	• Link 5c • Intel NetMerge Call Processing Software 6.0 • Meridian MAX version 9 with MSI	• Windows 2000 Server SP4 • Windows Server 2003
Nortel Meridian-1: • Meridian Link • Option 61, and 81 switches • X11 Release with V2111 patch (core patch 9MP05182) Version 5.42	• Link 5c • Intel NetMerge Call Processing Software 6.0 • IBM DCE 3.1 with patch 6 • Meridian MAX version 9 with MSI	• Solaris 8

Switch releases	Required software	Operating system support
Nortel Meridian-1: • Symposium Call Center Server 4.2 and 5.0 • Option 11, 61, and 81 switches • X11 Release with V2111 patch (core patch 9MP05182) • Version 5.42	• Intel NetMerge Call Processing Software 6.0 • Real Time Data Interface Toolkit	• Windows 2000 Server SP4 • Windows Server 2003
Nortel Meridian-1: • Symposium Call Center Server 4.2 and 5.0 • Option 61 & 81 switches • X11 Release with V2111 patch (core patch 9MP05182) • Version 5.42	• Intel NetMerge Call Processing Software 6.0 • IBM DCE 3.1 with patch 6 • Real Time Data Interface Toolkit	• Solaris 8

Required software for Web Management

Web Management components provide services for the following Avaya IC features:

- Web Management
- Email Management
- Voice Chat

This section lists the servers that support Web Management and the prerequisite software for those servers. This section includes the following topics:

- Web Management servers on page 52.
- Prerequisites for Web Management servers on page 53.

Web Management servers

The following table shows the servers that support Web Management in Avaya IC.

Component	Servers
Required Web Management servers	• WebACD server • ComHub server • Paging server • Attribute server • Tomcat server for Website • ICM server
Optional Web Management servers	• Central Internet Routing Service (CIRS)
Required servers for Voice Chat	• Required Web Management servers on page 52 • Required servers for Telephony on page 47 • Voice Media Manager (VMM) server
Required servers for Scheduled Call	• Required Web Management servers on page 52 • Outbound Contact servers on page 57
Required core servers for Web Management	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server • Secondary EDU server for chat contacts
Optional core servers for Web Management	For systems with multiple server machines, install additional core servers as described in the following sections: • Chapter 4: Avaya IC single site deployment scenarios on page 111 • Chapter 5: Avaya IC multi-site deployment scenarios on page 143

Prerequisites for Web Management servers

The following table shows the software that you must install on machines that host one or more Web Management servers.

Required software	Location	Supported versions					
		Windows		Solaris		AIX	
Operating systems	All server machines	Windows 2000 Server SP4	Windows Server 2003	Solaris 8	Solaris 9	AIX 5.1L ML3	AIX 5.2 ML2
Web server	Machine that communicates with Website application **Note:** can host server and application on same machine.	Microsoft IIS 5.0	Microsoft IIS 6.0	Sun ONE Web Server 7.0	Sun Java System Web Server 6.1 SP1	IBM HTTP Server 1.3.28	
Time synchronization utility	All server machines	Third party NTP application		NTP application		NTP application	
PDF reader for documentation	All machines	Adobe Acrobat Reader		Adobe Acrobat Reader		Adobe Acrobat Reader	
Java SDK	Machine that communicates with Website	Sun JDK 1.3.1_15		Sun JDK 1.3.1_15		IBM JDK 1.3.1 32 bit build ca131-20030329	
Web browser	Machines that hosts one or more Websites	Internet Explorer 6.0 SP1		Through Admin machine: Internet Explorer 6.0 SP1		Through Admin machine: Internet Explorer 6.0 SP1	

For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Note:

The Voice Media Manager (VMM) service required for Voice Chat does not support AIX. You must host the VMM on a Windows or Solaris machine. Voice Chat does not function with the VMM on AIX.

For information about the browsers supported for customers who access the Website, see Required software for customers of Web Management on page 69.

Required software for Email Management and Content Analyzer

Email Management and Content Analyzer components manage communication between email servers and Avaya IC, and control the routing of email contacts.

This section lists the servers that support Email Management and Content Analyzer for Avaya IC and the prerequisite software for those servers. This section includes the following topics:

- Email Management servers and Content Analyzer servers on page 54.
- Prerequisites for Email Management servers and Content Analyzer servers on page 55.

Email Management servers and Content Analyzer servers

The following table shows the servers that support Email Management and Content Analyzer.

Component	Servers
Required core servers for Email Management and Content Analyzer	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server • DUStore server
Required Email Management servers	• Email server • Tomcat server for Email Template Administration
Required Web Management servers for email	• WebACD server • Paging server • ComHub server • Tomcat server for WebACD administration pages.

Component	Servers
Content Analyzer servers	• Required Email Management servers on page 54 • Required Web Management servers for email on page 54 • Content Analyzer administration server • Content Analyzer operation server
Optional core servers for Email Management and Content Analyzer	For systems with multiple server machines, install additional core servers as described in the following sections: • Chapter 4: Avaya IC single site deployment scenarios on page 111 • Chapter 5: Avaya IC multi-site deployment scenarios on page 143

Prerequisites for Email Management servers and Content Analyzer servers

The following table shows the software that you must install on machines that host one or more servers for Email Management or Content Analyzer. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Required software	Location	Supported versions					
		Windows		Solaris		AIX	
Operating systems	All server machines	Windows 2000 Server SP 4	Windows Server 2003	Solaris 8	Solaris 9	AIX 5.1L ML3	AIX 5.2 ML2
Web server	Machine that communicates with Email Template Administration application **Note:** can host server and application on same machine.	Microsoft IIS 5.0	Microsoft IIS 6.0	Sun ONE Web Server 7.0	Sun Java System Web Server 6.1 SP1	IBM HTTP Server 1.3.28	

Required software	Location	Supported versions		
		Windows	Solaris	AIX
Time synchronization utility	All server machines	Third party NTP application	NTP application	NTP application
PDF reader for documentation	All machines	Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader
Java SDK	Machine that communicates with Email Template Administration	Sun JDK 1.3.1_15	Sun JDK 1.3.1_15	IBM JDK 1.3.1 32 bit build ca131-20030329
Email servers	Machine that communicates with Email server machine	SMTP and POP3 compliant email servers	SMTP and POP3 compliant email servers	SMTP and POP3 compliant email servers
Web browser	Machine that hosts Email Template Administration	Internet Explorer 6.0 SP1	Through Admin machine: Internet Explorer 6.0 SP1	Through Admin machine: Internet Explorer 6.0 SP1

Required software for Outbound Contact

Outbound Contact components provide services that manage communication between switches and Avaya IC, and control the routing of voice contacts.

This section lists the servers that support Telephony and Outbound Contact for Avaya IC and the prerequisite software for those servers. This section includes the following topics:

- Support for Outbound Contact on page 56
- Outbound Contact servers on page 57.
- Prerequisites for Outbound Contact servers on page 58.

Support for Outbound Contact

Outbound Contact is not supported with Avaya Agent Web Client.

Outbound Contact servers

The following table shows the servers that support Outbound Contact.

Component	Servers
Outbound Contact servers	• Dialing Kernel server • SoftDialer server • Required servers for Telephony on page 47
Required core servers for Outbound Contact	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server
Optional core servers for Outbound Contact	For systems with multiple server machines, install additional core servers as described in the following sections: • Chapter 4: Avaya IC single site deployment scenarios on page 111 • Chapter 5: Avaya IC multi-site deployment scenarios on page 143

Prerequisites for Outbound Contact servers

The following table shows the software that you must install on machines that host one or more servers for Outbound Contact.

For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Certain switches and software support only certain functions and components of Avaya IC. For more detailed information, see Chapter 12: Supported Telephony switches and software on page 265.

Required software	Location	Supported versions			
		Windows		Solaris	AIX
Operating systems	All core server machines	Windows 2000 Server SP4	Windows Server 2003	Not supported.	Not supported.
Time synchronization utility	All core server machines	Third party NTP application		Not supported.	Not supported.
PDF reader for documentation	All server machines	Adobe Acrobat Reader		Not supported.	Not supported.

Required software	Location	Supported versions		
		Windows	Solaris	AIX
Avaya switches and software	As required by switch or software	Definity G3 R8.3, R9, R10 *Required software:* • CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 9 or 8.2.5 or later. • ADJLK Adjunct Link (not asai link) on the switch • Call Center Elite with EAS for ASAI Agent States	Not supported.	Not supported.
		Communication Manager 1.1, 1.2, 1.3, 2.0 *Required software:* • CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 9 or 8.2.5 or later. • ADJLK Adjunct Link (not asai link) on the switch • Call Center Elite with EAS for ASAI Agent States	Not supported.	Not supported.
Aspect switches and software	As required by switch or software	Not supported.	Not supported.	Not supported.
Nortel switches and software	See Nortel Meridian switches and middleware on page 272.	Not supported.	Not supported.	Not supported.

Required software for Business Advocate

Business Advocate for Avaya IC includes a set of servers that provide services to intelligently match agents with contacts in all supported media channels, and to manage communication with other Avaya IC servers.

This section lists the servers that support Business Advocate for Avaya IC and the prerequisite software for those servers. This section includes the following topics:

- Business Advocate servers on page 60.
- Prerequisites for Business Advocate servers on page 62.

Business Advocate servers

The following table shows the servers that support Business Advocate for Avaya IC.

Component	Servers
Required Business Advocate servers	• Resource Manager server
Required servers for Business Advocate with Telephony	• Telephony Services Adaptor server • Required servers for Telephony on page 47
Optional servers for Business Advocate with Telephony	• VOX server
Required servers for Business Advocate with Web Management	• Web Advocate Adaptor server • Required Web Management servers on page 52
Optional servers for Business Advocate with Web Management	• Required servers for Voice Chat on page 52
Required servers for Business Advocate with Email Management	• Web Advocate Adaptor server • Required Email Management servers on page 54 • Required Web Management servers for email on page 54

Component	Servers
Required core servers	• ADU server • Alarm server • Blender server • Data server • Directory server • EDU server • License server • ORB server • Notification server • Report server • Workflow server • Secondary ADU servers on each machine with a Resource Manager server • Secondary EDU servers for contacts in supported media channels • DUStore server for Email Management
Optional core servers	For systems with multiple server machines, install additional core servers as described in the following sections: • Chapter 4: Avaya IC single site deployment scenarios on page 111 • Chapter 5: Avaya IC multi-site deployment scenarios on page 143

Prerequisites for Business Advocate servers

The following table shows the software that you must install on machines that host one or more Business Advocate servers. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Certain switches and software support only certain functions and components. For more detailed information, see Chapter 12: Supported Telephony switches and software on page 265.

Required software	Location	Supported versions					
		Windows		Solaris		AIX	
Operating systems	All server machines except Resource Manager server	Windows 2000 Server SP4	Windows Server 2003	Solaris 8	Solaris 9	AIX 5.1L ML3	AIX 5.2 ML2
	Machine that hosts Resource Manager server	Windows 2000 Server SP4	Windows Server 2003	Not supported		Not supported	
Microsoft Active Directory	Server machine that hosts Resource Manager and/or domain controller	Active directory provided with Windows Server operating system		Not supported		Not supported	
Windows Message Queuing services	Server machine that hosts Resource Manager	Provided with Windows 2000 Server and Windows Server 2003		Not supported		Not supported	
Time synchronization utility	All core server machines	Third party NTP application		NTP application		NTP application	
PDF reader for documentation	All server machines	Adobe Acrobat Reader		Adobe Acrobat Reader		Adobe Acrobat Reader	

Required software	Location	Supported versions		
		Windows	Solaris	AIX
Telephony switches and software	As required by switch or software	For information about required software for Telephony, see Required software for Telephony on page 47. Business Advocate does not have any special requirements for Telephony.		
Outbound Contact	As required by switch or software	For information about required software for Outbound Contact, see Required software for Outbound Contact on page 56. Business Advocate does not have any special requirements for Outbound Contact.		
Web Management	As required by software	For information about required software for Web Management, see Required software for Web Management on page 51. Business Advocate does not have any special requirements for Web Management.		
Email Management	As required by software	For information about supported software for Email Management, see Required software for Email Management and Content Analyzer on page 54. Business Advocate does not have any special requirements for Email Management.		
Content Analyzer	As required by software	For information about supported software for Content Analyzer, see Required software for Email Management and Content Analyzer on page 54. Business Advocate does not have any special requirements for Content Analyzer.		

Required software for Avaya IC for Siebel 7

The following table shows the software that you must install on machines that host one or more servers for Avaya IC for Siebel 7.

Avaya Interaction Center for Siebel 7 supports integration with the following versions of Siebel:

- Siebel 7.0.4
- Siebel 7.5.2
- Siebel 7.5.3
- Siebel 7.7

For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Note:

For detailed information about the components and prerequisites required for Avaya IC for Siebel 7, see *Avaya IC for Siebel 7 Integration*, which is available on the Avaya IC for Siebel 7 installation CD-ROM. For information about the requirements for Siebel, see the documentation provided by Siebel.

Required software	Location	Supported versions					
		Windows		Solaris		AIX	
Operating systems	All Avaya IC server machines and Siebel 7.7	Windows 2000 Server SP4	Windows Server 2003	Solaris 8[1]	Solaris 9	AIX 5.1L ML3	AIX 5.2 ML2
	Siebel 7.0 and 7.5 servers	Windows 2000 Server		Solaris 8		AIX 5.1	
Time synchronization utility	All core server machines	Third party NTP application		NTP application		NTP application	
PDF reader for documentation	All server machines	Adobe Acrobat Reader		Adobe Acrobat Reader		Adobe Acrobat Reader	
Java SDK	Machine that hosts WebLM	Sun JDK 1.3.1_15		Sun JDK 1.3.1_15		IBM JDK 1.3.1 32 bit build ca131-20030329	
Email servers	Machine that communicates with Notification server	SMTP and POP3 compliant email servers		SMTP and POP3 compliant email servers		SMTP and POP3 compliant email servers	
Web browser	Machine that hosts WebLM	Internet Explorer 6.0 SP1		Through Admin machine: Internet Explorer 6.0 SP1		Through Admin machine: Internet Explorer 6.0 SP1	

1. Solaris version 8 recommended patch cluster (kernel at level 13 or above) with one of the following patches: 109147-09 and above, or 108434-02 and above.

Required software for Design & Administration Tools

The Design & Administration Tools for Avaya IC include the following components:

- IC Manager

- Database Designer
- Workflow Designer

The following table shows the software that you must install on machines that host one or more of the Design & Administration Tools. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Required software	Location	Supported Windows versions
Operating systems	All machines	Windows 2003 Windows XP Professional SP1a Windows XP SP2
PDF reader for documentation	All machines	Adobe Acrobat Reader
Java Virtual Machine	Machine that runs the Web browser for Email Template Administration	Sun JVM 1.4.1
Web browser	All machines	Internet Explorer 6.0 SP1

Required software for agent interfaces

The agent interfaces for Avaya IC include the following:

- Avaya Agent
- Avaya Agent Web Client

This section describes the prerequisite software required to support the agent interfaces. This section includes the following topics:

- Prerequisites for Avaya Agent on page 66.
- Requirements for Avaya Agent Web Client on page 66
- Prerequisites for agent desktop applications on Citrix on page 68.

Prerequisites for Avaya Agent

The following table shows the software that you must install on machines that host Avaya Agent.

Required software	Location	Supported Windows versions
Operating systems	All machines	Windows 2000 Professional SP4 Windows XP Professional SP1a Windows XP SP2
PDF reader for documentation	All machines	Adobe Acrobat Reader
Java Virtual Machine	All machines	Sun JVM 1.4.1 **Note:** Windows 2000 includes the Microsoft JVM plugin which is not supported
Web browser	All machines	Internet Explorer 6.0 SP1

Requirements for Avaya Agent Web Client

The Avaya Agent Web Client software must be installed in addition to the software required by the Avaya Interaction Center servers. The Avaya Agent Web Client software provides a browser based application interface for the agents in your contact center.

This section includes the following topics:

- Required server software on page 67
- Required client software on page 67
- Required client hardware on page 67

Required server software

The following table lists the software you must install on an application server to enable Avaya Agent Web Client. This software is installed *in addition to* the software required by the Avaya IC servers.

Required software	Supported operating system versions		
	Windows	**Solaris**	**AIX**
IBM WAS 6.0	• Windows 2000 Server SP4 • Windows Server 2003	Solaris 9	AIX 5.2 ML2
IBM WAS AST	• Windows 2000 Server SP4 • Windows Server 2003	Not supported	Not supported
Time synchronization utility	Third party NTP application	NTP application	NTP application

Required client software

The following table lists the software you must install on your agent systems to enable the Avaya Agent Web Client interface.

Required software	Supported version
Java J2RE plug-in	Version 1.4.2_07 or newer
Web browser	Internet Explorer 6.0 SP1
DirectX	Version 9.0b
Operating system	Windows 2000 Professional Windows XP SP2 Windows XP SP1

Required client hardware

For voice channel only, the minimum machine requirements for a client system are a 700Mhz processor with 512MB RAM. For voice with chat or email channels, the minimum machine requirements for a client system are a 1.4GHz processor with 512 MB RAM.

Prerequisites for agent desktop applications on Citrix

Avaya IC supports only the following agent desktop applications on Citrix. For detailed information about the limitations of support for Citrix, see Limitations on support for Citrix on page 234.

- Avaya Agent with the following features:
  - Voice channel
  - Email channel
  - Chat channel
  - Voice Chat channel
  - Prompter

Note:

Avaya Agent Web Client is not supported with Citrix.

The following table shows the software that you must install on Citrix server machines and on agent machines if you want to host a supported agent desktop application on Citrix.

Required software	Location	Supported versions
Operating systems	Citrix server machines	• Citrix MetaFrame XP 1.0 • Citrix MetaFrame XP Presentation Server - Feature Release 3
	Agent machines	• Windows 2000 Professional SP4 • Windows XP Professional SP1a
PDF reader for documentation	All machines	Adobe Acrobat Reader
Java Virtual Machine	Citrix server machines	Sun JVM 1.4.1 **Note:** Windows 2000 includes the Microsoft JVM plugin which is not supported.
Web browser	All machines	Internet Explorer 6.0 SP1

Required software for customers of Web Management

Customers of your Website must have a supported Web browser to use the features of Web Management. This section includes the following topics:

- Supported Web browsers on page 69
- Customer HTML Chat Client on page 70
- Known exceptions to Web browser support on page 71
- Exceptions to support of Sun JVM for Website customers on page 72

Supported Web browsers

The following table shows the supported Web browsers for Website features. For information about the Web browsers supported with the customer HTML chat client, see Customer HTML Chat Client on page 70.

Website feature	Windows	Mac
Chat	• Internet Explorer 6 • Internet Explorer 5 • Netscape 6 • Netscape 7 • AOL 7, 8, or 9	• Internet Explorer 5 • Netscape 6 (OS X only) • Netscape 7 • AOL 6 • Safari 1
Page Push (includes Chat)	• Internet Explorer 6 • Internet Explorer 5 • Netscape 6 • Netscape 7 • AOL 7, 8, or 9	• Netscape 6 (OS X only) • Netscape 7 • Safari 1
Collaboration (includes Chat and Page Push) • Customer page send • Page synchronization • Form share	• Internet Explorer 6 • Internet Explorer 5 • Netscape 6 (versions equal to or higher than 6.2.1) • Netscape 7 • AOL 7, 8, or 9	• Netscape 6 (OS X only for versions equal to or higher than 6.2.1) • Netscape 7 • Safari 1
Voice Chat (includes Chat, Page Push, and Collaboration)	• Internet Explorer 6 • Internet Explorer 5 • Netscape 7	Not available

Note:

Customers who use Netscape 6 on MacOS X need to install the MRJPluginCarbon browser plugin and latest version of the Java Runtime OS (MRJ) to access the Website. For more information about the MRJ Plugin Carbon, see http://www.mozilla.org/oji/MRJPluginCarbon.html. For more information about the MRJ, see http://developer.apple.com/java/download.html.

For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Customer HTML Chat Client

The Customer HTML Chat Client is an alternative to the Customer Chat Applet that is also available with Avaya Web Management (Web Management). The Customer HTML Chat Client provides much of the functionality of the Customer Chat Applet in an HTML format that does not require contact center customers to install the Sun JVM on their machines before they can chat with an agent.

The following table describes what operating systems and internet browsers are supported by the Customer HTML Chat Client.

Browser	Version	Operating systems
Internet Explorer	6	• Windows XP • Windows ME • Windows 2000 • Windows 98
	5	• Windows 2000 (5.01 only) • Windows ME (5.5 only) • Mac OS X (5.2.3 only) • Mac OS 9 (5.1.7 only)

Browser	Version	Operating systems
Netscape	7	• Windows XP • Windows 2000 • Windows ME • Windows 98 • Mac OS X (7.2 and higher) • Mac OS 9 (7.0 only)
	6	• Windows XP • Windows 2000 • Windows ME • Windows 98 • Mac OS X (6.2.3 only) • Mac OS 9
AOL	9	• Windows XP • Windows 2000 • Windows ME • Windows 98
	8	• Windows XP • Windows 2000 • Windows ME • Windows 98
Safari	1	• Mac OS X

For more information about the Customer HTML Chat Client, see *IC Administration Volume 2: Agents, Customers, & Queues*.

Known exceptions to Web browser support

The following table describes the restrictions to Web browser support.

Website feature	Known exceptions
Collaboration	Collaboration does not support the following: • For Internet Explorer, Web pages that include iFrames. • For Netscape, Web pages that include layers. • For Netscape 6.2.1 or greater, Collaboration (shared browsing) is not supported when using HTTPS to download the chat client applet.
Colaborative form filling	Available only with Internet Explorer with Microsoft JVM.

Website feature	Known exceptions
Chat with the Customer Chat Applet	Netscape 6.x with the Sun Java Plugin can cause the following: • With Sun Java Plugin 1.3.x, Web browser may fail when a customer runs the chat client more than once in the same browser instance. • With Sun Java Plugin 1.3.0, chat client may not load.
HTTP(S) Tunneling	Chat client communication via HTTP(S) tunneling is not supported on Netscape
Chat and HTTP(S) Tunneling with the Customer Chat Applet	Chat client communication via HTTP(S) tunneling is not supported with the following: • Netscape 6.2 • Sun Java Plugin 1.4.2

Exceptions to support of Sun JVM for Website customers

If you use the Customer Chat Applet, the customer of the Website must have a supported JVM installed to chat with an agent. The Customer HTML Chat Client does not require a supported JVM.

Avaya IC 7.0 does not support the Microsoft JVM, you must install the Sun JVM. For information about where to obtain the Sun JVM, see Installing a Java Virtual Machine plugin for Internet Explorer on page 218.

The following table contains the limitations for Website customers and any workarounds, if available.

Website feature	Known limitation	Workaround
Page Push (includes Chat)	Customer cannot browse to a Web page, then select **Send Page**.	Customer must manually type in URL of the Web page, then select **Send Page** to put the page to the agent.
Form share	Form share, also called form filling, does not work.	-

Website feature	Known limitation	Workaround
Chat with the Customer Chat Applet and Sametime integration	With Sun JVM, the agent will be unable to automatically launch a Sametime session for an existing chat.	The agent must manually schedule a Sametime session on the Sametime server and paste the URL into the chat.
Voice Chat (VOIP)	The VOIP Applet will not work if the customer Internet Explorer browser is configured to work with the 1.4.x versions of the Sun Java Plugin, because of some security exceptions in Java.	The customer must install and use a 1.3.x version of the Sun Java Plugin to use the VOIP applet.

Chapter 3: Guidelines for an Avaya IC deployment

Before you deploy and configure Avaya Interaction Center (Avaya IC), you must plan the components in the system and how those components will be distributed across different machines. Planning an Avaya IC system requires that you understand the needs of the contact center, and that you understand how Avaya IC components work together and with other systems on the network.

If your Avaya IC system includes an integration with Siebel 7, see *Avaya IC for Siebel 7 Integration* for guidelines and planning information. This manual is available on the Avaya IC for Siebel 7 installation CD-ROM.

CAUTION:

Do not install Avaya IC on machines that also host software that filters or controls network access. These types of software can cause Avaya IC to fail or seriously impact performance. For example, pornography filters or software firewalls can affect network access in several ways. They can cause a slowdown in network access, cause applications that open a large number of sockets to fail, or rewrite packets.

This section includes the following topics:

- Performance factors on page 76
- Network topology and configuration guidelines on page 78
- Database guidelines on page 83
- Time zone handling on page 86
- Avaya IC server guidelines on page 88
- Avaya OA server guidelines on page 104
- Avaya OA reporting problems caused by incorrect server deployment on page 108

Tip:

The information in this chapter is general and cannot anticipate the needs of all contact centers. You can consult an Avaya IC specialist to create a deployment strategy that meets the needs of your contact center.

Performance factors

When you plan the deployment of your Avaya IC environment, you must review the answers to the following questions:

- Which Avaya IC components does the contact center require?
- How high do you expect the volume of contacts to be for each component?
- How many concurrently connected users do you expect the system to handle?

The answers to these questions will help you to decide the type and number of hardware components you need for the Avaya IC system, and the best way to distribute the servers among the hardware components.

This section does not provide you with answers to these questions. The answers are different for every Avaya IC system, because the needs of every contact center are different. This section discusses the issues to consider when you answer these questions for a contact center. This section includes the following topics:

- Avaya IC components on page 76.
- Volume of contacts on page 77.
- Number of concurrent users on page 77.

Avaya IC components

The components and the contact rate for an Avaya IC system affect how many machines you need to deploy. For example, a basic Avaya IC system requires:

- At least one server machine for each media
- One machine to host the Design & Administration Tools
- One machine to host the databases and relational database management system
- One machine to host the Avaya OA components
- One client machine for each concurrently active agent

Avaya IC requires additional machines if the system includes more than one site or additional components, such as Business Advocate.

For more information about the recommended number of machines for an Avaya IC system, see the following deployment scenarios:

- Chapter 4: Avaya IC single site deployment scenarios on page 111.
- Chapter 5: Avaya IC multi-site deployment scenarios.

Volume of contacts

Consider the volume of contacts that the contact center handles during peak periods of activity when you determine the following:

Processing power required for the machines that host Avaya IC servers - For example, if your contact center has a high contact delivery rate, ensure that the Avaya IC media servers, which support the contact qualifications and delivery, such as the Telephony server and Workflow server, have sufficient processing power.

Multiple servers to divide the responsibilities for the delivery of contacts - For example, the Workflow server processes the majority of the contacts and business rules. The Workflow server can handle tasks, such as media routing, agent blending, prompting, letter generation, and generic business logic. Distribute these responsibilities across multiple Workflow servers to maximize performance and response from the Workflow server and reduce the impact of one Workflow server on the other Workflow servers in an Avaya IC system.

Response time required for contacts in each media - For example, response time is critical for telephony services. Streamline the contact qualification and routing to ensure that telephony services respond in a timely manner during peak periods. Partition the load horizontally by increasing the number of servers. Configure each Workflow server to access only the database that contains the tables required by the workflows. Develop workflows that perform only a single database operation before the workflows make a routing decision.

Number of concurrent users

Consider the number of agents and other Avaya IC users who are typically logged in concurrently during peak periods of activity. The load in an IC system can be directly related to the number of concurrent users. The larger the user population, the more computational resources required.

To avoid performance issues, distribute the responsibilities for the Avaya IC users between multiple servers on different machines. For example, divide the responsibilities for the Avaya IC users between two ADU servers that are hosted on different machines.

Some servers have limitations on the number of concurrent users. For example, a Telephony server can support approximately 600 to 800 agents depending on the contact rate. If an Avaya IC system includes more than 800 agents who handle voice contacts, consider adding two Telephony servers that are hosted on different machines.

Network topology and configuration guidelines

Network topology and configuration have a direct impact on the performance of Avaya IC client-server communications.

Tip:

Consult with network specialists to determine the optimal network configuration.

This section includes general guidelines for network topology and configuration that typically result in good performance and reliability for Avaya IC. This section includes the following topics:

- Network security on page 78.
- Avaya IC communication protocol on page 78.
- WAN and LAN connections on page 79.
- Remote agents for Avaya Agent on page 79.
- Multiple network interface cards on page 81.
- Firewall guidelines for Avaya Agent on page 82.
- Network and Firewall requirements for Avaya Agent Web Client on page 83

Network security

Make sure that the network provides a minimum of the following security for all machines that host Avaya IC servers and applications:

- Secure physical location
- Properly administered user IDs and permissions
- Protection from network-based attacks
- Regular review of program logs

Avaya IC communication protocol

Avaya IC components use TCP/IP to communicate across the network. Consult the documentation for your network to determine the best configuration to support this communication protocol.

WAN and LAN connections

In general, LAN connectivity has higher bandwidth, lower delay, and is more stable than WAN connectivity.

If your Avaya IC system includes multiple sites that are connected by WANs, Avaya IC assumes and requires reliable WAN connections for proper operation and performance.

Avaya IC requires that backup services be configured on the same LAN. This helps to avoid the increased latency and limited bandwidth when failover occurs across a WAN.

Remote agents for Avaya Agent

If the Avaya IC system includes remote agents, the agents must have a VPN that meets the requirements of Avaya IC and the network must have sufficient bandwidth for each agent. Remote agents can be voice enabled with an IP Telephony solution such as Avaya IP Agent. For example, an Avaya IC system with remote agents could include all Avaya IC servers and the RDBMS located at a data center and the remote agents located at satellite sites.

This section includes the following topics:

- Connections for remote agents on page 79.
- Bandwidth for remote agents on page 80.

Connections for remote agents

CAUTION:

If the VPN that provides the connection does not assign a unique IP address to each remote agent, agents who log in with the same IP address after the first agent may not be able to communicate with certain Avaya IC servers, such as the Telephony server.

If the Avaya IC system includes agents who log in from remote sites, Avaya IC requires the following:

- Every agent must have a high-speed connection with a Virtual Private Network (VPN) client.
- The VPN client must establish a virtual device with a unique IP address for that agent.
- The VPN client must place the device, whether virtual or not, and the associated unique IP address as the first item in the list of devices that is presented to Avaya IC after login, as the IP address of the first device is included in the Avaya IC session ID for that agent.

Bandwidth for remote agents

To properly work in a remote agent environment, the underlying network topology must provide adequate bandwidth and latency. The required operational bandwidth in this table is based on the agent population and the incoming contact rate for each channel that an agent may handle. If the Avaya IC system also includes customization of the EDU, this variable can also change the bandwidth requirement. To estimate the required bandwidth, use the data in the following table and calculation.

Channel	Kilobits per contact
Chat	800
Email (10K message)	800
Voice (Avaya Agent)	480
Voice (Avaya Agent Web Client)	380

For example:

E * (B *2 + 480Kb) + E * (A*P) / 3600

V * 480Kb / 3600

C * (M * S + 480 Kb) / 3600

Where:

- E = number of email contacts per hour
- B = avg size of email body
- A = avg size of email attachment
- P = Percentage of email contact with attachments
- V = number of voice contacts per hour
- C = number of chat contacts per hour
- M = number of chat messages between customer and agent
- S = Average size of chat message

Multiply the value calculated for the channel by the number of agents for an estimate of your bandwidth requirements.

Important:
This value is only an estimate. PSO must be consulted for proper sizing based on the specific needs for the contact center.

Email contact bandwidth - For email contacts, the number of kilobits per contact will depend on the average size of the email message and reply, fequency, and size of attachments.

Chat contact bandwidth - For chat contacts, the number of kilobits per contact will depend on the number of messages exchanged within a single contact as well as the size of each message.

Latency - The latency between the Avaya Agent client and the data center should not exceed 150ms average round trip packet time as measured with “ping” with a 1024 byte data size. Anything greater will result in degraded client response time.

Impact of agent login - The login of an agent can generate a significant volume of traffic. When an agent logs in for the first time, 3MB of data is downloaded to the desktop. The bulk of this traffic consists of IC Scripts for Avaya Agent. Customizations might increase the number of IC Scripts downloaded. Following the initial login, the IC Scripts are cached on the local machine. For all subsequent logins, only changed IC Scripts and the VESP Implementation Repository (vesp.imp) are downloaded to the agent desktop, which can amount to 500KB. The size of the vesp.imp is directly related to the number of servers in the system with an average of 1KB per server.

Multiple network interface cards

You need to plan the assignment of your Network Interface Cards (NICs) if the server machines in your Avaya IC configuration include a supported Windows operating system.

CAUTION:

If you do not configure the correct NIC for Avaya IC, your system may have problems with NIC driver conflicts, Windows operating system errors, and Avaya IC errors.

When you plan the deployment of your Avaya IC system, consider the following guidelines:

First physical NIC - The Web License Manager uses the first physical NIC on the machine. The first physical NIC is the NIC that is located in the first slot in the PCI search order. Typically, this is the NIC closest to the central processor and is connected to the LAN or WAN. This NIC is typically the system default NIC in the registry of a Windows machine.

To verify the location and the physical address of the first physical NIC on the machine that hosts the Web License Manager, see Troubleshooting for license files on page 213.

Note:

Exercise caution when you add a NIC to the machine that hosts Web License Manager, or if you replace a NIC on that machine. Avaya IC license files are defined with the physical address of the NIC. If the physical address changes, the Web License Manager and the Avaya IC system cannot function.

ORB server - Deploy an ORB server for each system that runs Avaya IC servers.

Avaya Definity and Communication Manager switches and software - If your Avaya IC system includes a Telephony server that will communicate with an Avaya Definity G3 or Communication Manager switch and software, the machine that hosts the Telephony Server must have a secondary NIC. Avaya recommends that the secondary NIC be on the same 10Mbps, half-duplex private network segment as the MAPD for the Avaya switch. Variations to this configuration should include careful planning to minimize the higher risk of service failures that can be anticipated from alternate configurations.

Telephony licensing keys - Telephony licensing keys are written to the registry of the machine that hosts the Telephony server. If you change the IP address of the primary NIC or change the primary NIC on that machine, the licensing will be void and your Telephony server will not function properly.

Firewall guidelines for Avaya Agent

To provide security for the network, Avaya IC assumes that the customer Website for Web Management is located in the DMZ of the network, between the following two firewalls:

- Firewall between the Website machine and the internal network where the Avaya IC servers are deployed
- Firewall between the Website machine and the internet

The firewall is a hardware and software component of the network infrastructure. Firewalls can:

- Block certain network traffic in each direction
- Perform IP address translation in both directions
- Unexpectedly break connections

The firewall policy and design have a direct impact on the deployment and performance of Avaya IC components, such as Web Management servers.

DNS domains - In your network, servers outside the firewall may be in a different DNS domain from servers inside the firewall. Typically, DNS domains outside the firewall cannot resolve the names of DNS domains inside the firewall.

Deployment of Avaya IC components outside firewall - Customers require direct access to the Web Management Website to search the Web Self-Service database, or initiate chat contacts with agents in your contact center. Customers can also initiate email contacts from the Website. To make sure that customers do not have direct access to your network, deploy the Website outside the firewall.

Communication through the firewall - Web Management and Email Management components on the Website must communicate with components inside the firewall. This communication might require additional configuration of the operating system on machines that host these components. For example, you might need to add IP addresses to the Hosts table of the operating system on each machine.

Network and Firewall requirements for Avaya Agent Web Client

For Avaya Agent Web Application deployments, the agent desktop, HTTP server and application server must be on the same network. The Avaya Agent Web Client does not work across the public internet that might include proxy or network address translation (NAT) devices. Avaya IC 7.0 does not support network address translation for agent desktops. Remote agent desktops must be connected to the network hosting the application server by means of a VPN.

If there is a firewall between the agent machines that run Avaya Agent Web Client and the machine that hosts IBM WAS, you must open two configurable ports. The two ports are required because Avaya Agent Web Client receives data in real-time rather than by polling. The first port allows incoming HTTP traffic to the server the second port permits the server to notify the client of events. If there is a proxy server, Avaya Agent Web Client can use the proxy server, however, the IP address of the Avaya Agent Web Client must be identifiable and reachable from the machine that hosts IBM WAS.

Database guidelines

Avaya IC servers and client applications depend upon the databases to access, store, and retrieve vital data, including information about customers, contacts, employees, and configuration. Avaya OA uses data stored in the IC Repository database.

This section describes the databases that the components of Avaya IC use and provides some basic guidelines for their implementation and configuration. This section includes the following topics:

- Avaya IC databases on page 84.

- Avaya IC database performance guidelines on page 85.
- Database table limitations on page 86.

Avaya IC databases

The following table shows the databases that Avaya IC uses. An Avaya IC system might not include all of these databases, as some databases are only used by specific components of Avaya IC.

Database	Description
Customer Interaction Repository	Not a database in itself. Refers to the Avaya IC and Avaya OA database and storage components used by an Avaya IC system.
IC Repository	Stores system level information, including the Employee table with agent information. All Avaya IC systems require this database.
CCQ	Stores application level information for Avaya IC agent applications, such as Avaya Agent, Web Management, and Email Management. All Avaya IC systems require this database.
Dialer	Stores information for Outbound Contact. Only Avaya IC systems that include Outbound Contact require this database.
Business Advocate System Store	Stores administration information, such as system parameters, initialization parameters, location of MSMQ queues, location of servers, and the roles of the Resource Manager servers. This database also stores process definition, run time process, and historical data. Each Logical Resource Manager has a dedicated system store. Only Avaya IC systems that include Business Advocate require this databases.
Business Advocate Resource Store	Stores operation information, such as qualifiers, service classes, and agent records and the associated capability sets and profiles. All Resource Manager servers share one Resource store. Only Avaya IC systems that include Business Advocate require this databases.

Database	Description
Siebel 7	Stores information for Avaya IC for Siebel 7. Only Avaya IC systems that include Avaya IC for Siebel 7 require this database.
Avaya OA Real-time database	Stores information required by Avaya OA. For more information, see *Avaya OA Installation and Configuration*. All Avaya IC systems with Avaya OA require this database.
Avaya OA Historical database	Stores information required by Avaya OA. For more information, see *Avaya OA Installation and Configuration*. All Avaya IC systems with Avaya OA require this database.

Avaya IC database performance guidelines

Avaya IC components access the databases through a connection pool provided by the Data server. The performance of the Avaya IC clients and servers depends on:

- Access to the databases to store and retrieve information
- Availability of the databases
- Ability of the databases to process SQL calls effectively from the application software servers and reporting tools

The following guidelines for your database server typically result in good performance and reliability:

Dedicated database machine - Host your database on a dedicated machine. This dedicated location ensures that you can tune your database server to maximize database operations, and can improve the reliability and performance of the database. A poorly performing database server adversely affects Avaya IC performance.

Data server location - Do not install the Data server on the machine that hosts your database server.

Effect of contact volume on Data server - Consider the contact volume in your contact center when you deploy your Data server. In a high volume contact center, you can deploy secondary Data servers on the same machines as data-intensive Avaya IC servers.

Location of database files - Install the following database files on the machine that hosts the Data server:

- Database client software
- Database networking libraries

Client to connection ratio - Allocate a 10 to 1 client to connection ratio for the Data server.

Database sizing for contact records - Assume that each contact record occupies a minimum of 5 to 10 KB of disk space when you size the database.

Database server tuning - Contact your database software vendor for recommendations on tuning a server for a “decision support” type application, with the number of concurrent users and database size appropriate for your application and contact volumes.

Connection pool - Consider the size of the connection pool when you calculate the amount of memory required in megabtyes (MBs). For example, to calculate the amount of memory for Oracle databases, multiply the connection pool size by 3.

Database table limitations

The Avaya IC Data servers for SQL Server and for ODBC databases support a maximum of 255 columns in a select. Do not create tables with more than 255 columns in SQL Server databases and databases that will be access through an Avaya IC Data server for an ODBC database.

Time zone handling

This section describes the ways that different Avaya IC components handle and record dates and times. This section includes the following topics:

- Methods for time zone handling on page 87
- Time zone methods used by Avaya IC components on page 88.

Methods for time zone handling

Avaya IC components can use the following methods to handle and record dates and times.

Host/local - the Avaya IC records the date and time in the local time zone, as configured on the host machine.

Local - The Avaya IC component records the date and time in the local time zone.

RDBMS - The Avaya IC component records the date and time in the time zone used by the Avaya IC databases.

Regional - The Avaya IC component records the date and time in the time zone specified by the Region, as configured in Outbound Contact.

Translated to UTC - The Avaya IC component records and stores the date and time in UTC format. However, when Avaya IC displays the date and time of the event or contact to a user, the date and time is translated into the local time zone of the user.

UTC - The Avaya IC component records the date and time in Coordinated Universal Time (UTC) format.

Time zone methods used by Avaya IC components

The following table shows the ways that each type of Avaya IC component handles time zones.

Origin of time zone	Avaya IC Servers	Outbound Contact	IC Manager	Agent desktop applications
ADL file	Host/local	RDBMS	Host/local	Host/local
Database	UTC	UTC	UTC	UTC
Dates	UTC	Regional	Translated to UTC	Translated to UTC

Avaya IC server guidelines

This section includes general guidelines to consider when you plan your Avaya IC system. Consider these guidelines when you decide how many of each type of server the system requires, which machines will host the servers, where to locate those machines on the network. This section includes the following topics:

- Server naming guidelines on page 89
- Server partitioning guidelines on page 89
- Web License Manager guidelines on page 91
- Co-location of client applications with servers on page 91
- Time synchronization for servers on page 91
- Server failure considerations on page 93
- Avaya IC core server guidelines on page 93
- Voice channel server guidelines on page 98
- Chat channel server guidelines on page 99
- Email channel server guidelines on page 100
- Outbound Contact server guidelines on page 101
- Business Advocate server guidelines on page 101

For more information about server failover guidelines and about individual servers, see *IC Administration Volume 1: Servers & Domains*.

Server naming guidelines

Under certain circumstances, the Workflow server fails to connect with a server that uses the server type as the name of the server. For example, if an ADU server is named "ADU" or a Web Advocate Adaptor server is named "WAA".

To ensure optimal functioning of your Avaya IC system, Avaya recommends that you use the following naming conventions for your Avaya IC servers:

- Always use a unique server name of up to 32 characters long with no spaces.
- Name your Data servers Data_<*databasetype*>_<*domain*>. For example, **Data_Oracle_Default**.
- In a single site environment, name all other servers <*servername*>_<*domainname*>. For example: **ADU_User1**.
- In a multi-site environment, name all other servers <*servername*>_<*sitename*>_<*domainname*>. For example: **ADU_London_User1**.
- Do *not* set the server name to be the same as the server type, or Avaya IC may encounter errors during operation. For example, use **TS_Voice1** as the name of your Telephony server, not just **TS**.

Important:
Do not use the name **localVDU** or **localADU** for EDU or ADU servers. These are used when the servers are taken off-line to prevent communication with other EDU and ADU servers.

Server partitioning guidelines

The correct partitioning of an Avaya IC system is vital to achieve an optimal level of performance and security. Avaya IC servers use two types of partitioning: physical and logical.

This section describes the issues you need to consider when you decide how to partition an Avaya IC system. These issues do not stand alone. Consider these issues with all of the other guidelines in this chapter. This section includes the following topics:

- Physical partitioning on page 90.
- Logical partitioning on page 90.

Physical partitioning

How you deploy the Avaya IC servers on physical server machines in your system defines the physical partitioning of your Avaya IC system. The physical partitioning performs the following functions for Avaya IC:

- Determines the connectivity between servers.
- Defines how hardware and network failures will impact the servers.

You can deploy machines that host Avaya IC servers in a single site on one LAN, or across multiple sites on multiple LANs that are interconnected by WANs.

Logical partitioning

How you group the Avaya IC servers in Avaya IC domains defines the logical partitioning of an Avaya IC system. The Avaya IC domains determine preferred communication paths and how failover functions.

When you set up the domains for an Avaya IC system, you define the following communication paths:

- Between the Avaya IC servers
- Between the Avaya IC servers and the Avaya IC client applications

Important:
Each Avaya IC domain should only contain one server of that type. Certain specific circumstances include exceptions to this rule. For example, the Default domain can include more than ORB server. For more information about recommended logical partitioning of servers, see Chapter 4: Avaya IC single site deployment scenarios on page 111 and Chapter 5: Avaya IC multi-site deployment scenarios on page 143.

Use a common naming convention for your domains to ensure that you can easily identify where a component is deployed. In a multi-site deployment, you should use the following naming convention: `<site>_<service>`, where service represents the media channel or function of the servers in the domain. For example, in an Avaya IC system with a site in Boston, you could name a domain for the voice channel: Boston_VoiceA.

For more information about logical partitioning and how to use Avaya IC domains, see *IC Administration Volume 1: Servers & Domains*.

Web License Manager guidelines

Consider the following guidelines for the Web License Manager when you plan and deploy licensing for Avaya IC. The following guidelines can help to optimize the performance of an Avaya IC system:

- Location of Web License Manager

  Install at least one Web License Manager at each site.

  If you install a WebLM at each site, WAN segmentation should not prevent an Avaya IC server or client from getting the appropriate licenses. In the deployment scenarios with redundancy, the Core server machines at each site host a WebLM. This configuration has no significance except to reduce the total number of machines.

- Failover for Web License Manager

  You can install multiple WebLMs at each site for local physical redundancy. In this configuration, the license file should be segmented equally. Perform recursive segmentation to achieve local site redundancy. In the event of a catastrophic machine failure, other WebLM servers will redistribute the failed machines licenses for seventy-two hours.

Co-location of client applications with servers

Do not install agent desktop applications or the Design & Administration Tools on a machine that hosts Avaya IC servers or Avaya OA servers.

Installing client applications on server machines impacts the amount of available machine resources such as CPU and memory. This impact results in decreased performance and scalability of the servers.

As a general rule, host agent desktop applications or Design & Administration Tools on machines that will not impact server performance.

Time synchronization for servers

All servers require time synchronization. This requirement ensures that Avaya IC and Avaya OA maintain consistent time. If time is not synchronized, your reports may not be consistent. The clocks on all the server machines must also be synchronized to track issues in log files.

To achieve time synchronization if you do not have an existing infrastructure, install NTP (Network Time Protocol) software on all machines that host Avaya IC servers and Avaya OA servers. You can use a commercial time synchronization application that includes the

ability to provide gradual clock corrections over time such as Windows Time Service. Avaya IC may fail with timeout errors if you change the system clock in large increments (for example, more than two to three seconds per minute).

CAUTION:

Do not use batch scripts that periodically set the time. These scripts and tools are not accurate enough for the Avaya OA databases.

The following table describes the time synchronization utilities that you can use for each operating system supported by Avaya IC and Avaya OA.

Operating system	Time synchronization utility
Windows	Third party NTP utility. Avaya has successfully tested Tardis 2000 v1.4 with Avaya OA, and the time adjustment increments in milliseconds, as set out below. You can obtain a copy of Tardis shareware at the following Website: http://www.kaska.demon.co.uk.
Solaris	Third party NTP utility. Avaya has successfully tested the Solaris `ntpd` process.
AIX	Third party NTP utility. Avaya has successfully tested the AIX `ntpd` process.

Tardis can make large time changes at unpredictable times, instead of gradual adjustments. These large changes can cause some service requests to time out. For example, the ORB server and ORB NT service may not start automatically when you restart the machine.

To avoid this timeout problem with Tardis, set the time adjustment increments in milliseconds, as follows:

1. From the Windows Control Panel, open Tardis.
2. Adjust the following settings:
   - Maximum correction allowed set in a range from the minimum of 50 milliseconds to a maximum of 500 milliseconds.
   - How often the time is set to Every Minute.

For more information, see the Online Help provided with Tardis.

Server failure considerations

Whenever possible, design an Avaya IC system to ensure that failure of a single server does not impact all agents. Consider the following limitations when you design an Avaya IC system:

- Process redundancy limitations

  Web Management and Email Management do not support process redundancy. If the WebACD server or Email server fails, Avaya IC may not be able to route contacts for one or both of those media channels. To avoid this level of failure, consider whether to deploy a cold standby duplicate of the machines that host servers for the email and Web channels.

Avaya IC core server guidelines

Consider the following guidelines for the Avaya IC core servers when you plan and deploy those servers. These guidelines can help to optimize the performance of an Avaya IC system.

This section includes the following topics:

- ADU server guidelines on page 93
- Data server guidelines on page 94
- Directory server and Alarm server guidelines on page 94
- ORB server guidelines on page 95
- Notification server guidelines on page 96
- Report server guidelines on page 96
- Workflow server guidelines on page 96

ADU server guidelines

ADU servers support Avaya IC accounts for agents and administrators. Consider the following guidelines when you plan the deployment of ADU servers:

- ADU server limitations

  An ADU server can handle events from approximately 500 agents. Avaya recommends that you include a minimum of two ADU servers at each site.

- ADU server failover

  Do not configure agent domains to failover to an ADU server that:

  - Is not monitored by an Event Collector server at the same site

- Is monitored by an Event Collector server at a different site

- ADU persistence

  If the Avaya IC system requires ADU persistence, follow the guidelines for EDU persistence in EDU server guidelines on page 95.

Data server guidelines

Consider the following guidelines when you determine where to locate the Data servers in an Avaya IC system:

- Data server location

  Do not install the Data server on the machine that hosts your database server.

- Network location for Data server machine

  Locate machines that host a Data server topologically close to the machine that hosts the Avaya IC databases on a high-speed backbone. Avaya IC generates the bulk of database access traffic between the Data servers and the database server. This configuration minimizes network bandwidth.

- Data server and DUStore server location

  When on the same LAN as the database, install a Data server on every machine that hosts a DUStore server. Configure the DUStore server to use this Data server. Also host a backup Data server on another machine. This configuration minimizes network traffic and minimizes failure modes.

- Data server and Report server location

  When on the same LAN as the database, install a Data server on every machine that hosts a Report server. Configure the Report Server to use this Data server. Also host a backup Data server on another machine. This configuration minimizes network traffic and minimizes failure modes

  For more information about databases and the Data servers, see Database guidelines on page 83.

Directory server and Alarm server guidelines

In a multi-site deployment, when Avaya IC is deployed across a WAN, install a Directory server and Alarm server on every LAN.

These servers are critical for the operation of the other Avaya IC servers. If you have a Directory server and Alarm server on every LAN, a site can still function even if the WAN goes down.

EDU server guidelines

Consider the following guidelines when you set up an EDU server for an Avaya IC system:

- Multiple EDU servers

  Install a separate EDU server for every media channel domain. Different media channels have different requirements for configuring the EDU server to ensure optimal processing.

- Email EDU server configuration

  Configure the EDU server that processes email contacts as described in the following table.

Configuration parameter	Description
Enable EDU persistence	EDU persistence writes EDU information to the DUStore server based on the checkpoint interval setting and limits the EDU Server memory usage. If there is a failure in your system, Avaya IC can then reconstruct the emails in queue.
Checkpoint every five minutes	The Checkpoint feature ensures that Avaya IC persists changes to an EDU at the end of the checkpoint interval. This setting also minimizes the number of email EDUs in a queue that are lost if the EDU server fails.

- EDU limitations

  The EDU has a limitation if the contact center includes some Avaya IC agents and some agents who do not work in Avaya IC. Avaya IC cannot track an EDU outside the Avaya IC system.

  For example, if an Avaya IC agent transfers a contact out of Avaya IC to a non-Avaya IC agent, then Avaya IC terminates the EDU for that contact. Avaya IC considers the contact to be retired. If an agent transfers the contact back to an Avaya IC agent, Avaya IC assigns a second EDU to the contact.

  As a result, the same contact has two EDUs. This limitation can create problems with tracking and reporting for that contact.

ORB server guidelines

All machines that host Avaya IC servers require an ORB server. If a machine does not include an ORB server, you cannot start Avaya IC servers on that machine.

You must install an ORB server:

- On every machine that hosts Avaya IC servers (except the ICM server, CIRS server, and VMM server)

- For every network interface on a multi-homed machine with which an Avaya IC server needs to communicate

For guidelines on how to install and configure Avaya IC on a machine with multiple network cards, see Multiple network interface cards on page 81.

Notification server guidelines

Ensure that the Notification server has access to an SMTP email server to send alert messages.

Report server guidelines

Install a Report server on every machine that hosts an EDU server. This configuration minimizes failure modes and network traffic.

Workflow server guidelines

Consider the following guidelines when you set up a Workflow server for an Avaya IC system:

- Location of Workflow servers

  To mitigate the impact of a failure due to customized workflows, keep Workflow servers logically separate. For example, create a Workflow server for each media and host those servers with other servers that are specific to the same media.

- Customization of workflows

  Workflow servers typically have many external interfaces, such as interfaces to the database and Prompter. Because the Workflow server is scriptable and extensible, Avaya cannot test all possible customizations and usages as part of the out-of-the-box product.

  Customized workflows can be less reliable than the sample workflows and can impact the performance of other servers. Avaya recommends that you thoroughly test all customized workflows, including possible failure scenarios.

- Load partitioning

  Deploy several Workflow servers to provide general load partitioning for contacts, and to limit the types of workflows run by each Workflow server. If you limit the types of workflows, you minimize the possibility that a workflow will impact the performance of other Avaya IC system functions.

  Your Avaya IC system should include separate Workflow servers for the following:

  - Each Blender server in your Avaya IC system
  - Each media channel in your Avaya IC system
  - Each agent workgroup that uses Prompter

- Other utility functions run by the Workflow server, such as periodic tasks

You can configure a Workflow server for each machine that hosts media-specific servers. For example, create a Workflow server for each machine that hosts a Telephony server.

- Coupling between Blender server, Workflow server, and ADU server

  A tight coupling between the Blender server, Workflow server, and ADU server is critical for agent login and for agent channel assignment.

  If you install redundant servers, or the contact center requires higher available of agents, include the following in your deployment:

  - Install at least two sets of Blender server, Workflow server, and ADU server on every LAN in the Avaya IC system that includes agent desktop applications.
  - Configure each set of servers to fail over to the other set of servers.

  Split the agent population on the LAN between the two sets of servers. Each agent group should use one set of servers and use the second set as a backup. This set of servers is critical for agent login and agent channel assignment. If you split your agents across two sets of servers, a single server (or machine) failure cannot disable your contact center. One group of agents can continue uninterrupted operation while the other group restores connections through failover.

  Note:

  Some deployments do not include an ADU server in a user domain. Those deployments include the Blender server and Workflow server in the user domain, and the ADU server in a media domain. Those deployments also ensure that the failover is configured correctly for the user domains and the failover domains. For more information about how to configure the failover, see Chapter 4: Avaya IC single site deployment scenarios on page 111 and Chapter 5: Avaya IC multi-site deployment scenarios on page 143.

- Workflow server and Business Advocate

  Configure at least one Workflow server on the same machine as every Telephony Services Adaptor server and Web Advocate Adaptor server. This Workflow server handles the qualification and exceptions of all the contacts for that server. If the Telephony Services Adaptor server or Web Advocate Adaptor server handles a high volume of contacts, assign multiple Workflow servers to that server. The Telephony Services Adaptor server or Web Advocate Adaptor server can distribute contacts evenly between the assigned Workflow servers.

- Workflow server and email qualification

  To improve email processing throughput, run email qualification workflows on a different Workflow server than the email analysis workflows. Email analysis should always occur on a dedicated machine in the Email domain.

  Depending upon the volume of incoming email contacts, email qualification can occur on:

- The same Workflow server as chat qualification for a contact center with a low to medium volume of email and chat contacts.
- A dedicated Workflow server for a contact center with a medium to high volume of email and chat contacts.

Voice channel server guidelines

Consider the following guidelines for the Avaya IC servers that are specific to the voice channel when you plan and deploy those servers. These guidelines can help to optimize the performance of an Avaya IC system.

This section includes the following topics:

- Telephony server guidelines on page 98.
- Telephony Queue Statistics server guidelines on page 98.
- DUStore server for voice guidelines on page 99.

Telephony server guidelines

Locate your Telephony server in the same LAN as the associated telephony switch and software. This location provides Avaya IC telephony services with high-speed access to telephony devices, such as telephony switches or IVRs.

Telephony Queue Statistics server guidelines

Consider the following guidelines when you plan the deployment of Telephony Queue Statistics (TSQS) servers:

- Potential queue limitations

  If there are more than 500 queues defined on the system, the TSQS server may timeout in a failover situation.

- Configuration requirements for multiple TSQS servers

  Do not configure more than one TSQS server with the same Site and ACD Name. If you configure redundant TSQS servers with the same Site and ACD name, both servers will attempt to create and update the ADU for the queue. This simultaneous update can cause the following problems:

  - Incorrect and duplicate data in Avaya OA reports
  - Problems with creation of multiple ADUs
  - Failure of both TSQS servers

- Backup TSQS servers

  If the Avaya IC system requires a backup TSQS server, configure:

  - The backup TSQS server NOT to autostart
  - The backup Telephony server for the queue as the first server in the TS Set list for the Voice Device in IC Manager

DUStore server for voice guidelines

If you enable EDU persistence in the EDU server that handles voice contacts, the DUStore server must be in the same domain as the EDU server for voice contacts. If the DUStore server and EDU server are not in the same domain, the Avaya IC system will not be able to properly route voice contacts.

Chat channel server guidelines

Consider the following guidelines for the Avaya IC servers that are specific to the chat channel when you plan and deploy those servers. These guidelines can help to optimize the performance of an Avaya IC system.

This section includes the following topics:

- Attribute server guidelines on page 99.
- DUStore server for chat guidelines on page 99.
- ICM server and CIRS server guidelines on page 100.
- Web Management servers guidelines on page 100.

Attribute server guidelines

Install an Attribute server in the DMZ on the machine that hosts your Avaya IC Website if your Avaya IC system records datawake information.

An Attribute server inside the firewall can record datawake information. However, if you install an Attribute server on the Website machine, you will reduce network traffic across the firewall.

DUStore server for chat guidelines

If you enable EDU persistence in the EDU server that handles chat contacts, the DUStore server must be in the same domain as the EDU server for chat contacts. If the DUStore server and EDU server are not in the same domain, the Avaya IC system will not be able to properly route chat contacts.

ICM server and CIRS server guidelines

If you expect a high volume of customer interaction and chat contacts on the Web Management Website, you can add more than one ICM server to increase the number of supported chat contacts and permit greater scalability.

If the Avaya IC system includes more than one ICM server:

- Configure a CIRS server to provide load balancing for the ICM servers.
- Host each ICM server on a separate machine

Web Management servers guidelines

Provide Web Management servers with high-speed access to Web and email servers.

Email channel server guidelines

Consider the following guidelines for the Avaya IC servers that are specific to the email channel when you plan and deploy those servers. These guidelines can help to optimize the performance of an Avaya IC system.

This section includes the following topics:

- IC Email server guidelines on page 100
- DUStore server for email guidelines on page 100
- Email EDU server guidelines on page 101

IC Email server guidelines

Provide the IC Email server with high-speed access to SMTP email servers and POP3 email servers.

DUStore server for email guidelines

Include the following in the deployment of any Avaya IC system that includes the email channel to minimize network traffic, provide load balancing, and minimize failure modes:

- Configure a secondary DUStore server for the email EDU server only
- Locate the secondary DUStore server on the same machine as the email EDU server
- Configure the email EDU server to use this DUStore server
- In case of a failure of the DUStore server, install and configure a backup DUStore server

Email EDU server guidelines

Verify that persistence is on for the email EDU server

Outbound Contact server guidelines

Consider the following guidelines when you plan the deployment of Outbound Contact servers:

- Outbound Contact servers and Avaya IC sites

  Each Avaya IC site can include only one Dialing Kernel server. The Softdialer servers and associated Telephony servers that are associated with the Dialing Kernel server must be in the same Avaya IC site.

- Outbound Contact servers and Avaya IC domains

  Include the Dialing Kernel server and the associated Softdialer server in the same domain.

Business Advocate server guidelines

This section includes general guidelines to consider when you plan an Avaya IC system that includes Business Advocate. Consider these guidelines when you decide how many of each type of server the system requires, which machines will host the servers, where to locate those machines on the network.

This section includes the following topics:

- Logical Resource Manager guidelines on page 102.
- Resource Manager server guidelines on page 102.
- Business Advocate databases guidelines on page 102.
- Telephony Services Adaptor server guidelines on page 103.
- Web Advocate Adaptor server guidelines on page 104.
- Workflows for Business Advocate guidelines on page 104.

For more information about guidelines that affect Business Advocate, see Event Collector Bridge guidelines on page 107,

Logical Resource Manager guidelines

Consider the following guidelines for each Logical Resource Manager in an Avaya IC system:

- ADU server location

  Install a separate ADU server for each Logical Resource Manager. Host this ADU server on a machine in the same LAN as the Logical Resource Manager.

  This ADU server keeps the Business Advocate statistics for that Logical Resource Manager. Create a redundant ADU server in case of ADU failure.

- ADU server domain

  Create a separate Avaya IC domain for this ADU server. Do not place this ADU server in the same domain as the Resource Manager servers in the Logical Resource Manager.

Resource Manager server guidelines

Consider the following guidelines for each Resource Manager server in an Avaya IC system:

- Resource Manager server domain

  Create a separate domain for each Resource Manager server in an Logical Resource Manager. Do not include more than one Resource Manager server in an Avaya IC domain.

- Operating system

  The Resource Manager server requires a Windows 2000 Server or Windows Server 2003 operating system. You can host other Avaya IC servers on supported Solaris or AIX operating systems.

- Resource Manager location

  Host each Resource Manager server, whether primary or standby, on a separate Windows Server machine. Do not host more than one Resource Manager server on the same machine.

- Resource Manager failover

  Resource Manager servers typically work in pairs, with one active Resource Manager server and one standby Resource Manager server. The standby Resource Manager server becomes the active Resource Manager server if the active server fails.

Business Advocate databases guidelines

For an Avaya IC system that uses DB2 for Avaya IC databases, install an Oracle database or SQL Server database to host the Business Advocate database stores.

Telephony Services Adaptor server guidelines

Consider the following guidelines for each Telephony Services Adaptor server in an Avaya IC system:

- Telephony Services Adaptor server and Telephony server

  Business Advocate requires a tight coupling between the Telephony Services Adaptor server and the Telephony server. These two servers handle voice contacts from a single CTI link on a switch.

- Telephony Services Adaptor server and ADU server

  A Telephony Services Adaptor server may require a dedicated ADU server if Business Advocate includes either or both of the following:

  - A large number of service classes
  - Several Logical Resource Managers
  - Telephony Services Adaptor server location

  Host the Telephony Services Adaptor server on the same machine as the associated Telephony Server. Include both these servers in the same Avaya IC domain.

  For redundancy, host pairs of Telephony Services Adaptor server and Telephony server on two separate machines. The total number of agents on both pairs must not exceed the maximum number of agents supported for one CTI link (MAPD).

- Telephony Services Adaptor server and CTI link

  Install a Telephony Services Adaptor server for each CTI link that processes incoming voice contacts. All incoming voice contacts to be routed by Business Advocate require a Telephony Services Adaptor server.

- Telephony Services Adaptor server and switch

  Install at least one pair of Telephony Services Adaptor server and Telephony server per switch. Each switch must have at least one CTI link controlled by a Telephony Services Adaptor server and Telephony server pair. Even if the switch does not accept incoming voice contacts a Telephony Services Adaptor server and Telephony server pair is required to transfer voice contacts.

- Telephony Server Adaptor server and failover

  The Telephony Server Adaptor server does not use the domain mechanism for failover. If the Telephony server or the Telephony Server Adaptor server fails, voice contact routing in Business Advocate fails over to the switch.

Web Advocate Adaptor server guidelines

Consider the following guidelines for each Web Advocate Adaptor server in an Avaya IC system:

- Web Advocate Adaptor server and WebACD server

  Business Advocate requires a tight coupling between the Web Advocate Adaptor server and WebACD server. These two servers handle all chat contacts and email contacts in an Avaya IC system.

- Web Advocate Adaptor server location

  Install a Web Advocate Adaptor server on the same machine as the WebACD server. Include both these servers in the same Avaya IC domain.

Workflows for Business Advocate guidelines

Consider the following guidelines for each Workflow server that runs Business Advocate workflows in an Avaya IC system:

- Qualification workflows and exception workflows

  Run Business Advocate qualification workflows and exception workflows on the same dedicated Workflow server.

- Voice qualification workflows

  Configure at least one Workflow server for every Telephony Services Adaptor server in a LAN. Depending on the volume of voice contacts, multiple Workflow servers can run voice qualification workflows for a single Telephony Services Adaptor server.

Avaya OA server guidelines

The Event Collector server is the Avaya OA server that acts as a bridge between the ADU server in Avaya IC and the real-time subsystem in Avaya OA. The Event Collector server collects ADU data from the ADU server and delivers the data to the real-time subsystem.

In addition to the guidelines in the previous sections, consider the guidelines in this section when you deploy Avaya OA with your Avaya IC system. This section includes the following topics:

- Event Collector server guidelines on page 105
- Event Collector Bridge guidelines on page 107
- Event Collector server failover guidelines on page 107

Event Collector server guidelines

This section describes the guidelines to follow when you deploy the Avaya OA Event Collector server and Real-time subsystem in an Avaya IC system. This section includes the following topics:

- Location of Event Collector server on page 105
- Event Collector server and Avaya IC domains on page 105
- Event Collector server and Avaya IC sites on page 105
- Event Collector server and ADU servers on page 105
- Event Collector server and Telephony on page 106
- Event Collector server and Business Advocate on page 106
- Limitations on ADU data collection on page 106

Location of Event Collector server

Install the Event Collector on a machine with the following:

- Avaya OA real-time subsystem
- Avaya IC secondary ORB server

For a single site, you can install all Avaya OA components on the same machine if the event traffic does not exceed the capacity of the machine.

Event Collector server and Avaya IC domains

Create a dedicated domain for the Event Collector server.

The Event Collector server does not need to be in the same domain as an ADU server.

Event Collector server and Avaya IC sites

Install and configure an Event Collector server and Avaya OA real-time subsystem for each Avaya IC site where an ADU server monitors agents. This Event Collector server must monitor all agent ADU servers at that site.

Event Collector server and ADU servers

The Event Collector server must monitor all ADU servers in an Avaya IC system.

Install the Event Collector server as follows:

- If each Avaya IC site in your system includes ADU servers that are located on multiple machines, install the Event Collector server on a different machine.

- If each Avaya IC site in your system includes all ADU servers on the same machine and that machine has sufficient RAM and processor speed, you can install the Event Collector server on the same machine as the ADU servers.

Event Collector server and Telephony

Ensure that the site administered for the Event Collector server matches the site administered for the Telephony servers in use at the site.

The Event Collector server does not receive voice queue ADU events from Telephony servers that are configured for different sites. The Event Collector server expects to receive Queue ADU data from all email and Web ADU servers across all sites. These ADU events are delivered via proxy through the local ADU server. However, voice ADU events are treated differently. These events are also delivered by proxy, but they are filtered based on the site specified in the Event Collector administration when you create and configure the Event Collector server.

Event Collector server and Business Advocate

For Avaya IC systems with Business Advocate, the Event Collector server must monitor the following ADU servers:

- The ADU server where the Telephony Services Adaptor server records the service class detail records. This ADU server is typically in the same domain as the Telephony server, or in a domain that fails over from the domain of the Telephony server.
- The ADU server where the Web Advocate Adaptor server records the service class detail records. This ADU server is typically in the same domain as the WebACD server, or in a domain that fails over from the domain of the WebACD server.
- The ADU server where the Resource Manager server records the service class state records. This ADU server is typically on the same machine as the Resource Manager server.

Limitations on ADU data collection

Limit ADU data collection from an Event Collector server to local site ADU servers and the proxying of remote ADU data through the local site ADU servers.

This configuration assumes that the local domain ADU handles agent data, and that the proxy data consists of queue statistics for the local site. Do not proxy agent ADU data, because this creates a proxy overhead of large agent ADU volumes. Collect agent ADU data directly from the Agent ADU server on the same physical system.

Event Collector Bridge guidelines

In an Avaya IC system, the Event Collector Bridge queries Business Advocate for administrative information and processes all administration-related events.

This section describes the guidelines to follow when you deploy an Event Collector Bridge. This section includes the following topics:

- Minimum deployment on page 107.
- Event Collector Bridge and Resource Manager server on page 107.

Minimum deployment

Install a minimum of two Event Collector Bridges in an Avaya IC system.

Event Collector Bridge and Resource Manager server

Install multiple Event Collector Bridges on each machine that hosts a Resource Manager server.

The Event Collector Bridge requires access to the same Windows Message Queuing service (MSMQ) as the Resource Manager server. Multiple Event Collector Bridges can compete for access to the MSMQ, but only one can use MSMQ.

This deployment provides redundancy and helps to ensure availability if an Event Collector Bridge fails.

Tip:

The deployment scenarios show only one Event Collector Bridge per Resource Manager server. However, redundancy requires a minimum of two Event Collector Bridges for each Resource Manager server.

Event Collector server failover guidelines

The following configuration guidelines for failover minimize the potential loss of data if an ADU server fails. If you follow these guidelines and an ADU server fails, each agent who logged in through that ADU server will fail over to another ADU server in the failover configuration. Because both ADU servers will be monitored by the same Event Collector server, Avaya OA will record the agent data correctly.

Consider the following when you configure failover for the Event Collector server and ADU servers in your Avaya IC system:

- Failover for Event Collector server

  You cannot configure failover for an individual Event Collector server with its Real-time subsystem. The Event Collector servers must be in agent domains that failover to other Event Collector server domains.

- Failover for ADU servers in agent domains

  Ensure that ADU servers in agent domains never failover to an ADU server that is not monitored by an Event Collector server.

  Normal failover paths may result in an agent ADU entry being created in the ADU server that the Telephony server and WebACD server use for queue ADU entries. This “channel ADU server” is not monitored by an Event Collector. Therefore, Avaya OA cannot report on the failed-over agents. Use the “Server Groups” feature of the channel ADU servers to ensure that no requests from agent domains are resolved to this server.

- Failover for ADU servers in agent domains across multiple sites

  Do not configure ADU servers in agent domains to failover to an ADU server at another site, unless both sites are monitored by a single Event Collector server.

- Failover for non-agent ADU servers

  Configure all ADU servers in non-agent domains to accept only failover requests from other ADU servers in non-agent domains.

Avaya OA reporting problems caused by incorrect server deployment

If you do not follow the guidelines for deploying and configuring the Event Collector server and ADU servers, your Avaya OA reports will be missing data or will contain incorrect data. This section describes some of the problems that can occur if you do not follow these guidelines.

This section includes the following topics:

- Agent fails over to an ADU server that is monitored by a different Event Collector server on page 109
- An agent fails over to an ADU server that is not monitored by an Event Collector server on page 109
- Two Event Collector servers monitor the same agent domains on page 109

For more information about OA server guidelines, see Avaya OA server guidelines on page 104, and *Avaya OA Installation and Configuration*.

Agent fails over to an ADU server that is monitored by a different Event Collector server

For a brief period, the agent may appear to be logged in on both real-time sources simultaneously. Avaya OA will track contacts in progress at the time of failover incorrectly. However, subsequent contacts will be tracked correctly. Historical data for the agent will be associated with multiple sources.

This configuration is not recommended for the following reasons:

- Real-time report users encounter difficulty monitoring specific agents. A real-time report can only view data within a single real time database. If an agent fails over to an ADU server that is monitored by a different Event Collector, the data for that agent is collected into a different real-time database.
- To view all relevant data, supervisors need to run a separate report for each real-time database where an agent may be represented.
- Some data anomalies occur during the interval when the failover occurred. For example, an agent's data is spread between two real-time databases. Certain data about the contact in progress will be lost.
- Historical report users encounter difficulty monitoring specific agents. To improve the performance of reports, the historical data is summarized into daily, weekly, and monthly summaries using containers. To correctly track the agent, you must add an entry for the agent to the container for each real-time database that contains data for the agent. Unfortunately, you cannot add these entries until after the failover has occurred.

An agent fails over to an ADU server that is not monitored by an Event Collector server

Avaya OA does not collect data for that agent after the failover. The agent will appear to be logged out.

Two Event Collector servers monitor the same agent domains

Avaya OA does not currently support this configuration.

If you configure two Event Collector servers to monitor the same agent domains, your Avaya OA system includes two real-time databases with the same real-time data.

Although this could provide some redundancy to your system and ensure that if one Event Collector server or Real-time subsystem fails, the other continues to collect data. However, you will encounter the following problems if you use this configuration:

- The real-time reports do not support duplicate real-time data in multiple real-time databases. Report users will need to be aware of the redundant databases and choose an appropriate source to monitor.
- If an Event Collector server fails, Avaya OA does not provide a failure indication to real-time report users. Report users will see stale, unchanging data and will not receive an indication that the user needs to switch to another source.
- After an Event Collector server recovers, interval data will be incomplete and will not match the other real-time database. No mechanism is available to resynchronize the databases.
- Historical data will be duplicated across sources, doubling the amount of database space required to store Avaya IC summary data. Historical data during intervals when an Event Collector failed will not match between the sources.
- Historical reports may show misleading data if containers are administered that contain data from multiple duplicated sources. Data items that contain counts will be double counted, and data collected during intervals when an Event Collector server failed may be difficult to interpret.

Chapter 4: Avaya IC single site deployment scenarios

This section includes scenarios of sample deployments for an Avaya IC system in a single site. These scenarios estimate an average system load for a site with fewer than 1,200 agents. If your plan includes an Avaya IC site with a high system load, or more than 1,200 agents, you must adapt the deployment scenario.

This section includes the following scenarios:

- Adapting deployment scenarios on page 111
- Rules for items not shown in the deployment scenarios on page 114
- Scenario 1: Single site, voice only on page 114
- Scenario 2: Business Advocate for single site, voice only on page 118
- Scenario 3: Business Advocate for single site, high volume voice on page 121
- Scenario 4: Single site, multi-channel on page 125
- Scenario 5: Single site, multi-channel with high volume voice on page 130
- Scenario 6: Business Advocate for single site, multi-channel on page 135
- Scenario 7: Single site, chat and email only on page 138

If your Avaya IC system includes an integration with Siebel 7, see *Avaya IC for Siebel 7 Integration* for deployment guidelines, which is available on the Avaya IC for Siebel 7 CD-ROM.

Adapting deployment scenarios

You can adapt the recommended deployment scenarios to meet the specific needs of a contact center. This section includes some suggestions about how and when to adapt these scenarios.

This section includes the following topics:

- Adding more servers and domains on page 112

- Deploying servers on multi-processor machines on page 112
- Including additional server machines in a deployment on page 113
- Co-locating servers on one machine on page 113

Adding more servers and domains

These deployment scenarios show the recommended number of machines, servers, and domains. If you expect an extremely high volume of contacts or a high volume of database lookups, you can adjust the scenario to include additional servers and domains.

For example, if the Avaya IC system will have a high volume of database searches and lookups, you can add an additional Data server on each machine and place those Data servers in dedicated domains. For an example of how to deploy a "Data" domain and configure the failover for that domain and the other domains in the system, see Scenario 1: Single site, voice only on page 114.

Deploying servers on multi-processor machines

These deployment scenarios show servers on separate machines. With enough CPU capacity, memory, and disk resources, you can host some Avaya IC servers on different processors in multi-processor machines.

You might host Avaya IC servers on multi-processor machines if you need to reduce the number of server machines in an Avaya IC system. However, this deployment reduces the physical redundancy in the system. If that single machine fails, you would lose all servers on that machine.

If the plan for an Avaya IC system includes Avaya IC servers on different physical partitions in a multi-processor machine, you must use the Avaya IC Sizing Tool to determine the capacity required for those servers. The Avaya IC Sizing Tool takes the following into account:

- System load
- CPU capacity
- Memory
- Disk resources

Contact your Avaya representative or Avaya Business Partner representative for assistance with the Avaya IC Sizing Tool.

Important:
Do not host IC Manager on a multi-processor machine.

Including additional server machines in a deployment

You can add more server machines in any of these deployment scenarios. These additional machines can:

- Improve throughput and system load capacity.
- Add physical redundancy and failover capacity in the event that a server machine fails.

For example, you can add server machines to improve the throughput and system load capacity for Telephony. The increased number of server machines can support an increased agent population or increased contact rate. These additional server machines would be dedicated to servers in the same domain that serve a single purpose, such as:

- Machines dedicated to servers that support inbound routing, including a Telephony server, TSQS server, EDU server, ADU server, Report server, and Workflow server.
- Machines dedicated to servers that support agent handling, including a Blender server and a Workflow server that support only agents in a specific domain.

Co-locating servers on one machine

You can reduce the number of server machines in any of these deployment scenarios by co-locating some Avaya IC servers on the same machine. You can co-locate servers on a machine if:

- You need to reduce the number of physical machines.
- You do not require the Avaya IC servers on that machine to handle a high system load or provide rapid throughput.
- You do not need physical redundancy and failover for those servers in the event that the server machine fails.
- You ensure that your machine has sufficient CPU and memory capacity to support all co-located services.

For example, if the system load for the chat channel and email channel is relatively light, you can co-locate these services on a single server machine.

Note:

Do not locate all Avaya IC servers on a single machine. Avaya does not support an Avaya IC system with all Avaya IC servers on a single machine.

Rules for items not shown in the deployment scenarios

The following items are not shown in these deployment scenarios but the following rules apply:

- The deployments do not show a RDBMS machine but the RDBMS software must be located on a separate machine.
- The deployment scenarios show only one Event Collector Bridge per Resource Manager server. If you want redundancy, a minimum of two Event Collector Bridges for each Resource Manager server is required.
- The deployments do not show a SMTP/POP server machine, but the SMTP/POP server software must be located on a separate machine.

Scenario 1: Single site, voice only

This scenario is the recommended minimum configuration for a basic Telephony only deployment. If you customize your Telephony deployment, you may need to include additional Avaya IC components.

Topics for this scenario include:

- Scenario 1: Deployment overview on page 114.
- Scenario 1: Avaya IC domain overview on page 115.
- Scenario 1: Partitioning of servers on page 115.
- Scenario 1: Failover strategy on page 117.

Scenario 1: Deployment overview

This scenario shows a potential production system with the following deployment:

- Voice channel only (no other media channels)
- Single site
- Two machines for all Avaya IC servers
- One machine for Avaya OA Event Collector server and Real-time subsystem
- One machine for IC Manager, Database Designer, and Workflow Designer

- One or more machines for agent applications, such as Avaya Agent and Avaya Agent Web Client
- Hardware redundancy
- Server (VESP) failover

Scenario 1: Avaya IC domain overview

The Avaya IC components and Avaya OA servers in this scenario are distributed across the following Avaya IC domains:

- Default
- Core2
- User1
- User2
- Voice1
- Voice2
- Prompter1
- Prompter2
- Data1
- Data2
- OA

These domains use the following naming convention: *<service>*. If you plan to scale the deployment to multiple sites, use a different naming convention for domains, such as *<site>_<service>*.

Scenario 1: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

Some of these components, such as the Web License Manager, are not servers.

The following figure shows the distribution of components on the server machines. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.

ICVoice1

Default
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

User1
1/2 Agents
* Blender
* Workflow

Voice1
* ADU
* EDU
* Dialing Kernel
* Report
* Softdialer
* Telephony
* TSQS
* Workflow
* VOX

Prompter1
* HTTP Connector
* Workflow

Data1
* Data server

X WebLM

ICVoice2

Core2
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

User2
1/2 Agents
* Blender
* Workflow

Voice2
* ADU
* EDU
* Report
* Telephony
* TSQS
* Workflow

Prompter2
* HTTP Connector
* Workflow

Data2
* Data server

X WebLM

OAEvent

Default
* ORB

OA
* Event Collector

X OA-RT

X OA-Historic

X OA-Reports

Scenario 1: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Avaya IC domain in the left column failover to the Avaya IC domains in the right column in the order listed.

Domain	Failover domains
Default	1. Default 2. Core2
Core2	1. Core2 2. Default
User1	1. User1 2. User2 3. Prompter1 4. Prompter2 5. Voice1 6. Voice2 7. Data1 8. Data2 9. Default 10. Core2
User2	1. User2 2. User1 3. Prompter2 4. Prompter1 5. Voice2 6. Voice1 7. Data2 8. Data1 9. Core2 10. Default
Voice1	1. Voice1 2. Voice2 3. Data1 4. Data2 5. Default 6. Core2
Voice2	1. Voice2 2. Voice1 3. Data2 4. Data1 5. Core2 6. Default

Domain	Failover domains
Prompter1	1. Prompter1 2. Prompter2 3. Data1 4. Data2 5. Default 6. Core2 7. Voice1 8. Voice2
Prompter2	1. Prompter2 2. Prompter1 3. Data2 4. Data1 5. Core2 6. Default 7. Voice2 8. Voice1
Data1	1. Data1 2. Default 3. Core2
Data2	1. Data2 2. Core2 3. Default
OA	1. OA 2. Voice1 3. Voice2 4. Default 5. Core2

Scenario 2: Business Advocate for single site, voice only

This scenario extends Scenario 1: Single site, voice only on page 114 to include Business Advocate. This scenario is the recommended minimum configuration to add Business Advocate components to a basic single site, voice only deployment in a contact center which expects a low to medium volume of voice contacts.

Topics for this scenario include:

- Scenario 2: Deployment overview on page 119.

- Scenario 2: Avaya IC domain overview on page 119.
- Scenario 2: Partitioning of Business Advocate servers on page 120.
- Scenario 2: Failover strategy on page 121.

Scenario 2: Deployment overview

This scenario adds Business Advocate servers to the machines that host Avaya IC servers, described in Scenario 1: Deployment overview on page 114. This deployment includes a single Logical Resource Manager with two Resource Manager servers. The Resource Manager server in RM1 is the primary. The Resource Manager server in RM2 is the standby.

If you host:

- Avaya IC servers on Windows, this scenario does not require additional machines.
- Avaya IC servers on Solaris or AIX, this scenario requires two windows machines to host the Resource Manager servers.
- Avaya IC and Avaya OA databases in DB2 on AIX, this scenario requires the following:
  - A Windows or Solaris machine to host the Business Advocate databases. If desired, you can install SQL Server on a machine that hosts a Resource Manager server.
  - An additional Data server on the same machines as the Resource Manager servers to provide Avaya IC with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 2: Avaya IC domain overview

The Business Advocate server components in this scenario are distributed across the following Avaya IC domains in addition to those listed in Scenario 1: Avaya IC domain overview on page 115:

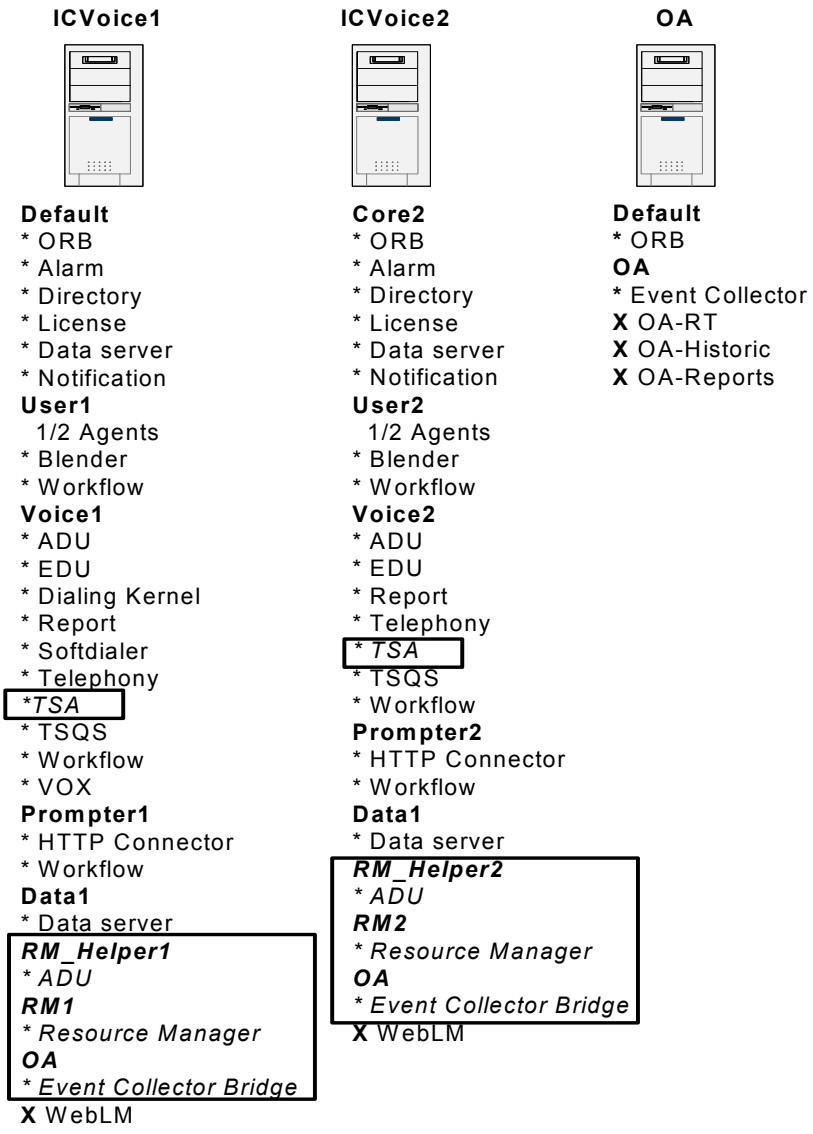
- RM1
- RM2
- RM_Helper1
- RM_Helper2

These domains use the following naming convention: *<service>*. If you plan to scale the deployment to multiple sites, use a different naming convention for domains, such as *<site>_<service>*.

Scenario 2: Partitioning of Business Advocate servers

The physical partitioning of the servers reflects the distribution of the Business Advocate components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

The following figure shows the distribution of Business Advocate servers on the server machines. The highlighted servers are in addition to those components described in Scenario 1: Partitioning of servers on page 115.



Scenario 2: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration*.

The following table shows the failover strategy for the Business Advocate domains in this scenario. The Business Advocate domains do not failover to any of the other Avaya IC domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 1: Failover strategy on page 117.

Domain	Failover domains
RM_Helper1	1. RM_Helper1 2. Default 3. Core2
RM_Helper2	1. RM_Helper2 2. Default 3. Core2
RM1	1. RM1 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2
RM2	1. RM2 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2

Scenario 3: Business Advocate for single site, high volume voice

This scenario is the recommended minimum configuration to add Business Advocate components to Scenario 1: Single site, voice only in a contact center which expects a high volume of voice contacts.

This deployment shows a single Logical Resource Manager with two Resource Manager servers. The Resource Manager server in RM1 is the primary. The Resource Manager

server in RM2 is the standby. The Logical Resource Manager components are hosted on dedicated processors to support the higher volume of contacts.

For more information, see *IC Business Advocate Configuration and Administration*.

Topics for this scenario include:

- Scenario 3: Deployment overview on page 122.
- Scenario 3: Avaya IC domain overview on page 122.
- Scenario 3: Partitioning of Business Advocate servers on page 123.
- Scenario 3: Failover strategy on page 124.

Scenario 3: Deployment overview

This scenario adds Business Advocate servers to the machines that host Avaya IC servers, described in Scenario 1: Deployment overview on page 114. This scenario also adds the following:

- Two machines to host Telephony servers and other Avaya IC servers
- Two machines to host Resource Manager servers and other Avaya IC servers

If you host Avaya IC and Avaya OA databases in DB2 on AIX, this scenario also requires the following:

- A Windows or Solaris machine to host the Business Advocate databases. If desired, you can install SQL Server on a machine that hosts a Resource Manager server.
- An additional Data server on the same machine as a Resource Manager server. This Data server will provide Avaya IC with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 3: Avaya IC domain overview

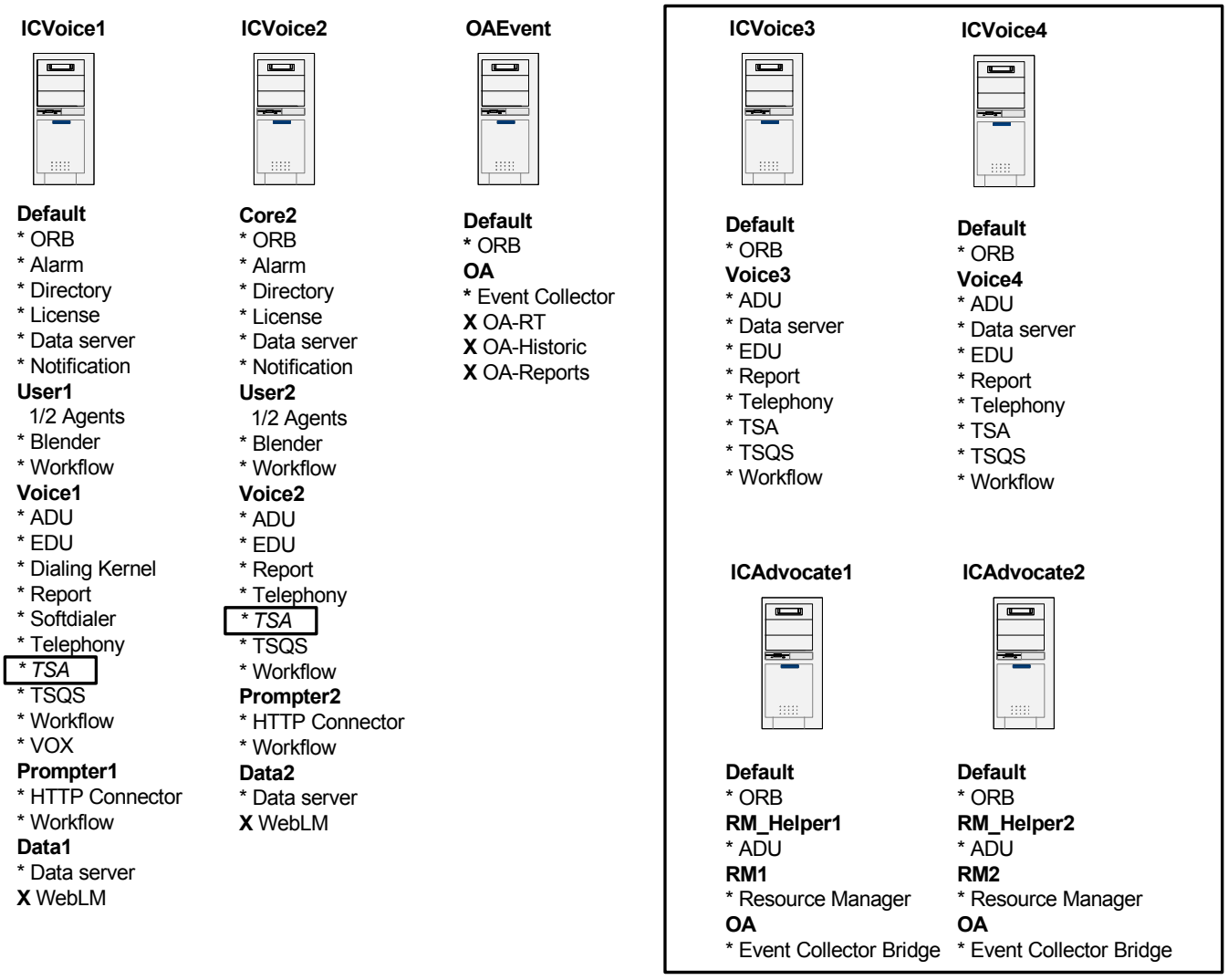
The Business Advocate server components in this scenario are distributed across the following Avaya IC domains in addition to those listed in Scenario 1: Avaya IC domain overview on page 115:

- Voice3
- Voice4
- RM1
- RM2
- RM_Helper1
- RM_Helper2

Scenario 3: Partitioning of Business Advocate servers

The physical partitioning of the servers reflects the distribution of the Business Advocate components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

The following figure shows the distribution of Business Advocate servers on the server machines. The highlighted servers are in addition to those components described in Scenario 1: Partitioning of servers on page 115.



Scenario 3: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration*.

The following table shows the failover strategy for the new Avaya IC domains and the Business Advocate domains in this scenario. For failover information for the domains not listed in this table, see Scenario 1: Failover strategy on page 117.

The Business Advocate domains do not failover to any of the other Avaya IC domains. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
Voice3	1. Voice3 2. Voice4 3. Default 4. Core2
Voice4	1. Voice4 2. Voice3 3. Core2 4. Default
RM_Helper1	1. RM_Helper1 2. Default 3. Core2
RM_Helper2	1. RM_Helper2 2. Default 3. Core2
RM1	1. RM1 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2
RM2	1. RM2 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2

Scenario 4: Single site, multi-channel

This scenario is the recommended minimum configuration for a basic single site, multi-channel deployment. If you customize your multi-channel deployment, you may need to include additional machines and Avaya IC components.

Topics for this scenario include:

- Scenario 4: Deployment overview on page 125.
- Scenario 4: Avaya IC domain overview on page 126.
- Scenario 4: Partitioning of servers on page 127.
- Scenario 4: Failover strategy on page 128.

Scenario 4: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels
- Single site
- One machine for the Website and Web-related servers in the network DMZ
- Four machines for all other Avaya IC servers
- One machine for Avaya OA Event Collector server and Real-time subsystem
- One machine for IC Manager, Database Designer, and Workflow Designer
- One or more machines for agent applications, such as Avaya Agent
- One machine for SMTP and POP servers
- One machine for your RDBMS
- Hardware redundancy
- Server (VESP) failover

Scenario 4: Avaya IC domain overview

The Avaya IC server components in this scenario are distributed across the following Avaya IC domains:

- Default
- Rome_Core2
- Rome_User1
- Rome_User2
- Rome_Voice1
- Rome_Voice2
- Rome_Prompter1
- Rome_Prompter2
- Rome_Web
- Rome_Web_Helper
- Rome_Website
- Rome_Email
- Rome_Email_Helper
- OA

These domains use the following naming convention: <*site*>_<*service*>. For a single site deployment that will not expand to more sites, you can use a different naming convention for domains, such as <*machine_name*>_<*service*>.

Scenario 4: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

The following figure shows the distribution of components on the server machines. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.

ICVoice1

Default
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

Rome_User1
1/2 agents on site
* Blender
* Workflow

Rome_Voice1
* ADU
* EDU
* Dialing Kernel
* Report
* Softdialer
* Telephony
* TSQS
* Workflow
* VOX

Rome_Prompter1
* HTTP Connector
* Workflow

X WebLM

ICVoice2

Rome_Core2
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

Rome_User2
1/2 agents on site
* Blender
* Workflow

Rome_Voice2
* ADU
* EDU
* Report
* Telephony
* TSQS
* Workflow

Rome_Prompter2
* HTTP Connector
* Workflow

X WebLM

ICWeb

Default
* ORB

Rome_Web
* ADU
* Attribute
* Comhub
* Data server
* Paging
* WebACD
* Workflow

Rome_Web_Helper
* EDU
* Report

Rome_Website
* Workflow

ICEmail

Default
* ORB

Rome_Email
* CA Admin
* CA server
* Data server
* IC Email
* Workflow

Rome_Email_Helper
* DUStore
* EDU
* Report server

OAEvent

Default
* ORB

OA
* Event Collector

X OA-RT

X OA-Historic

X OA-Reports

DMZ
ICWebsite

Default
* ORB

Rome_Website
* Attribute

X CIRS

X ICM

X VMM

X Website

Scenario 4: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Avaya IC domain in the left column failover to the Avaya IC domains in the right column in the order listed.

Domain	Failover domains
Default	1. Default 2. Rome_Core2
Rome_Core2	1. Rome_Core2 2. Default
Rome_User1	1. Rome_User1 2. Rome_User2 3. Rome_Prompter1 4. Rome_Prompter2 5. Rome_Voice1 6. Rome_Voice2 7. Default 8. Rome_Core2 9. Rome_Email 10. Rome_Email_Helper 11. Rome_Web 12. Rome_Web_Helper
Rome_User2	1. Rome_User2 2. Rome_User1 3. Rome_Prompter2 4. Rome_Prompter1 5. Rome_Voice2 6. Rome_Voice1 7. Rome_Core2 8. Default 9. Rome_Email 10. Rome_Email_Helper 11. Rome_Web 12. Rome_Web_Helper
Rome_Voice1	1. Rome_Voice1 2. Rome_Voice2 3. Default 4. Rome_Core2
Rome_Voice2	1. Rome_Voice2 2. Rome_Voice1 3. Rome_Core2 4. Default

Domain	Failover domains
Rome_Prompter1	1. Rome_Prompter1 2. Rome_Prompter2 3. Default 4. Rome_Core2 5. Rome_Voice1 6. Rome_Voice2
Rome_Prompter2	1. Rome_Prompter2 2. Rome_Prompter1 3. Rome_Core2 4. Default 5. Rome_Voice2 6. Rome_Voice1
Rome_Email	1. Rome_Email 2. Rome_Email_Helper 3. Rome_Web 4. Default 5. Rome_Core2
Rome_Email_Helper	1. Rome_Email_Helper 2. Rome_Email 3. Default 4. Rome_Core2
Rome_Web	1. Rome_Web 2. Rome_Web_Helper 3. Rome_Email 4. Default 5. Rome_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Rome_Web: Priority Value = 1
Rome_Web_Helper	1. Rome_Web_Helper 2. Rome_Web 3. Default 4. Rome_Core2
Rome_Website	1. Rome_Website 2. Rome_Web 3. Rome_Voice1 4. Default 5. Rome_Core2

Domain	Failover domains
OA	1. OA 2. Rome_Voice1 3. Rome_Voice2 4. Default 5. Rome_Core2

Scenario 5: Single site, multi-channel with high volume voice

This scenario is the recommended minimum configuration for a basic single site, multi-channel deployment in a contact center which expects a high volume of voice contacts. If you customize your multi-channel deployment, you may need to include additional machines and Avaya IC components.

This deployment is similar to Scenario 4: Single site, multi-channel on page 125. However, the Voice services are on dedicated processors to increase their ability to handle higher voice contact transaction rates.

This deployment also shows how you can configure redundancy for Core and Voice services. Telephony Servers are paired for redundancy. Web and Email services do not have redundancy support.

Topics for this scenario include:

- Scenario 5: Deployment overview on page 130.
- Scenario 5: Avaya IC domain overview on page 131.
- Scenario 5: Partitioning of servers on page 131.
- Scenario 5: Failover strategy on page 133.

Scenario 5: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels with high volume voice traffic
- Single site
- One machine for the Website and Web-related servers in the network DMZ
- Six machines for all other Avaya IC servers

- One machine for Avaya OA Event Collector server and Real-time subsystem
- One machine for IC Manager, Database Designer, and Workflow Designer
- One or more machines for agent applications, such as Avaya Agent
- One machine for SMTP and POP servers
- One machine for your RDBMS
- Hardware redundancy
- Server (VESP) failover

Scenario 5: Avaya IC domain overview

The Avaya IC server components in this scenario are distributed across the following Avaya IC domains:

- Default
- Taos_User1
- Taos_User2
- Taos_Voice1
- Taos_Voice2
- Taos_Prompter1
- Taos_Prompter2
- Taos_Core2
- Taos_Web
- Taos_Website
- Taos_Web_Helper
- Taos_Email
- Taos_Email_Helper
- Taos_OA

These domains use the following naming convention: <*site*>_<*service*>. For a single site deployment that will not expand to more sites, you can use a different naming convention for domains, such as <*machine_name*>_<*service*>.

Scenario 5: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

The following figure shows the distribution of components on the server machines. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.

ICCore1

Default
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

Taos_User1
1/2 agents on site
* Blender
* Workflow

Taos_Prompter1
* HTTP Connector
* Workflow

X WebLM

ICCore2

Taos_Core2
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

Taos_User2
1/2 agents on site
* Blender
* Workflow

Taos_Prompter2
* HTTP Connector
* Workflow

X WebLM

ICVoice1

Default
* ORB

Taos_Voice1
* ADU
* EDU
* Dialing Kernel
* Report
* Softdialer
* Telephony
* TSQS
* VOX
* Workflow

ICVoice2

Taos_Core2
* ORB

Taos_Voice2
* ADU
* EDU
* Report
* Telephony
* TSQS
* Workflow

ICWeb

Default
* ORB

Taos_Web
* ADU
* Attribute
* Comhub
* Data server
* Paging
* WebACD
* Workflow

Taos_Web_Helper
* EDU
* Report

Taos_Website
* Workflow

ICEmail

Default
* ORB

Taos_Email
* CA Admin
* CA server
* Data server
* IC Email
* Workflow

Taos_Email_Helper
* DUStore
* EDU
* Report

OAEvent

Default
* ORB

Taos_OA
* Event Collector

X OA-RT

X OA-Historic

X OA-Reports

DMZ ICWebsite

Default
* ORB

Website
* Attribute

X CIRS

X ICM

X VMM

X WebSite

Scenario 5: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Avaya IC domain in the left column failover to the Avaya IC domains in the right column in the order listed.

Domain	Failover domains
Taos_User1	1. Taos_User1 2. Taos_User2 3. Taos_Prompter1 4. Taos_Prompter2 5. Taos_Voice1 6. Taos_Voice2 7. Default 8. Taos_Core2 9. Taos_Email 10. Taos_Email_Helper 11. Taos_Web 12. Taos_Web_Helper
Taos_User2	1. Taos_User2 2. Taos_User1 3. Taos_Prompter2 4. Taos_Prompter1 5. Taos_Voice2 6. Taos_Voice1 7. Taos_Core2 8. Default 9. Taos_Email 10. Taos_Email_Helper 11. Taos_Web 12. Taos_Web_Helper
Taos_Voice1	1. Taos_Voice1 2. Taos_Voice2 3. Default 4. Taos_Core2
Taos_Voice2	1. Taos_Voice2 2. Taos_Voice1 3. Taos_Core2 4. Default

Domain	Failover domains
Taos_Prompter1	1. Taos_Prompter1 2. Taos_Prompter2 3. Default 4. Taos_Core2 5. Taos_Voice1 6. Taos_Voice2
Taos_Prompter2	1. Taos_Prompter2 2. Taos_Prompter1 3. Taos_Core2 4. Default 5. Taos_Voice2 6. Taos_Voice1
Default	1. Default 2. Taos_Core2
Taos_Core2	1. Taos_Core2 2. Default
Taos_Email	1. Taos_Email 2. Taos_Email_Helper 3. Taos_Web 4. Default 5. Taos_Core2
Taos_Email_Helper	1. Taos_Email_Helper 2. Taos_Email 3. Default 4. Taos_Core2
Taos_Web	1. Taos_Web 2. Taos_Web_Helper 3. Taos_Email 4. Default 5. Taos_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Taos_Web: Priority Value = 1
Taos_Web_Helper	1. Taos_Web_Helper 2. Taos_Web 3. Default 4. Taos_Core2

Domain	Failover domains
Taos_Website	1. Taos_Website 2. Taos_Web 3. Taos_Voice1 4. Default 5. Taos_Core2
Taos_OA	1. Taos_OA 2. Taos_Voice1 3. Taos_Voice2 4. Default 5. Taos_Core2

Scenario 6: Business Advocate for single site, multi-channel

This scenario extends Scenario 4: Single site, multi-channel on page 125 to include Business Advocate. This scenario is the recommended minimum configuration to add Business Advocate components to a basic single site, multi-channel deployment in a contact center which does not expect a high volume of contacts.

A single instance of Business Advocate indicates that the Avaya IC system includes only one Logical Resource Manager for Business Advocate. For more information about Logical Resource Managers, see *IC Business Advocate Configuration and Administration*.

Topics for this scenario include:

- Scenario 6: Deployment overview on page 136.
- Scenario 6: Avaya IC domain overview on page 136.
- Scenario 6: Partitioning of Business Advocate servers on page 137.
- Scenario 6: Failover strategy on page 138.

Scenario 6: Deployment overview

This scenario adds Business Advocate servers to the machines that host Avaya IC servers, described in Scenario 4: Deployment overview on page 125.

If you host:

- Avaya IC servers on Windows, this scenario does not require additional machines.
- Avaya IC servers on Solaris or AIX, this scenario requires two Windows machines to host the Resource Manager servers.
- Avaya IC and Avaya OA databases in DB2 on AIX, this scenario requires the following:
  - A Windows or Solaris machine to host the Business Advocate databases. If desired, you can install SQL Server on a machine that hosts a Resource Manager server.
  - An additional Data server on the same machine as a Resource Manager server. This Data server will provide Avaya IC with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 6: Avaya IC domain overview

The Business Advocate server components in this scenario are distributed across the following Avaya IC domains in addition to those listed in Scenario 4: Avaya IC domain overview on page 126:

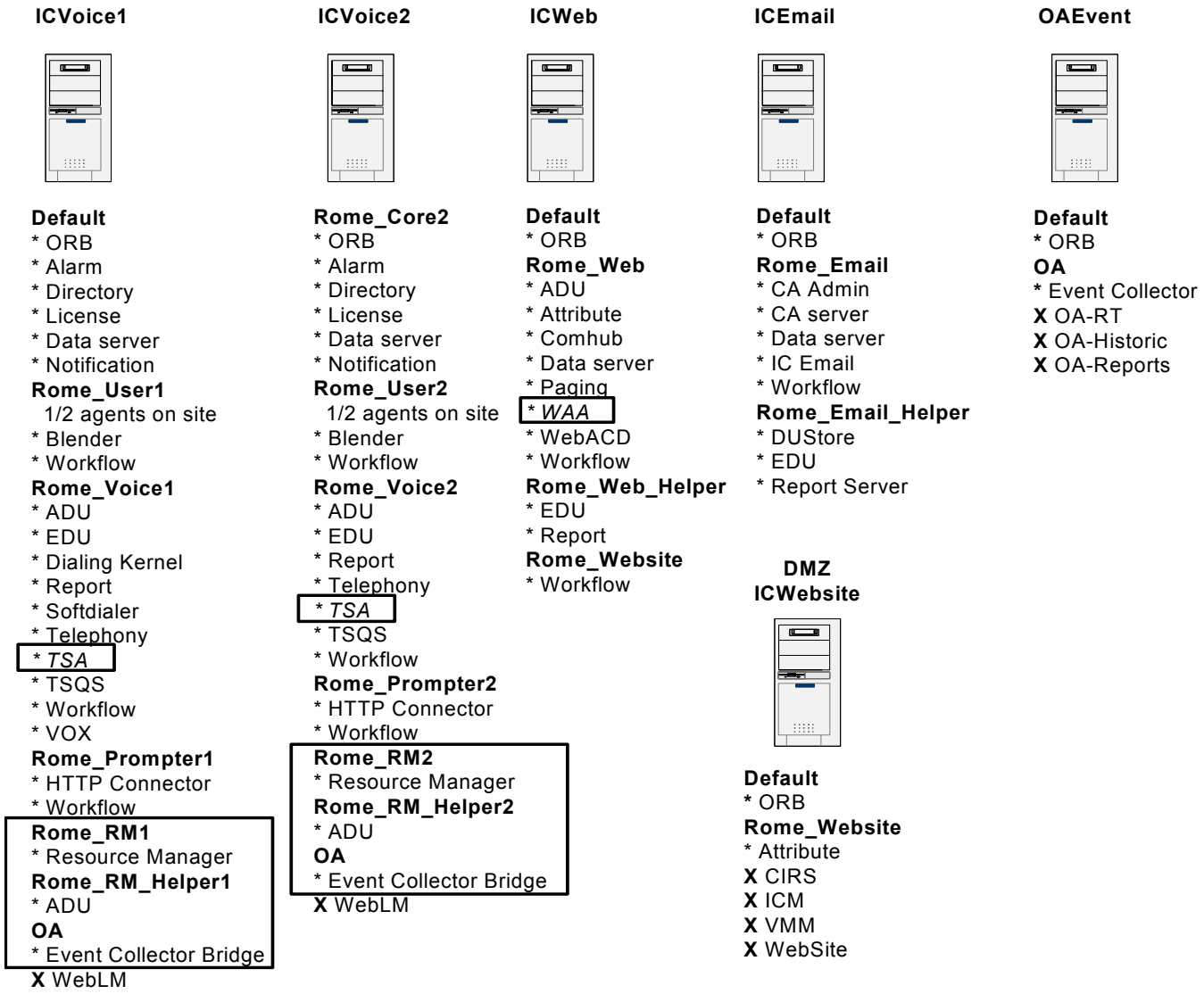
- Rome_RM1
- Rome_RM2
- Rome_RM_Helper1
- Rome_RM_Helper2

These domains use the following naming convention: `<site>_<service>`. For a single site deployment that will not expand to more sites, you can use a different naming convention for domains, such as `<machine_name>_<service>`.

Scenario 6: Partitioning of Business Advocate servers

The physical partitioning of the servers reflects the distribution of the Business Advocate components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

The following figure shows the distribution of Business Advocate servers on the server machines. The highlighted servers are in addition to those components described in Scenario 4: Partitioning of servers on page 127.



Scenario 6: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration*.

The following table shows the failover strategy for the Business Advocate domains in this scenario. The Business Advocate domains do not failover to any of the other Avaya IC domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 4: Failover strategy on page 128.

Domain	Failover domains
RM_Helper1	1. RM_Helper1 2. Default 3. Core2
RM_Helper2	1. RM_Helper2 2. Default 3. Core2
RM1	1. RM1 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2
RM2	1. RM2 2. RM_Helper1 3. RM_Helper2 4. Default 5. Core2

Scenario 7: Single site, chat and email only

This scenario is the recommended minimum configuration for a basic single site deployment in a contact center which includes chat and email channels. This deployment does not include redundancy. If you customize this deployment, you may need to include additional machines and Avaya IC components.

Topics for this scenario include:

- Scenario 7: Deployment overview on page 139.

- Scenario 7: Avaya IC domain overview on page 139.
- Scenario 7: Partitioning of servers on page 140.
- Scenario 7: Failover strategy on page 141.

Scenario 7: Deployment overview

This scenario shows a potential production system with the following deployment:

- Chat and email media channels
- Single site
- One machine for the Website and Web-related servers in the network DMZ
- Two machines for all other Avaya IC servers
- One machine for Avaya OA Event Collector server and Real-time subsystem
- One machine for IC Manager, Database Designer, and Workflow Designer
- One or more machines for agent applications, such as Avaya Agent
- One machine for SMTP and POP servers
- One machine for your RDBMS
- Hardware redundancy
- Server (VESP) failover

Scenario 7: Avaya IC domain overview

The Avaya IC server components in this scenario are distributed across the following Avaya IC domains:

- Default
- Taos_User1
- Taos_Prompter1
- Taos_Web
- Taos_Web_Helper
- Taos_Website
- Taos_Email
- Taos_Email_Helper
- Taos_OA

These domains use the following naming convention: <*site*>_<*service*>. For a single site deployment that will not expand to more sites, you can use a different naming convention for domains, such as <*machine_name*>_<*service*>.

Scenario 7: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

The following figure shows the distribution of components on the server machines. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.

ICWeb

Default
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

Taos_User1
All agents on site
* Blender
* Workflow

Taos_Prompter1
* HTTP Connector
* Workflow

Taos_Web
* ADU
* Attribute
* Comhub
* Data server
* Paging
* WebACD
* Workflow

Taos_Web_Helper
* EDU
* Report

Taos_Website
* Workflow

X WebLM

ICEmail

Default
* ORB

Taos_Email
* CA Admin
* CA server
* Data server
* IC Email
* Workflow

Taos_Email_Helper
* DUStore
* EDU
* Report

OAEvent

Default
* ORB

Taos_OA
* Event Collector

X OA-RT

X OA-Historic

X OA-Reports

DMZ
ICWebsite

Default
* ORB

Taos_Website
* Attribute

X CIRS

X ICM

X VMM

X Website

Scenario 7: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Avaya IC domain in the left column failover to the Avaya IC domains in the right column in the order listed.

Domain	Failover domains
Taos_User1	1. Taos_User1 2. Taos_Prompter1 3. Default 4. Taos_Email 5. Taos_Web 6. Taos_Email_Helper 7. Taos_Web_Helper
Taos_Prompter1	1. Taos_Prompter1 2. Default
Default	1. Default
Taos_Email	1. Taos_Email 2. Taos_Email_Helper 3. Taos_Web 4. Default
Taos_Email_Helper	1. Taos_Email_Helper 2. Taos_Email 3. Default
Taos_Web	1. Taos_Web 2. Taos_Web_Helper 3. Default 4. Taos_Email
Taos_Web_Helper	1. Taos_Web_Helper 2. Taos_Web 3. Default
Taos_Website	1. Taos_Website 2. Default
Taos_OA	1. Taos_OA 2. Taos_Web 3. Default

Chapter 5: Avaya IC multi-site deployment scenarios

This section includes scenarios of sample deployments for an Avaya IC system with two sites. These scenarios estimate an average system load for a site with fewer than 1,200 agents. If your plan includes an Avaya IC site with a high system load, or more than 1,200 agents, you must adapt the deployment scenario.

Tip:

The deployment scenarios show only one Event Collector Bridge per Resource Manager server. However, redundancy requires a minimum of two Event Collector Bridges for each Resource Manager server.

This section includes the following scenarios:

- Scenario 8: Two sites, voice only on page 144
- Scenario 9: Two sites, multi-channel on page 152
- Scenario 10: Single instance Business Advocate for two sites, multi-channel on page 160
- Scenario 11: Multi-instance Business Advocate for two sites, multi-channel on page 164.
- Scenario 12: Two sites, chat and email only on page 170
- Scenario 13: Two sites, multi-channel, data center on page 174
- Scenario 14: Business Advocate for two sites, multi-channel, data center on page 181

If your Avaya IC system includes an integration with Siebel 7, see *Avaya IC for Siebel 7 Integration* for deployment guidelines. This manual is available on the Avaya IC for Siebel 7 installation CD-ROM.

For information on how to adapt these deployment scenarios, see Adapting deployment scenarios on page 111.

Scenario 8: Two sites, voice only

This scenario is the recommended minimum configuration for a basic multi-site, voice media only deployment in a contact center. If you customize your Telephony deployment, you may need to include additional machines and Avaya IC components.

Topics for this scenario include:

- Scenario 8: Deployment overview on page 144
- Scenario 8: Avaya IC domain overview on page 145
- Scenario 8: Partitioning of Avaya IC servers on page 145
- Scenario 8: Failover strategy on page 147

Scenario 8: Deployment overview

This scenario shows a potential production system with the following deployment:

- Voice channel only (no other media channels)
- Two sites (London and Chicago) connected by a WAN
- Two machines at each site for your Avaya IC servers
- One machine at each site for Avaya OA Event Collector server and Real-time subsystem
- One machine for IC Manager, Database Designer, and Workflow Designer
- One machine for agent applications, such as Avaya Agent
- One machine for SMTP and POP servers
- One machine for your RDBMS

  Tip:

  You can locate the RDBMS machine in the London LAN with WAN access from Chicago, or at a third site with WAN access from London and Chicago. If you deploy one of these options, host the Data servers on machines that are local to the RDBMS.

- Hardware redundancy
- Server (VESP) failover

Scenario 8: Avaya IC domain overview

This scenario includes two sites: London and Chicago. The following table shows the Avaya IC domains in each site. The Default domain is used in both sites.

Site 1 – London	Site 2 – Chicago
• London_User1 • London_User2 • London_Voice1 • London_Voice2 • London_Prompter1 • London_Prompter2 • Default • London_Core2 • London_Data1 • London_Data2 • London_OA	• Chicago_User1 • Chicago_User2 • Chicago_Voice1 • Chicago_Voice2 • Chicago_Prompter1 • Chicago_Prompter2 • Chicago_Core1 • Chicago_Core2 • Chicago_Data1 • Chicago_Data2 • Chicago_OA

Scenario 8: Partitioning of Avaya IC servers

The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

This section includes the following topics:

- Partitioning at London site on page 146
- Partitioning at Chicago site on page 147

Partitioning at London site

The following figure shows the distribution of components on the server machines at the London site. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.

London ICVoice1

Default
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

London_User1
1/2 agents on site
* Blender
* Workflow

London_Voice2
* ADU
* EDU
* Dialing Kernel
* Report
* Softdialer
* Telephony
* TSQS
* Workflow
* VOX

London_Prompter1
* HTTP Connector
* Workflow

London_Data1
* Data server

X WebLM

London ICVoice2

London_Core2
* ORB
* Alarm
* Directory
* License
* Data server
* Notification

London_User2
1/2 agents on site
* Blender
* Workflow

London_Voice2
* ADU
* EDU
* Report
* Telephony
* TSQS
* Workflow

London_Prompter2
* HTTP Connector
* Workflow

London_Data2
* Data server

X WebLM

London OAEvent

Default
* ORB

London_OA
* Event Collector

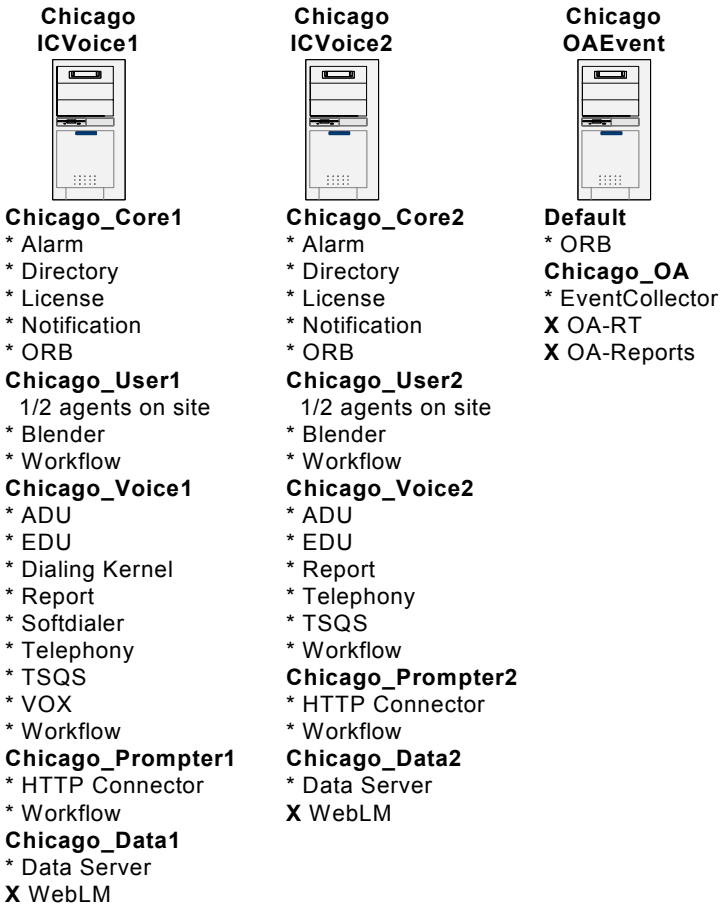
X OA-RT

X OA-Historic

X OA-Reports

Partitioning at Chicago site

The following figure shows the distribution of components on the server machines at the Chicago site. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.



Scenario 8: Failover strategy

This section includes the following topics:

- Failover strategy at London site on page 148
- Failover strategy at Chicago site on page 150

Failover strategy at London site

The following table shows the failover strategy for the London site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
London_User1	1. London_User1 2. London_User2 3. London_Prompter1 4. London_Prompter2 5. London_Voice1 6. London_Voice2 7. Default 8. London_Core2
London_User2	1. London_User2 2. London_User1 3. London_Prompter2 4. London_Prompter1 5. London_Voice2 6. London_Voice1 7. London_Core2 8. Default
London_Voice1	1. London_Voice1 2. London_Voice2 3. Default 4. London_Core2
London_Voice2	1. London_Voice2 2. London_Voice1 3. London_Core2 4. Default
London_Prompter1	1. London_Prompter1 2. London_Prompter2 3. Default 4. London_Core2 5. London_Voice1 6. London_Voice2
London_Prompter2	1. London_Prompter2 2. London_Prompter1 3. London_Core2 4. Default 5. London_Voice2 6. London_Voice1

Domain	Failover domains
London_OA	1. London_OA 2. London_Voice1 3. London_Voice2 4. Default 5. London_Core2
London_Data1	1. London_Data1 2. Default 3. London_Core2
London_Data2	1. London_Data2 2. Default 3. London_Core2
Default	1. Default 2. London_Core2
London_Core2	1. London_Core2 2. Default

Failover strategy at Chicago site

The following table shows the failover strategy for the Chicago site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
Chicago_User1	1. Chicago_User1 2. Chicago_User2 3. Chicago_Prompter1 4. Chicago_Prompter2 5. Chicago_Voice1 6. Chicago_Voice2 7. London_Data1 8. London_Data2 9. Chicago_Core1 10. Chicago_Core2
Chicago_User2	1. Chicago_User2 2. Chicago_User1 3. Chicago_Prompter2 4. Chicago_Prompter1 5. Chicago_Voice2 6. Chicago_Voice1 7. London_Data2 8. London_Data1 9. Chicago_Core2 10. Chicago_Core1
Chicago_Voice1	1. Chicago_Voice1 2. Chicago_Voice2 3. London_Data1 4. London_Data2 5. Chicago_Core1 6. Chicago_Core2
Chicago_Voice2	1. Chicago_Voice2 2. Chicago_Voice1 3. London_Data2 4. London_Data1 5. Chicago_Core2 6. Chicago_Core1

Domain	Failover domains
Chicago_Prompter1	1. Chicago_Prompter1 2. Chicago_Prompter2 3. London_Data1 4. London_Data2 5. Chicago_Core1 6. Chicago_Core2 7. Chicago_Voice1 8. Chicago_Voice2
Chicago_Prompter2	1. Chicago_Prompter2 2. Chicago_Prompter1 3. London_Data2 4. London_Data1 5. Chicago_Core2 6. Chicago_Core1 7. Chicago_Voice2 8. Chicago_Voice1
Chicago_Data1	1. Chicago_Data1 2. Chicago_Core1 3. Chicago_Core2
Chicago_Data2	1. Chicago_Data2 2. Chicago_Core1 3. Chicago_Core2
Chicago_OA	1. Chicago_OA 2. Chicago_Voice1 3. Chicago_Voice2 4. Chicago_Core1 5. Chicago_Core2
Chicago_Core1	1. Chicago_Core1 2. Chicago_Core2 3. Default 4. London_Core2
Chicago_Core2	1. Chicago_Core2 2. Chicago_Core1 3. London_Core2 4. Default

Scenario 9: Two sites, multi-channel

This scenario is the recommended minimum configuration for a basic multi-site, multi-channel deployment. This configuration combines the following previous scenarios:

- York – Scenario 1: Single site, voice only on page 114
- Paris – Scenario 4: Single site, multi-channel on page 125

In this scenario, you add Email and Web domains to the end of the York agent lists to bridge the York agent pools to Paris for non-voice channels. If you customize your multi-site, multi-channel deployment, you may need to include additional machines and Avaya IC components.

Topics for this scenario include:

- Scenario 9: Deployment overview on page 152
- Scenario 9: Avaya IC domain overview on page 153
- Scenario 9: Partitioning of servers on page 153
- Scenario 9: Failover strategy on page 155

Scenario 9: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels
- Two sites connected by a WAN
- Two machines for Avaya IC Telephony components at York
- Five machines for all other Avaya IC components at Paris
- One machine at each site for Avaya OA Event Collector server and Real-time subsystem
- One machine for IC Manager, Database Designer, and Workflow Designer
- One machine for the Website and Web-related servers in the network DMZ
- One or more machines for agent applications, such as Avaya Agent
- One machine for SMTP and POP servers
- One machine for your RDBMS

Tip:

You can locate the RDBMS machine in the York LAN with WAN access from Paris, or at a third site with WAN access from York and Paris.

- Hardware redundancy
- Server (VESP) failover

Scenario 9: Avaya IC domain overview

This scenario includes two sites: York and Paris. The following table shows the Avaya IC domains in each site. The Default domain is used in both sites.

Site 1 – York	Site 2 – Paris
• York_User1 • York_User2 • York_Voice1 • York_Voice2 • York_Prompter1 • York_Prompter2 • York_Core1 • York_Core2 • York_OA	• Paris_User1 • Paris_User2 • Paris_Voice1 • Paris_Voice2 • Paris_Prompter1 • Paris_Prompter2 • Default • Paris_Core2 • Paris_Web • Paris_Web_Helper • Paris_Email • Paris_Email_Helper • Paris_Website • Paris_OA

Scenario 9: Partitioning of servers

The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

This section includes the following topics:

- Partitioning at York site on page 154
- Partitioning at Paris site on page 155

Partitioning at York site

The following figure shows the distribution of components on the server machines at the York site. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.

York ICVoice1

York_Core1
* Alarm
* Directory
* License
* Notification
* ORB

York_User1
1/2 agents on site
* Blender
* Workflow

York_Voice1
* ADU
* EDU
* Dialing Kernel
* Report
* Softdialer
* Telephony
* TSQS
* VOX
* Workflow

York_Prompter1
* HTTP Connector
* Workflow

X WebLM

York ICVoice2

York_Core2
* Alarm
* Directory
* License
* Notification
* ORB

York_User2
1/2 agents on site
* Blender
* Workflow

York_Voice2
* ADU
* EDU
* Report
* Telephony
* TSQS
* Workflow

York_Prompter2
* HTTP Connector
* Workflow

X WebLM

York OAEvent

Default
* ORB

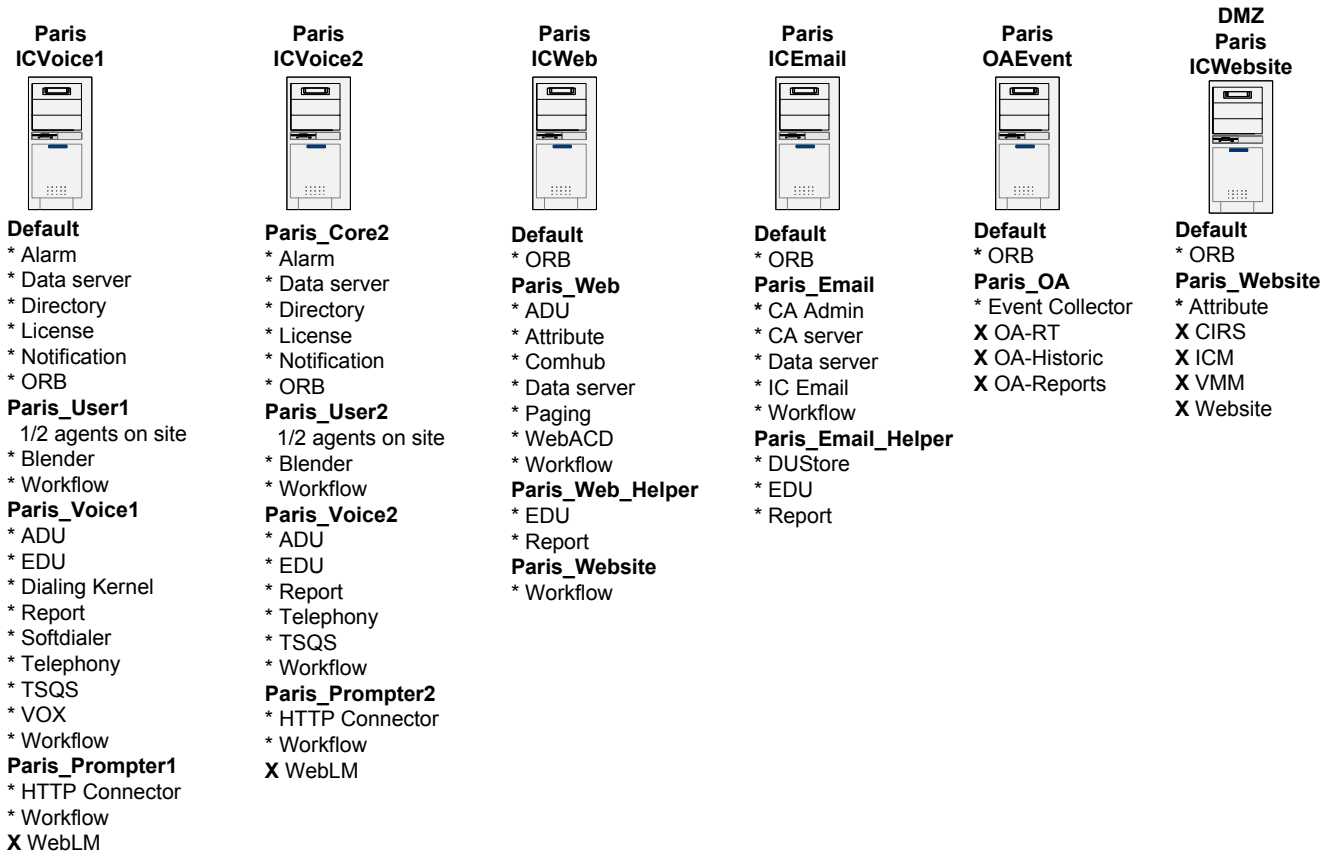
York_OA
* EventCollector

X OA-RT

X OA-Report

Partitioning at Paris site

The following figure shows the distribution of components on the server machines at the Paris site. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.



Scenario 9: Failover strategy

This section includes the following topics:

- Failover strategy at York site on page 156
- Failover strategy at Paris site on page 158

Failover strategy at York site

The following table shows the failover strategy at the York site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
York_User1	1. York_User1 2. York_User2 3. York_Prompter1 4. York_Prompter2 5. York_Voice1 6. York_Voice2 7. York_Core1 8. York_Core2 9. Default 10. Paris_Core2 11. Paris_Email 12. Paris_Email_Helper 13. Paris_Web 14. Paris_Web_Helper
York_User2	1. York_User2 2. York_User1 3. York_Prompter2 4. York_Prompter1 5. York_Voice2 6. York_Voice1 7. York_Core2 8. York_Core1 9. Paris_Core2 10. Default 11. Paris_Email 12. Paris_Email_Helper 13. Paris_Web 14. Paris_Web_Helper
York_Voice1	1. York_Voice1 2. York_Voice2 3. York_Core1 4. York_Core2 5. Default 6. Paris_Core2

Domain	Failover domains
York_Voice2	1. York_Voice2 2. York_Voice1 3. York_Core2 4. York_Core1 5. Paris_Core2 6. Default
York_Prompter1	1. York_Prompter1 2. York_Prompter2 3. York_Core1 4. York_Core2 5. York_Voice1 6. York_Voice2 7. Default 8. Paris_Core2
York_Prompter2	1. York_Prompter2 2. York_Prompter1 3. York_Core2 4. York_Core1 5. York_Voice2 6. York_Voice1 7. Paris_Core2 8. Default
York_OA	1. York_OA 2. York_Voice1 3. York_Voice2 4. York_Core1 5. York_Core2
York_Core1	1. York_Core1 2. York_Core2 3. Default 4. Paris_Core2
York_Core2	1. York_Core2 2. York_Core1 3. Paris_Core2 4. Default

Failover strategy at Paris site

The following table shows the failover strategy at the Paris site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
Paris_User1	1. Paris_User1 2. Paris_User2 3. Paris_Prompter1 4. Paris_Prompter2 5. Paris_Voice1 6. Paris_Voice2 7. Default 8. Paris_Core2 9. Paris_Web 10. Paris_Email 11. Paris_Email_Helper 12. Paris_Web_Helper
Paris_User2	1. Paris_User2 2. Paris_User1 3. Paris_Prompter2 4. Paris_Prompter1 5. Paris_Voice2 6. Paris_Voice1 7. Paris_Core2 8. Default 9. Paris_Web 10. Paris_Email 11. Paris_Email_Helper 12. Paris_Web_Helper
Paris_Voice1	1. Paris_Voice1 2. Paris_Voice2 3. Default 4. Paris_Core2
Paris_Voice2	1. Paris_Voice2 2. Paris_Voice1 3. Paris_Core2 4. Default
Paris_Prompter1	1. Paris_Prompter1 2. Paris_Prompter2 3. Paris_Core2 4. Default 5. Paris_Voice1 6. Paris_Voice2

Domain	Failover domains
Paris_Prompter2	1. Paris_Prompter2 2. Paris_Prompter1 3. Default 4. Paris_Core2 5. Paris_Voice2 6. Paris_Voice1
Default	1. Default 2. Paris_Core2
Paris_Core2	1. Paris_Core2 2. Default
Paris_Email	1. Paris_Email 2. Paris_Email_Helper 3. Paris_Web 4. Paris_Core2 5. Default
Paris_Email_Helper	1. Paris_Email_Helper 2. Paris_Email 3. Paris_Core2 4. Default
Paris_Web	1. Paris_Web 2. Paris_Web_Helper 3. Paris_Email 4. Paris_Core2 5. Default **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Paris_Web: Priority Value = 1
Paris_Web_Helper	1. Paris_Web_Helper 2. Paris_Web 3. Paris_Core2 4. Default
Paris_Website	1. Paris_Website 2. Paris_Web 3. Paris_Voice1 4. Default 5. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Voice1 3. Paris_Voice2 4. Default 5. Paris_Core2

Scenario 10: Single instance Business Advocate for two sites, multi-channel

This scenario extends Scenario 9: Two sites, multi-channel on page 152 to include Business Advocate. This scenario is the recommended minimum configuration to add one instance of Business Advocate to a basic multi-site, multi-channel deployment in a contact center. If you customize your multi-channel deployment, you might need to include additional machines and Avaya IC components.

Note:

This scenario uses the same Workflow servers as Scenario 9: Two sites, multi-channel on page 152. However, to correctly run with Business Advocate, these Workflow servers must run the Business Advocate workflows to qualify and transfer contacts.

A single instance of Business Advocate indicates that the Avaya IC system includes only one Logical Resource Manager for Business Advocate. For more information about Logical Resource Managers, see *IC Business Advocate Configuration and Administration*.

Topics for this scenario include:

- Scenario 10: Deployment overview on page 160
- Scenario 10: Avaya IC domain overview on page 161
- Scenario 10: Partitioning of Business Advocate servers on page 161
- Scenario 10: Failover strategy for Business Advocate domains on page 163

Scenario 10: Deployment overview

This scenario adds Business Advocate servers to some of the machines that host Avaya IC servers, described in Scenario 9: Deployment overview on page 152. This scenario also adds two machines to host the Resource Manager server and other Avaya IC servers in the Paris domain.

If you host Avaya IC and Avaya OA databases in DB2 on AIX, this scenario requires the following:

- A Windows or Solaris machine to host the Business Advocate databases. If desired, you can install SQL Server on a machine that hosts a Resource Manager server.
- An additional Data server on the same machine as a Resource Manager server. This Data server will provide Avaya IC with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 10: Avaya IC domain overview

This scenario includes two sites: York and Paris. The Business Advocate servers in this scenario are distributed across the following Avaya IC domains including those listed in Scenario 9: Avaya IC domain overview on page 153.

The following table shows the Avaya IC domains in each site. The highlighted domains were added to support Business Advocate.

Site 1 – York	Site 2 – Paris
• York_User1 • York_User2 • York_Voice1 • York_Voice2 • York_Prompter1 • York_Prompter2 • York_Core1 • York_Core2 • York_OA	• Paris_User1 • Paris_User2 • Paris_Voice1 • Paris_Voice2 • Paris_Prompter1 • Paris_Prompter2 • Default • Paris_Core2 • Paris_Email • Paris_Email_Helper • Paris_Web • Paris_Web_Helper • Paris_Website • **Paris_OA** • **Paris_RM1** • **Paris_RM2** • **Paris_RM_Helper1** • **Paris_RM_Helper2**

Scenario 10: Partitioning of Business Advocate servers

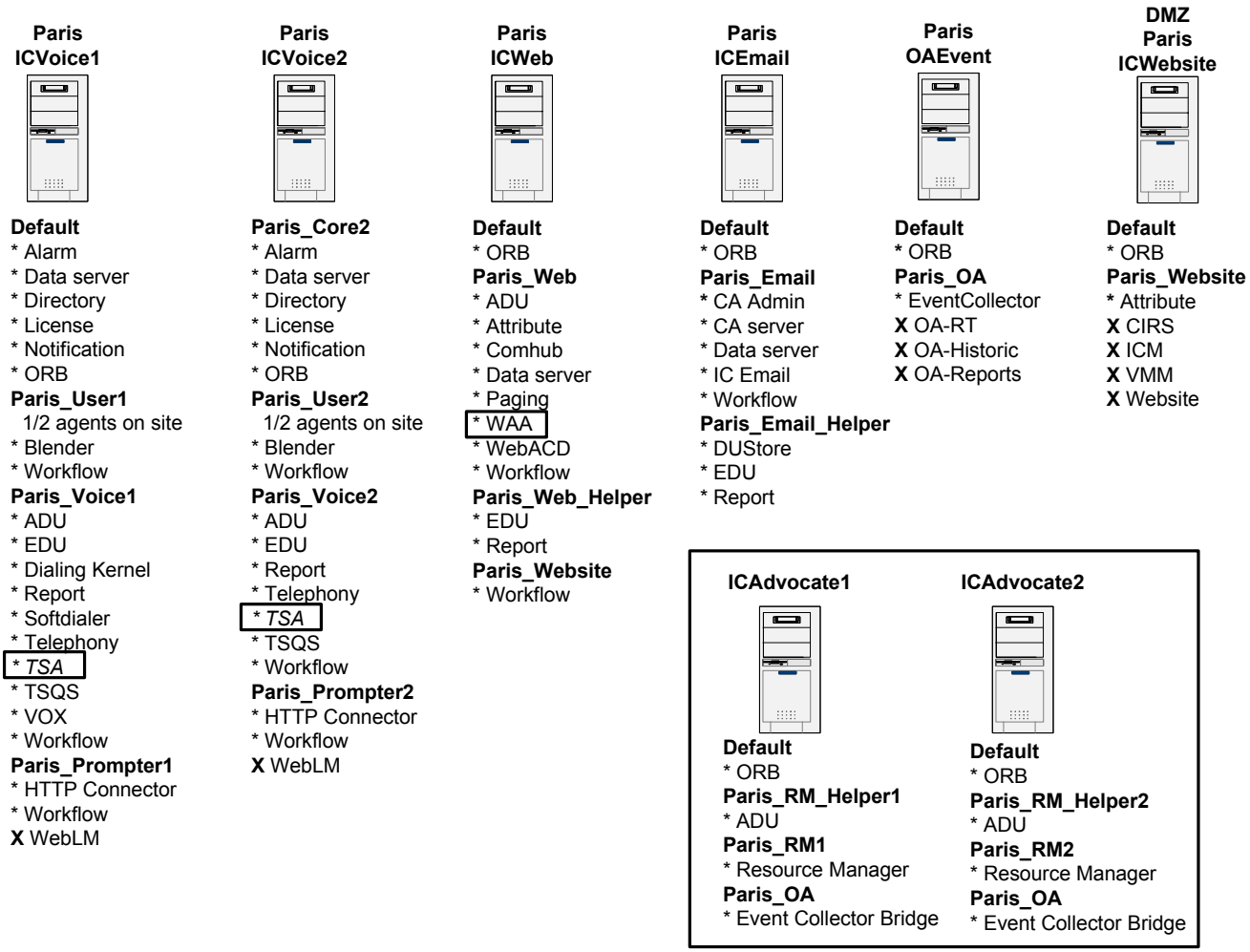
The physical partitioning of the servers reflects the distribution of the Business Advocate components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

This section includes the following topics:

- Partitioning of Business Advocate servers at Paris site on page 162
- Partitioning of Business Advocate servers at York site on page 163

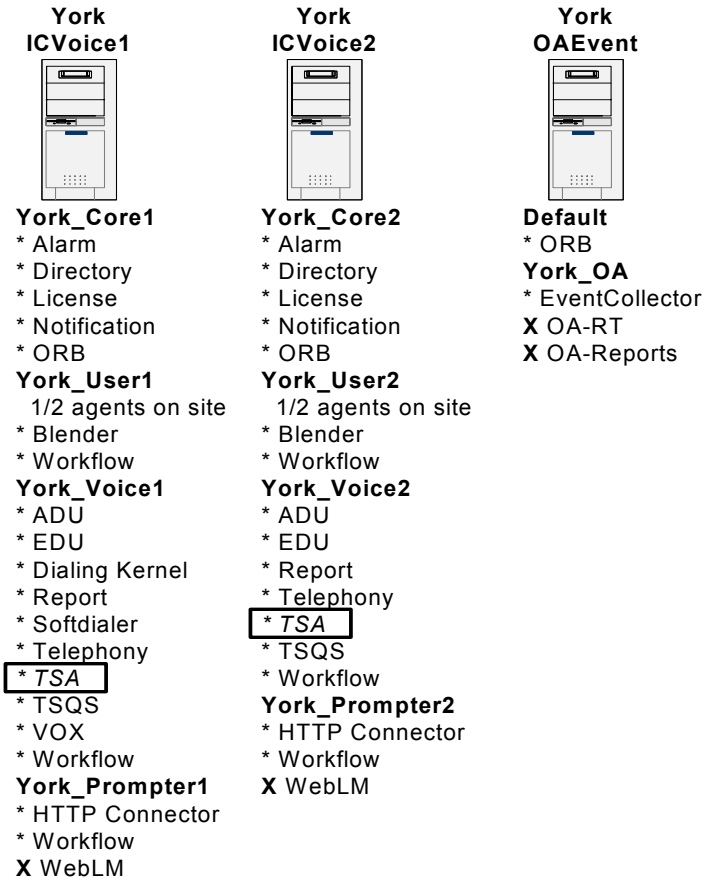
Partitioning of Business Advocate servers at Paris site

The following figure shows the distribution of Business Advocate servers on the server machines at the Paris site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 153.



Partitioning of Business Advocate servers at York site

The following figure shows the distribution of Business Advocate servers on the server machines at the York site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 153.



Scenario 10: Failover strategy for Business Advocate domains

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration*.

The following table shows the failover strategy for the Business Advocate domains in this example. The Business Advocate domains do not failover to any of the other Avaya IC domains. The components in the domain in the left column failover to the domains in the

right column in the order listed. For failover information for the domains not listed in this table, see Scenario 9: Failover strategy on page 155.

Domain	Failover domains
Paris_RM_Helper1	1. Paris_RM_Helper1 2. Default 3. Paris_Core2
Paris_RM_Helper2	1. Paris_RM_Helper2 2. Default 3. Paris_Core2
Paris_RM1	1. Paris_RM1 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_RM2	1. Paris_RM2 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Voice1 3. Paris_Voice2 4. Default 5. Paris_Core2

Scenario 11: Multi-instance Business Advocate for two sites, multi-channel

This scenario extends Scenario 9: Two sites, multi-channel on page 152 to include Business Advocate. This scenario is the recommended minimum configuration to add two instances of Business Advocate to a basic multi-site, multi-channel deployment in a

contact center. If you customize your multi-channel deployment, you might need to include additional machines and Avaya IC components.

Note:

This scenario uses the same Workflow servers as Scenario 9: Two sites, multi-channel on page 152. However, to correctly run with Business Advocate, these Workflow servers must run the Business Advocate workflows to qualify and transfer contacts.

Multi-instance Business Advocate indicates that the Avaya IC system includes more than one Logical Resource Manager for Business Advocate. Each Logical Resource Manager handles a separate population of agents.

You can configure a Logical Resource Manager:

- For groups of agents across all sites who handle specific types of contacts
- For agents in each site

Avaya does not recommend that you configure a Logical Resource Manager for each Telephony switch in an Avaya IC system.

For more information about Logical Resource Managers, see *IC Business Advocate Configuration and Administration*.

Topics for this scenario include:

- Scenario 11: Deployment overview on page 165
- Scenario 11: Avaya IC domain overview on page 166
- Scenario 11: Partitioning of Business Advocate servers on page 167
- Scenario 11: Failover strategy for Business Advocate domains on page 169

Scenario 11: Deployment overview

Use this deployment in the following circumstances:

- To provide on-site physical redundancy.
- To configure Business Advocate for a contact center that exceeds the capacities of a single instance of Business Advocate.

This scenario does not prevent delivery of contacts to another site. If you want to prevent delivery of contacts to another site, you must create a qualifier to represent each site. For more information about qualifiers, see *IC Business Advocate Configuration and Administration*.

This scenario adds Business Advocate servers to some of the machines that host Avaya IC servers, described in Scenario 9: Deployment overview on page 152. This scenario also adds two machines at each site to host a Resource Manager server and an ADU server

If you host Avaya IC and Avaya OA databases in DB2 on AIX, this scenario also requires the following:

- A Windows or Solaris machine to host the Business Advocate databases. If desired, you can install SQL Server on a machine that hosts a Resource Manager server.
- An additional Data server on the same machine as a Resource Manager server. This Data server will provide Avaya IC with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 11: Avaya IC domain overview

This scenario includes two sites: York and Paris. The Business Advocate servers in this scenario are distributed across the following Avaya IC domains including those listed in Scenario 9: Avaya IC domain overview on page 153.

The following table shows the Avaya IC domains in each site. The highlighted domains were added to support Business Advocate.

Site 1 – York	Site 2 – Paris
• York_User1 • York_User2 • York_Voice1 • York_Voice2 • York_Prompter1 • York_Prompter2 • York_Core1 • York_Core2 • York_OA • **York_RM1** • **York_RM2** • **York_RM_Helper1** • **York_RM_Helper2**	• Paris_User1 • Paris_User2 • Paris_Voice1 • Paris_Voice2 • Paris_Prompter1 • Paris_Prompter2 • Default • Paris_Core2 • Paris_Email • Paris_Email_Helper • Paris_Web • Paris_Web_Helper • Paris_Website • **Paris_OA** • **Paris_RM1** • **Paris_RM2** • **Paris_RM_Helper1** • **Paris_RM_Helper2**

Scenario 11: Partitioning of Business Advocate servers

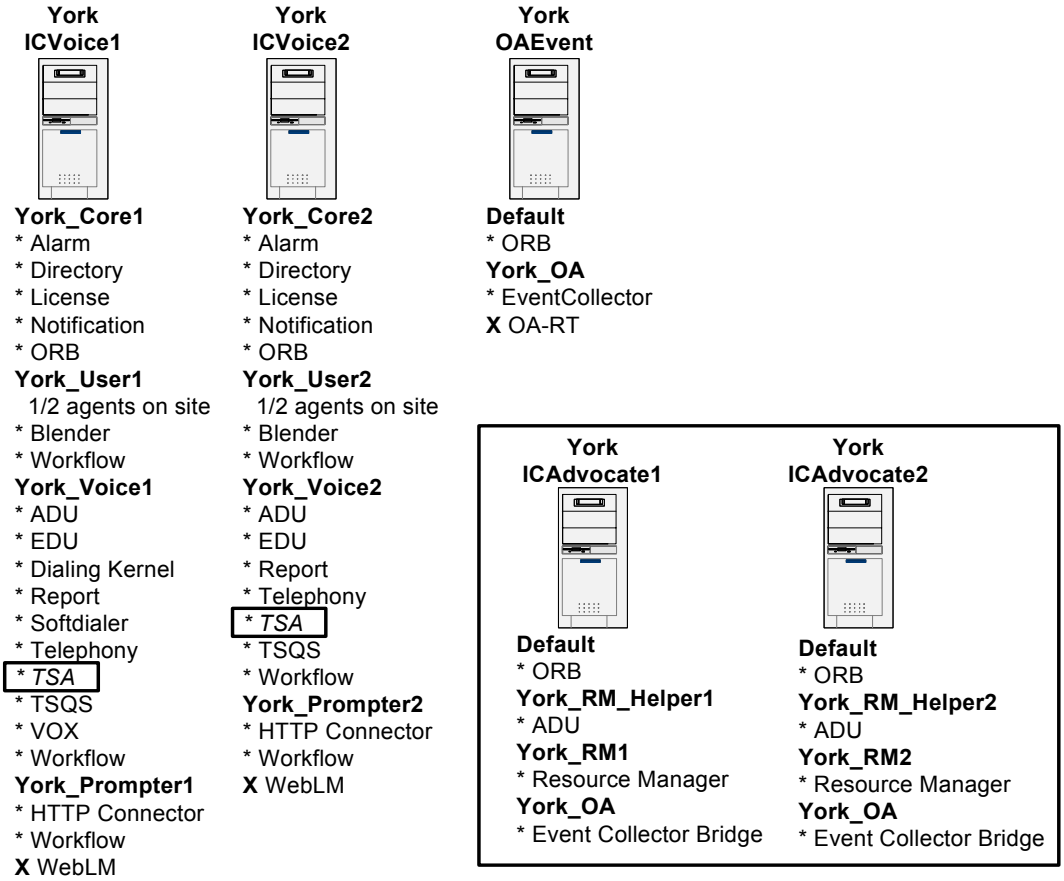
The physical partitioning of the servers reflects the distribution of the Business Advocate components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

This section includes the following topics:

- Partitioning of Business Advocate servers at York site on page 167
- Partitioning of Business Advocate servers at Paris site on page 168

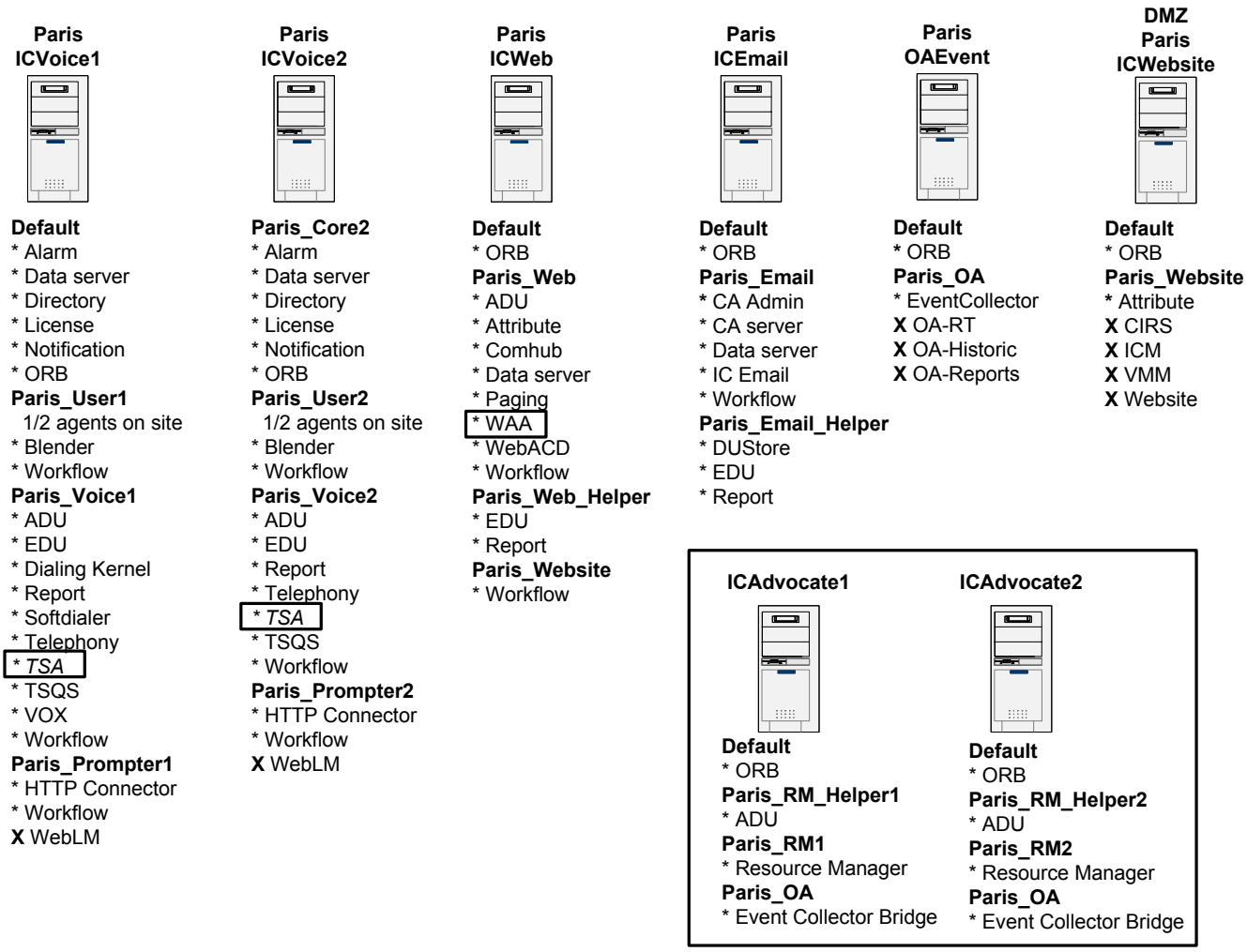
Partitioning of Business Advocate servers at York site

The following figure shows the distribution of Business Advocate servers on the server machines at the York site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 153.



Partitioning of Business Advocate servers at Paris site

The following figure shows the distribution of Business Advocate servers on the server machines at the Paris site. The highlighted servers are in addition to those components described in Scenario 9: Partitioning of servers on page 153.



Scenario 11: Failover strategy for Business Advocate domains

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration*.

This section includes the following topics:

- Failover strategy at York site on page 169
- Failover strategy at Paris site on page 170

Failover strategy at York site

The following table shows the failover strategy for the Business Advocate domains at the York site in this example. The Business Advocate domains do not failover to any of the other Avaya IC domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 9: Failover strategy on page 155.

Domain	Failover domains
York_RM_Helper1	1. York_RM_Helper1 2. York_Core1 3. York_Core2
York_RM_Helper2	1. York_RM_Helper2 2. York_Core2 3. York_Core1
York_RM1	1. York_RM1 2. York_RM_Helper1 3. York_RM_Helper2 4. York_Core1 5. York_Core2
York_RM2	1. York_RM2 2. York_RM_Helper1 3. York_RM_Helper2 4. York_Core2 5. York_Core1
York_OA	1. York_OA 2. York_Voice1 3. York_Voice2 4. York_Core2 5. York_Core1

Failover strategy at Paris site

The following table shows the failover strategy for the Business Advocate domains at the Paris site in this example. The Business Advocate domains do not failover to any of the other Avaya IC domains. The components in the domain in the left column failover to the domains in the right column in the order listed. For failover information for the domains not listed in this table, see Scenario 9: Failover strategy on page 155.

Domain	Failover domains
Paris_RM_Helper1	1. Paris_RM_Helper1 2. Default 3. Paris_Core2
Paris_RM_Helper2	1. Paris_RM_Helper2 2. Default 3. Paris_Core2
Paris_RM1	1. Paris_RM1 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_RM2	1. Paris_RM2 2. Paris_RM_Helper1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Voice1 3. Paris_Voice2 4. Default 5. Paris_Core2

Scenario 12: Two sites, chat and email only

This scenario is the recommended minimum configuration for a basic multi-site deployment in a contact center which includes chat and email channels. If you customize this deployment, you may need to include additional machines and Avaya IC components.

Topics for this scenario include:

- Scenario 12: Deployment overview on page 171

- Scenario 12: Avaya IC domain overview on page 171
- Scenario 12: Partitioning of Avaya IC servers on page 172
- Scenario 12: Failover strategy on page 173

Scenario 12: Deployment overview

This scenario shows a potential production system with the following deployment:

- Chat and email media channels
- Two sites (Taos and Tokyo) connected by a WAN
- One machine for the Website and Web-related servers in the network DMZ
- Two machines in Taos and one machine in Tokyo for all other Avaya IC servers
- One machine for Avaya OA Event Collector server and Real-time subsystem
- One machine for IC Manager, Database Designer, and Workflow Designer
- One or more machines for agent applications, such as Avaya Agent
- One machine for SMTP and POP servers
- One machine for your RDBMS
- Hardware redundancy
- Server (VESP) failover

Scenario 12: Avaya IC domain overview

This scenario includes two sites: Taos and Tokyo. The following table shows the Avaya IC domains in each site.

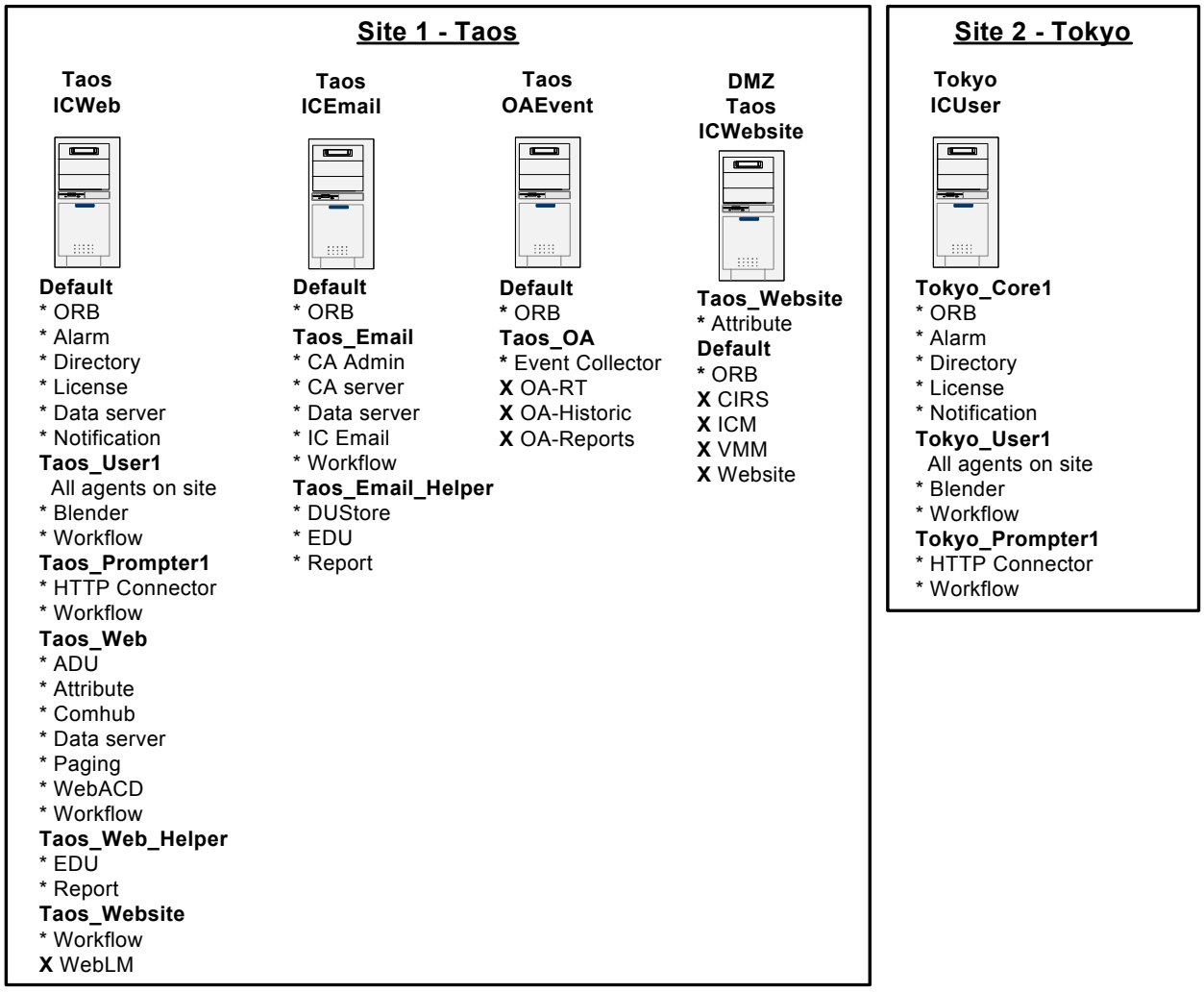
Site 1 – Taos	Site 2 – Tokyo
• Default • Taos_User1 • Taos_Prompter1 • Taos_Email • Taos_Email_Helper • Taos_Web • Taos_Web_Helper • Taos_Website • Taos_OA	• Tokyo_User1 • Tokyo_Prompter1 • Tokyo_Core1

These domains use the following naming convention: *<site>_<service>*. For a single site deployment that will not expand to more sites, you can use a different naming convention for domains, such as *<machine_name>_<service>*.

Scenario 12: Partitioning of Avaya IC servers

The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

The following figure shows the distribution of components on the server machines at both sites. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.



Scenario 12: Failover strategy

The following table shows the failover strategy in this scenario. The components in the Avaya IC domain in the left column failover to the Avaya IC domains in the right column in the order listed.

Domain	Failover domains
Taos_User1	1. Taos_User1 2. Taos_Prompter1 3. Default 4. Taos_Email 5. Taos_Web 6. Taos_Email_Helper 7. Taos_Web_Helper
Taos_Prompter1	1. Taos_Prompter1 2. Default
Default	1. Default 2. Tokyo_Core1
Taos_Email	1. Taos_Email 2. Taos_Email_Helper 3. Taos_Web 4. Default
Taos_Email_Helper	1. Taos_Email_Helper 2. Taos_Email 3. Default
Taos_Web	1. Taos_Web 2. Taos_Web_Helper 3. Default 4. Taos_Email
Taos_Web_Helper	1. Taos_Web_Helper 2. Taos_Web 3. Default
Taos_Website	1. Taos_Website 2. Default
Taos_OA	1. Taos_OA 2. Taos_Web 3. Default

Domain	Failover domains
Tokyo_User1	1. Tokyo_User1 2. Tokyo_Core1 3. Default 4. Tokyo_Prompter1 5. Taos_Email 6. Taos_Web 7. Taos_Email_Helper 8. Taos_Web_Helper
Tokyo_Prompter1	1. Tokyo_Prompter1 2. Tokyo_Core1 3. Default
Tokyo_Core1	1. Tokyo_Core1 2. Default

Scenario 13: Two sites, multi-channel, data center

This scenario is a modification of Scenario 9: Two sites, multi-channel on page 152 to include a single data center. Both sites access the data center.

In this scenario, the site with the data center includes the RDBMS, all Data servers, the Event Collector server, Web servers, and Email servers. The data center does not support agents or Voice servers. The second site includes all agents and Voice servers. You can deploy several satellite sites with the same configuration, but different domains, as the second site.

To implement a data center, the WAN connection between the sites must have sufficient bandwidth and must always be available to prevent any disruption to service that a single site dependency can cause.

Topics for this scenario include:

- Scenario 13: Deployment overview on page 175
- Scenario 13: Avaya IC domain overview on page 175
- Scenario 13: Partitioning of servers on page 176
- Scenario 13: Failover strategy on page 177

Scenario 13: Deployment overview

This scenario shows a potential production system with the following deployment:

- All media channels
- Two sites connected by a WAN
- Six machines for the data center, Web components, and Email components at the Paris site
- Two machines for agent services and Voice components at the York site
- One machine for the Avaya OA Event Collector server and Real-time subsystem at each site
- One machine for IC Manager, Database Designer, and Workflow Designer
- One machine for the Website and Web-related servers at the Paris site, in the network DMZ
- One or more machines for agent applications, such as Avaya Agent
- One machine for SMTP and POP servers
- One machine for your RDBMS at the Paris site
- Hardware redundancy
- Server (VESP) failover

Scenario 13: Avaya IC domain overview

This scenario includes two sites: York and Paris. The following table shows the Avaya IC domains in each site. The Default domain is used in both sites.

Site 1 – Paris	Site 2 – York
• Default • Paris_Core2 • Paris_Email • Paris_Email_Helper • Paris_Web • Paris_Web_Helper • Paris_Website • Paris_Data1 • Paris_Data2 • Paris_OA	• York_Core1 • York_Core2 • York_User1 • York_User2 • York_Voice1 • York_Voice2 • York_Prompter1 • York_Prompter2 • York_OA

Scenario 13: Partitioning of servers

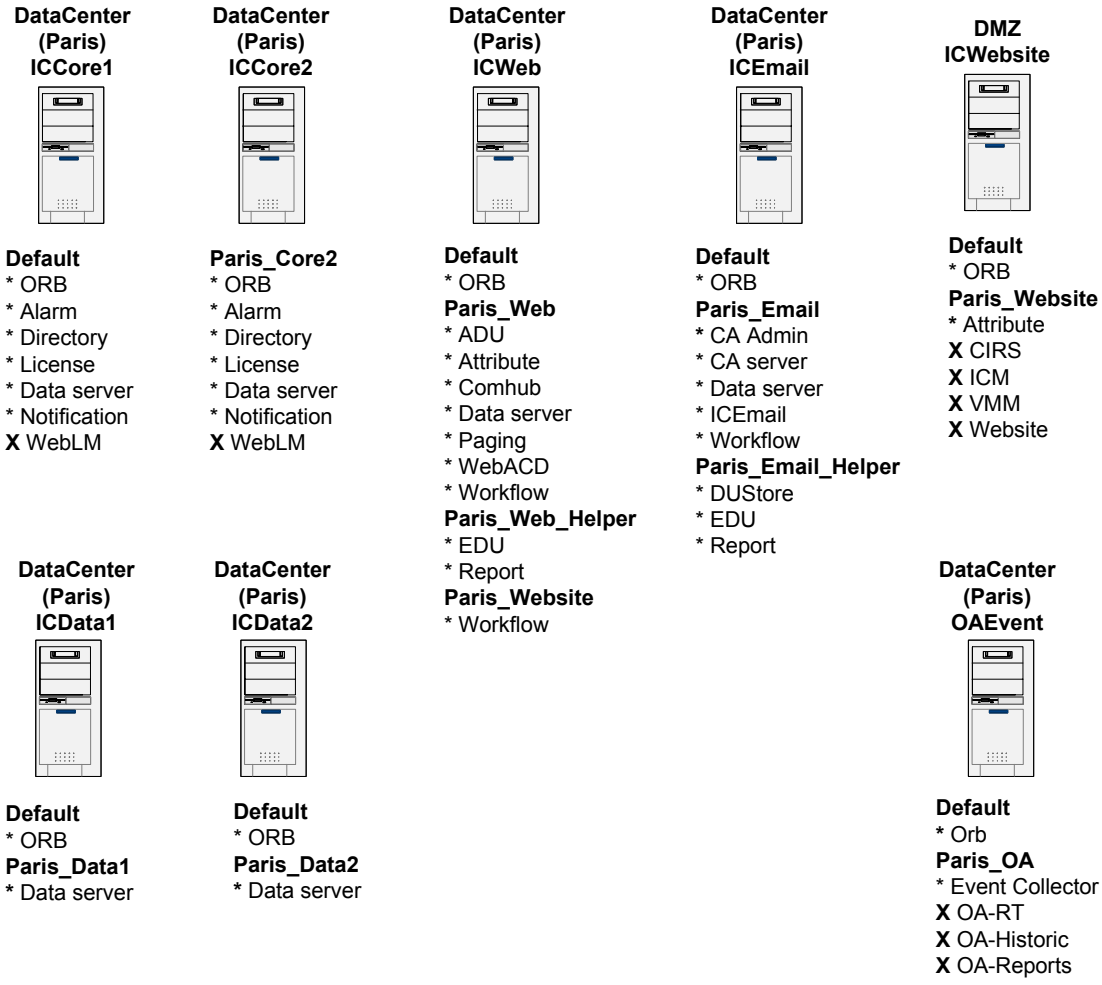
The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

This section includes the following topics:

- Partitioning at Paris site on page 176
- Partitioning at York site on page 177

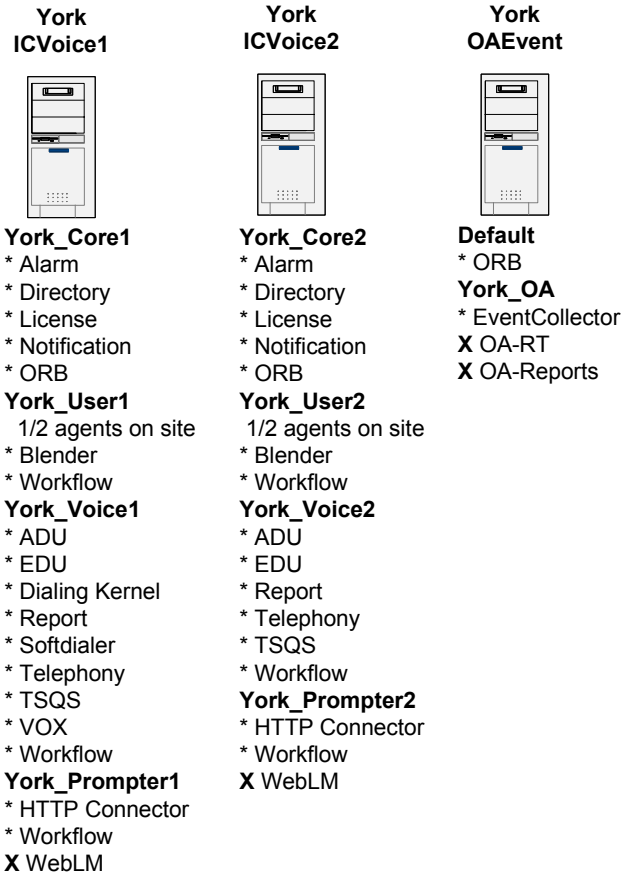
Partitioning at Paris site

The following figure shows the distribution of components on the server machines at the Paris site. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.



Partitioning at York site

The following figure shows the distribution of components on the server machines at the York site. An **X** before a component indicates that component is installed on the machine, but does not belong to an Avaya IC domain.



Scenario 13: Failover strategy

This section includes the following topics:

- Failover strategy at York site on page 156
- Failover strategy at Paris site on page 158

Failover strategy at Paris site

The following table shows the failover strategy at the Paris site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
Default	1. Default 2. Paris_Core2
Paris_Core2	1. Paris_Core2 2. Default
Paris_Data1	1. Paris_Data1 2. Default 3. Paris_Core2
Paris_Data2	1. Paris_Data2 2. Paris_Core2 3. Default
Paris_Email	1. Paris_Email 2. Paris_Email_Helper 3. Paris_Web 4. Default 5. Paris_Core2
Paris_Email_Helper	1. Paris_Email_Helper 2. Paris_Email 3. Default 4. Paris_Core2
Paris_Web	1. Paris_Web 2. Paris_Web_Helper 3. Paris_Email 4. Default 5. Paris_Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the **Advanced** tab as follows: Paris_Web: Priority Value = 1
Paris_Web_Helper	1. Paris_Web_Helper 2. Paris_Web 3. Default 4. Paris_Core2

Domain	Failover domains
Paris_Website	1. Paris_Website 2. Paris_Web 3. York_Voice1 4. Default 5. Paris_Core2
Paris_OA	1. Paris_OA 2. Paris_Web 3. Default 4. Paris_Core2

Failover strategy at York site

The following table shows the failover strategy at the York site in this example. The components in the domain in the left column failover to the domains in the right column in the order listed.

Domain	Failover domains
York_Core1	1. York_Core1 2. York_Core2 3. Paris_Data1 4. Paris_Data2
York_Core2	1. York_Core2 2. York_Core1 3. Paris_Data2 4. Paris_Data1
York_User1	1. York_User1 2. York_User2 3. York_Prompter1 4. York_Prompter2 5. Paris_Data1 6. Paris_Data2 7. York_Voice1 8. York_Voice2 9. York_Core1 10. York_Core2 11. Paris_Email 12. Paris_Email_Helper 13. Paris_Web 14. Paris_Web_Helper

Domain	Failover domains
York_User2	1. York_User2 2. York_User1 3. York_Prompter2 4. York_Prompter1 5. Paris_Data2 6. Paris_Data1 7. York_Voice2 8. York_Voice1 9. York_Core2 10. York_Core1 11. Paris_Email 12. Paris_Email_Helper 13. Paris_Web 14. Paris_Web_Helper
York_Voice1	1. York_Voice1 2. York_Voice2 3. York_Core1 4. York_Core2 5. Paris_Data1 6. Paris_Data2
York_Voice2	1. York_Voice2 2. York_Voice1 3. York_Core2 4. York_Core1 5. Paris_Data2 6. Paris_Data1
York_Prompter1	1. York_Prompter1 2. York_Prompter2 3. York_Core1 4. York_Core2 5. Paris_Data1 6. Paris_Data2 7. York_Voice1 8. York_Voice2

Domain	Failover domains
York_Prompter2	1. York_Prompter2 2. York_Prompter1 3. York_Core2 4. York_Core1 5. Paris_Data2 6. Paris_Data1 7. York_Voice2 8. York_Voice1
York_OA	1. York_OA 2. York_Voice1 3. York_Voice2 4. York_Core1 5. York_Core2

Scenario 14: Business Advocate for two sites, multi-channel, data center

This scenario is a modification of Scenario 13: Two sites, multi-channel, data center on page 174 to include Business Advocate. Both sites access the data center.

A single instance of Business Advocate indicates that the Avaya IC system includes only one Logical Resource Manager for Business Advocate. This Logical Resource Manager can monitor all agents in the network and select a qualified, available agent for a contact.

Note:

This scenario uses the same Workflow servers as Scenario 13: Two sites, multi-channel, data center on page 174. However, to correctly run with Business Advocate, these Workflow servers must run the Business Advocate workflows to qualify and transfer contacts.

In this scenario, the site with the data center includes the Business Advocate Logical Resource Manager, the RDBMS, all Data servers, the Event Collector server, Web servers, and Email servers. The data center does not support agents or Voice servers. The second site includes all agents and Voice servers. You can deploy several satellite sites with the same configuration, but different domains, as the second site.

To implement a data center, the WAN connection between the sites must have sufficient bandwidth and must always be available to prevent any disruption to service that a single site dependency can cause.

Topics for this scenario include:

- Scenario 14: Deployment overview on page 182
- Scenario 14: Avaya IC domain overview on page 183
- Scenario 14: Partitioning of servers on page 183
- Scenario 14: Failover strategy on page 185

Scenario 14: Deployment overview

This scenario adds Business Advocate servers to some of the machines that host Avaya IC servers, described in Scenario 13: Two sites, multi-channel, data center on page 174. This scenario also adds two machines to host the Resource Manager servers and other Avaya IC servers in the Paris domain.

If you host Avaya IC and Avaya OA databases in DB2 on AIX, this scenario requires the following:

- A Windows or Solaris machine to host the Business Advocate databases. If desired, you can install SQL Server on a machine that hosts a Resource Manager server.
- An additional Data server on the same machine as a Resource Manager server. This Data server will provide Avaya IC with access to the Business Advocate database and data, such as service classes. Configure this Data server in its own domain, such as RM_Data. Add the RM_Data domain to the failover path for all domains that include Directory servers and Workflow servers that run contact qualification workflows.

Scenario 14: Avaya IC domain overview

This scenario includes two sites: Paris and York. The Business Advocate servers in this scenario are distributed across the following Avaya IC domains including those listed in Scenario 13: Two sites, multi-channel, data center on page 174.

The following table shows the Avaya IC domains in each site. The highlighted domains were added to support Business Advocate. The following table shows the Avaya IC domains in each site. The Default domain is used in both sites.

Site 1 – Paris	Site 2 – York
• Default • Paris_Core2 • Paris_Email • Paris_Email_Helper • Paris_Web • Paris_Web_Helper • Paris_Website • Paris_Data1 • Paris_Data2 • Paris_OA • **Paris_RM1** • **Paris_RM2** • **Paris_RM_Helper1** • **Paris_RM_Helper2**	• York_Core1 • York_Core2 • York_User1 • York_User2 • York_Voice1 • York_Voice2 • York_Prompter1 • York_Prompter2 • York_OA

Scenario 14: Partitioning of servers

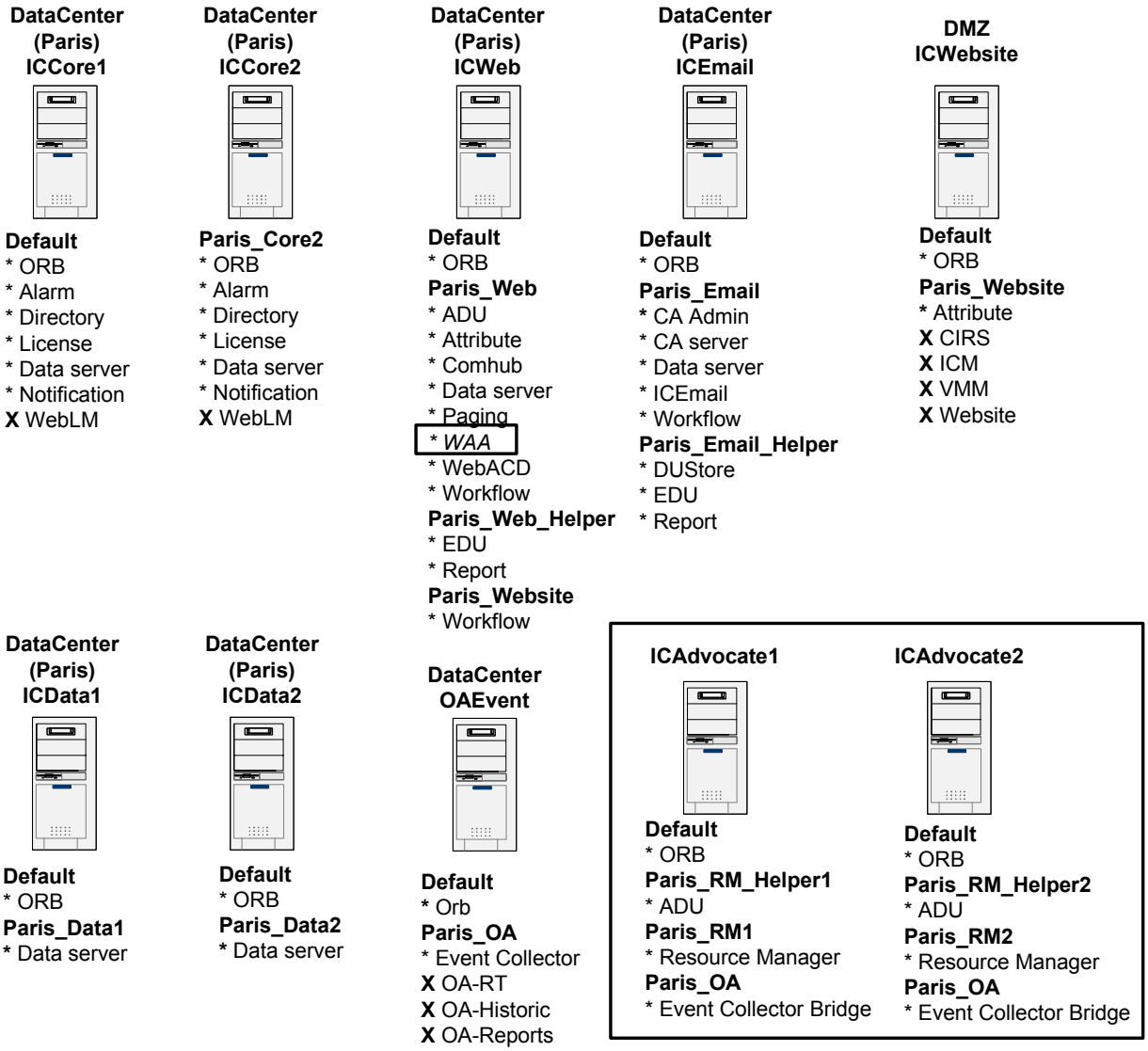
The physical partitioning of the servers reflects the distribution of the Avaya IC and Avaya OA components on the server machines. The logical partitioning reflects the distribution of servers and agents across the Avaya IC domains.

This section includes the following topics:

- Partitioning at Paris site on page 184
- Partitioning at York site on page 185

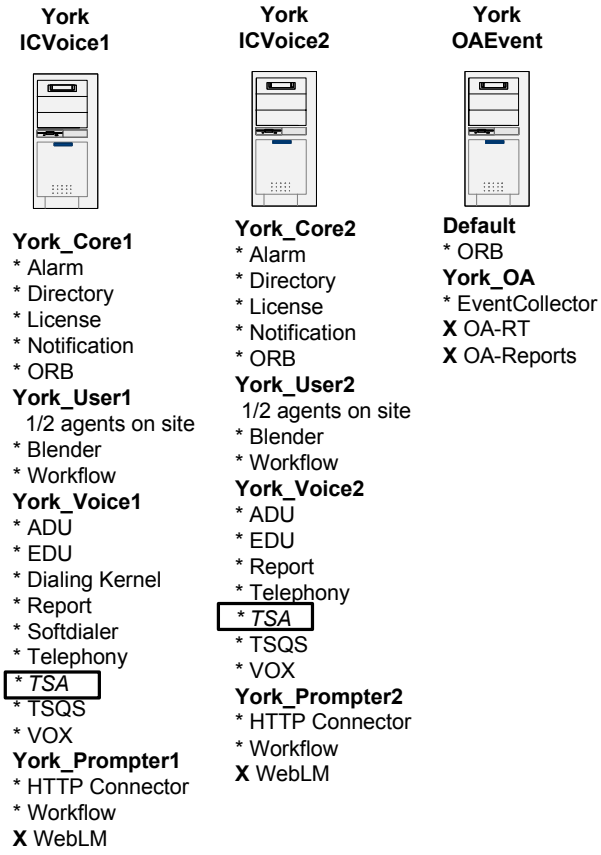
Partitioning at Paris site

The following figure shows the distribution of Business Advocate servers on the server machines at the Paris site. The highlighted servers are in addition to those components described in Scenario 13: Partitioning of servers on page 176.



Partitioning at York site

The following figure shows the distribution of Business Advocate servers on the server machines at the York site. The highlighted servers are in addition to those components described in Scenario 13: Partitioning of servers on page 176.



Scenario 14: Failover strategy

Business Advocate has some unique failover strategies for the Resource Manager and the voice channel. For details about those strategies, see *IC Business Advocate Configuration and Administration*.

The following table shows the failover strategy for the Business Advocate domains in this example. The Business Advocate domains do not failover to any of the other Avaya IC domains. The components in the domain in the left column failover to the domains in the

right column in the order listed. For failover information for the domains not listed in this table, see Scenario 13: Failover strategy on page 177.

Domain	Failover domains
Paris_RM1	1. Paris_RM1 2. Paris_RM2 3. Paris_RM_Helper1 4. Default 5. Paris_Core2
Paris_RM2	1. Paris_RM2 2. Paris_RM1 3. Paris_RM_Helper2 4. Default 5. Paris_Core2
Paris_RM_Helper1	1. Paris_RM_Helper1 2. Default 3. Paris_Core2
Paris_RM_Helper2	1. Paris_RM_Helper2 2. Default 3. Paris_Core2

Chapter 6: Avaya Agent Web Client server deployment scenarios

This section includes scenarios of sample deployments of the Avaya Agent Web Client software with Avaya IC 7.0. Avaya Agent Web Client provides a browser based application interface for the agents in your contact center. Agents access the interface by connecting to the Avaya Agent Web Client server through a Web browser. The Java Application Bridge server allows the Avaya Agent Web Client application to communicate with the IC servers. These deployment scenarios are to be used with the non-Avaya Agent Web Client deployment scenarios. These scenarios describe the Avaya Agent Web Client server deployment on top of a completed Avaya IC server deployment.

If you need information about Avaya IC server deployments, see Avaya IC single site deployment scenarios on page 111 and Avaya IC multi-site deployment scenarios on page 143.

You can use these deployment scenarios across multiple sites. There is no requirement for all sites to use the same deployment scenario. A site with a large agent population or a high availability requirement might require a cluster of WAS servers with load balancing while a much smaller branch site would only require a single computer to host Avaya Agent Web Client.

This section includes the following topics:

- Avaya Agent Web Client deployment guidelines on page 188
- Deployment summary on page 189
- Basic deployment on page 191
- Clustered deployment on page 192
- Load balancing deployment on page 194
- Multiple cell deployment on page 196

Avaya Agent Web Client deployment guidelines

The following guidelines apply for all Avaya Agent Web Client deployments:

- All IBM WAS application servers that are part of the same cluster must be located at the same site.
- All machines that host IBM WAS must be on the same subnet as the primary Avaya IC servers.

  If a contact center has remote voice users for example, the machine that hosts IBM WAS must be on the same subnet as the Avaya IC Telephony server. The Avaya IC Data server can be on a different subnet.
- Only one instance of Avaya Agent Web Client software can exist on an IBM WAS application server. If additional instances of Avaya Agent Web Client are required, you can choose one of the following options:
  - Create additional instances of Avaya Agent Web Client and IBM WAS on multiple systems.
  - Create multiple IBM WAS instances on a single system. The system must have sufficient CPU, memory, and storage capacity.
- All clients must be within the enterprise network security perimeter. Remote clients must be connected through a VPN.
- Avaya Agent Web Client supports SSL. Avaya Agent Web Client is able to use this support to provide encrypted communications between the browser-based application and the Avaya Agent Web Client process running on IBM WAS.
- Proxy servers are not supported. Clients must have a direct connection to a HTTP server, or a load balancer. IBM WAS creates a separate connection back to the Avaya Agent Web Client software for event notification.
- An IBM web plug-in is required to support session affinity between Avaya Agent Web Client and IBM WAS. The IBM web plug-in allows IBM WAS to use a HTTP server installed on a separate system. For more information about supported HTTP servers, see Requirements for Avaya Agent Web Client on page 66.
- Redundancy and failover are supported, but recovery is not transparent. Agents will need to re-login following a failure.
- If Avaya Agent Web Client is installed on a system with other enterprise applications, you must consider the system capacity required to run all of the applications at the same time. If the system does not have sufficient capacity, Avaya Agent Web Client performance will be impacted.
- If you use Windows based platforms, the Avaya Agent Web Client software and the Avaya IC core servers must be installed on separate systems. This restriction does not apply to Unix based platforms.

- Do not run any other applications on the IBM WAS server that hosts Avaya Agent Web Client. If you do, IBM WAS could fail.
- The Java Application Bridge must be in an Avaya IC user domain. For more information, see *IC Installation and Configuration* and *IC Administration Volume 1: Servers & Domains*.

Deployment summary

The deployments described in this section are based on IBM deployments in *WebSphere System Management and Configuration Guide*. The following table lists the IBM deployment that is similar to the Avaya IC deployment.

Avaya IC deployment	IBM deployment
Basic	Vertical scaling
Cluster	HTTP server separate, horizontal scaling with clusters
Load balancing	Horizontal scaling with IP sprayer
Multi-site	Multiple WebSphere cells, combined

The following table lists the main advantages and disadvantages for each type of deployment.

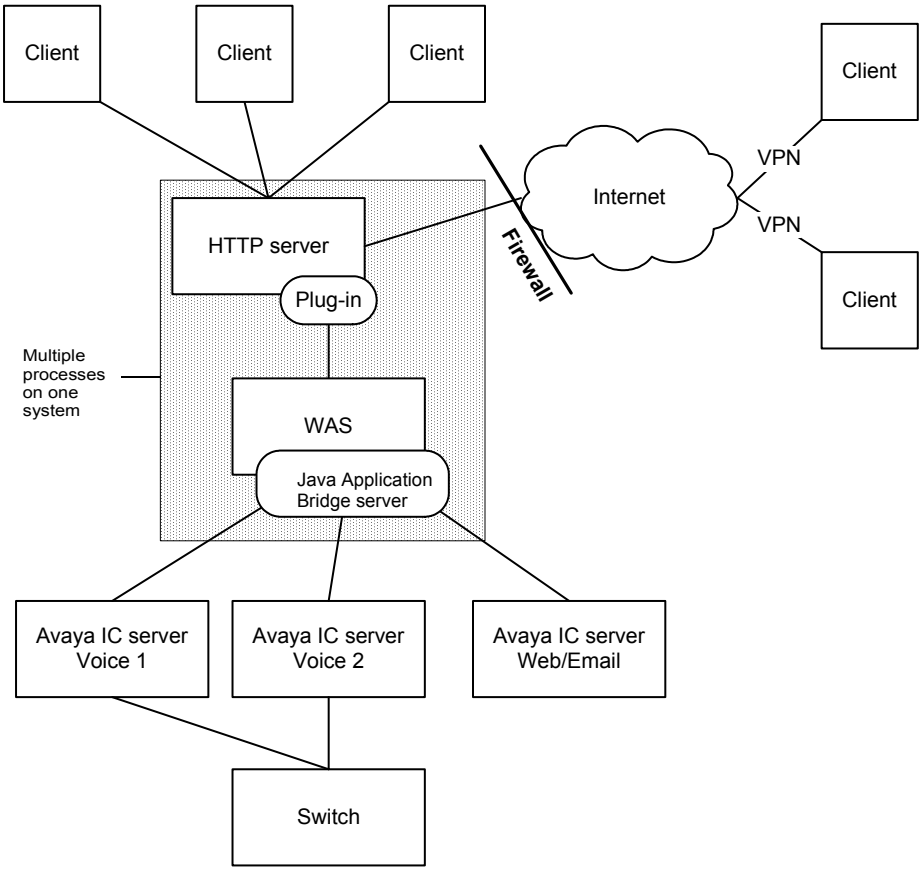
Note:

Additional points of failure could exist depending on your Avaya IC deployment.

Deployment type	Advantages	Disadvantages
Basic	• Appropriate for low volume or less than 500 users. • Easiest deployment to administer • Single computer solution	No redundancy to support failover recovery
Clustered	• Improved availability through hardware redundancy. Clients can failover to other members of the cluster • Improved scalability by adding additional nodes to the cluster • Load balancing using HTTP Server. Network clients connect to the HTTP server to start a session. One the session starts, all communication is between the client browser and the WAS.	The HTTP server is a single point of failure
Load balancing	• Inherits the benefits of the clustered deployment • No single point of failure for Avaya Agent Web Client.	• More complex configuration setup and administration • More hardware resources required
Multiple cell	• Administrative partitioning to support multiple sites • Can implement Load Balancing deployment at each site for increased scalability and availability.	• More administration than a single cell • More hardware resources required

Basic deployment

The following diagram provides an overview of the network structure for a basic deployment.

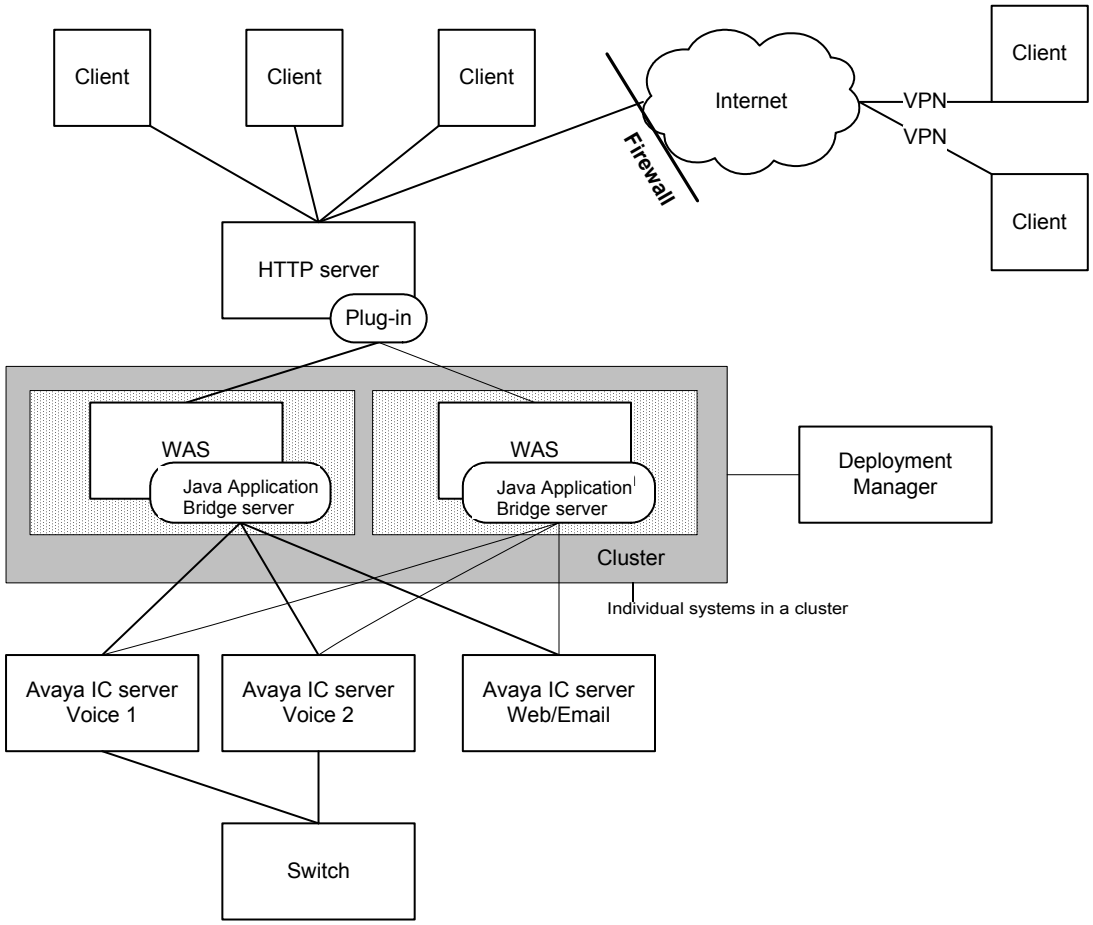


The basic Avaya Agent Web Client server deployment scenario has a single computer installed with the HTTP server software and one or more instances of the WAS software. All network clients communicate to the WAS software through the HTTP server. Clients external to the business network must establish a VPN connection to the network.

The basic deployment is the simplest scenario and allows vertical scaling. Larger IC contact rates can be supported if you increase the CPU speed, memory, and storage capacity of the computer. The HTTP server software, WAS software, and computer where the software is installed and running are single points of failure. If any of these components stop functioning, some IC services will be interrupted until normal operations are resumed. Avaya Agent Web Client services will be interrupted if the WAS fails. New logins will not succeed if the HTTP server fails, but active sessions should be uninterrupted.

Clustered deployment

The following diagram provides an overview of the network structure for a clustered deployment.

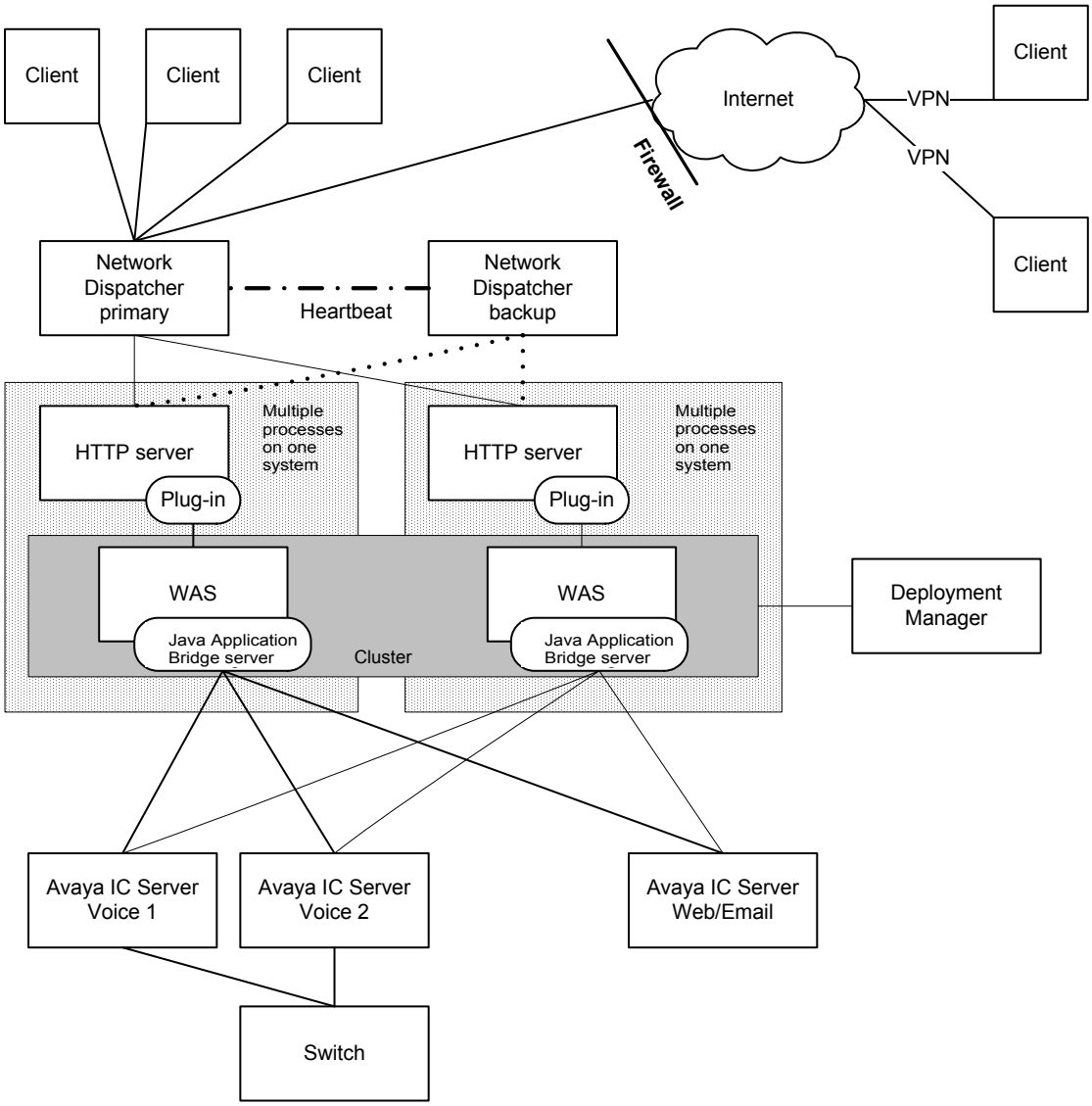


The clustered Avaya Agent Web Client server deployment scenario has the WAS software installed and running on two computers with similar configurations. The WAS computers are assigned to the same cluster. The IBM Deployment Manager is required to support cluster administration and configuration. IBM recommends that you install the Deployment Manager software on a dedicated computer. A separate computer has the HTTP server software installed. The HTTP server will load balance between the different nodes in the cluster. Once the session has been created, no further interaction takes place between the client browser and HTTP server.

Creating a cluster of WAS computers increases availability. If one WAS computer fails the second WAS computer can handle all the client requests. Scalability is improved because load balancing is performed by the HTTP server at the beginning of each client session. Avaya Agent Web Client requires session affinity, so only the original request to establish the session will be load balanced. Once the session is established, the client will be redirected to the same application server by the HTTP server web plug-in.

Load balancing deployment

The following diagram provides an overview of the network structure for a load balancing deployment.



The Avaya Agent Web Client server deployment scenario for load balancing adds the Network Dispatcher component of the IBM Edge Server to increase the availability of Avaya Agent Web Client. Only the IBM Edge Server network dispatcher is certified for load balancing with Avaya IC. The network dispatcher relays Avaya Agent Web Client requests to group of computers instead of to a single computer. The Avaya Agent Web Client software does not place a significant processing load on the Network Dispatcher system.

This scenario uses two Network Dispatcher systems. One Network Dispatcher system functions as the primary system, and the second Network Dispatcher system functions as a backup system. All requests to the cluster are handled by the primary system. Both the primary and backup systems use a heartbeat to verify that the other system is functioning correctly. If the primary system fails, the backup system performs the primary systems work.

The cluster can consist of multiple systems with the WAS software installed. The number of systems required is determined by the peak contact rate, the hardware selected, and your failure tolerance.

Note:

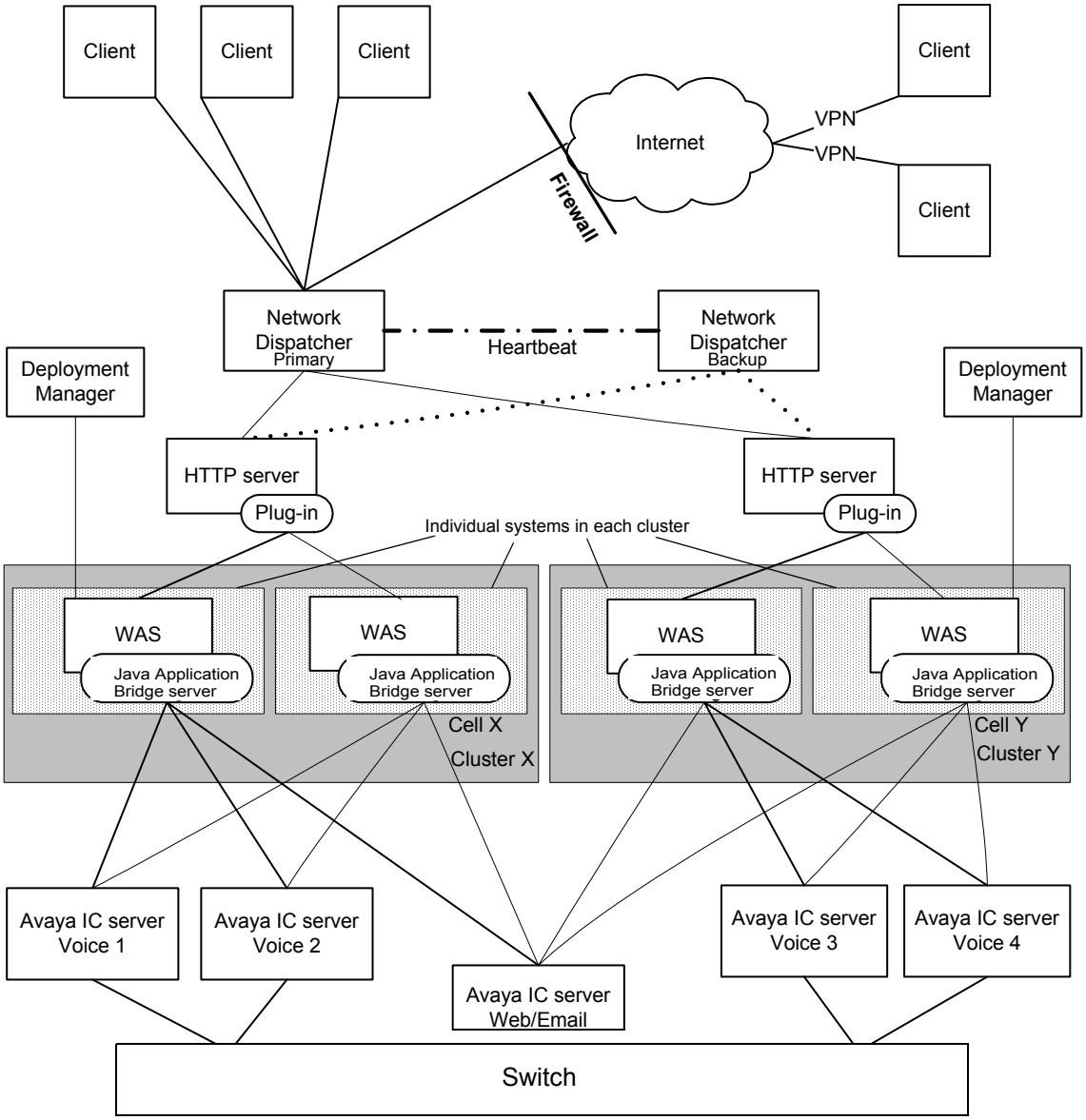
There are two acceptable variations of this deployment. You can install the HTTP server software on a separate system, or you can install the HTTP server software on the same system that has the Network Dispatcher software installed. Avaya IC will not place a significant processing load on either the HTTP server or the Network Dispatcher system.

For example, if you want to prevent performance issues in the event of a single node failure:

- The network dispatcher should be located on the same subnet as the WAS systems.
- If your cluster only consists of two systems and you want to support the failure of a single system, each system must:
  - Be able to handle the full processing requirements of your configuration
  - Not exceed 50% capacity during normal operations

Multiple cell deployment

The following diagram provides an overview of the network structure for a multiple cell deployment.



The Avaya Agent Web Client server deployment scenario for multiple cells is similar to the Avaya Agent Web Client deployment scenario for load balancing. This deployment consists of multiple clusters with each cluster in its own cell. A cell is created to partition the administration as well as the agent population. Each cell has a specific set of WAS servers forming its cluster. Agents are assigned to a specific cluster.

Multiple cells allow you to:

- Partition agents to support organization structures or to optimize agent network connectivity
- Locate each cell and cluster across multiple sites to increase availability.

  To prevent a WAN outage from impacting all remote sites, the network dispatchers and HTTP servers need to be distributed to multiple sites.
- Support the transition to Avaya Agent Web Client updates that have been modified with new customization or fixes

  A new cell can be created for the new version of Avaya Agent Web Client without impacting the currently working version. Both cells can be active until the transition has been successful.

Chapter 7: Avaya IC hardware requirements

The following hardware requirements are the minimum requirements for an Avaya Interaction Center (Avaya IC) installation.

These hardware requirements do not include third party components, such as database management, email, telephony, and web-hosting services. For information about requirements for these components, see the manufacturer's documentation.

This information includes estimated hardware requirements for Avaya OA components that are run on the same machines as Avaya IC components. If you plan to run all Avaya OA components on dedicated machines, you must use the hardware requirements for Avaya OA for those machines. For more information about the hardware requirements for Avaya OA, see *Avaya OA Installation Planning and Prerequisites*.

Important:
The following hardware requirements are estimates only. Contact your Avaya representative or Avaya Business Partner representative for assistance with sizing your Avaya IC system.

This section includes the following topics:

- Hardware requirements for deploying Avaya IC on page 199.
- Hardware guidelines for Avaya IC servers on page 200.
- Hardware requirements for Design & Administration Tools on page 203.
- Required hardware for agent workstations on page 204.

Hardware requirements for deploying Avaya IC

Avaya IC servers, Design & Administration Tools, and agent desktop applications have different hardware requirements. You cannot install them on the same machines. For example:

Servers - Do not install and run Avaya IC servers on the same machine as Design & Administration Tools or agent desktop applications. You can host multiple servers on the same machine.

Design & Administration Tools - Do not install and run Design & Administration Tools on the same machine as Avaya IC servers or agent desktop applications. Do not run more than one IC Manager concurrently. You can run all of the Design & Administration Tools on the same machine.

Agent desktop applications - Do not install and run agent desktop applications on the same machine as Avaya IC servers or Design & Administration Tools. You can run more than one agent desktop application on the same machine.

Hardware guidelines for Avaya IC servers

Avaya IC can run on a variety of machines from different hardware vendors. All machines that host Avaya IC servers require fast CPUs and sufficient available memory. To increase the availability of your Avaya IC servers, replicate the servers on independent server machines. For examples of how to replicate your servers to meet the needs of your Avaya IC system, see Chapter 4: Avaya IC single site deployment scenarios on page 111, and Chapter 5: Avaya IC multi-site deployment scenarios on page 143.

The performance of your Avaya IC servers is completely dependent on the hardware and networking systems being available and properly configured.

This section includes the following topics which describe guidelines that typically result in good performance and reliability:

- Hardware requirements on page 201.
- Server distribution on page 201.
- Server failover on page 201.
- Server machine speed on page 201.
- Server configuration impact on page 202.
- Disk space for Avaya IC servers on page 202.
- Disk space for server log files on page 202.
- Validation of Avaya IC configuration on page 202.
- IBM Logical Partition (LPAR) technology on page 202

Hardware requirements

The hardware requirements for servers depend upon the deployment of an Avaya IC system, the volume of contacts in the contact center, and performance requirements.

You can distribute the disk space and CPU requirements across more than one physical hard drive or processor in the same server machine.

Your Avaya representative or Avaya Business Partner representative has documentation and information to estimate hardware sizing for an Avaya IC system. For assistance with sizing an Avaya IC system, contact your Avaya representative or Avaya Business Partner representative.

Server distribution

Distribute application servers across multiple physical machines to meet performance and fault tolerance requirements.

Note:

If you run CPU-intensive third party applications on the same machines as Avaya IC servers, the third party applications will impact the performance of your Avaya IC system.

Server failover

Failure of a single server machine should not impact all agents in the contact center. Partition Avaya IC servers appropriately across physical machines, and configure failover appropriately.

Server machine speed

Install application servers on machines with fast CPUs and adequate memory. These servers primarily require disk space for paging tasks and temporary files.

Server configuration impact

If your configuration includes certain conditions, such as large reporting loads or integration program loads, you may need to re-size the machines that host the servers or configure secondary application servers.

Disk space for Avaya IC servers

Allocate sufficient disk space on each server machine for all Avaya IC servers. Avaya IC copies all server files to a machine, even if that machine will not host all servers.

Disk space for server log files

Allocate 4MB for server log files for each Avaya IC server. Avaya IC installs most servers with a default log size of 2MB. However, when a log file reaches 2MB, Avaya IC automatically creates a backup copy of the log file. You can configure the size of each server's log file in IC Manager.

Validation of Avaya IC configuration

Validate your configuration with hardware, network, security, and database vendors.

IBM Logical Partition (LPAR) technology

Avaya IC provides the following support for the IBM Logical Partition (LPAR) technology:

1. The following platforms are supported for all IC servers.
   - Single/Multi CPU POWER3
   - Single CPU POWER4
   - Single CPU POWER5
2. The following platforms are not supported for voice channel servers (TS and TSQS), but are supported for all other IC servers.
   - Multi CPU POWER4/POWER5

3. The following are additional requirements across all hardware platforms when running AIX 5.2:
   - Upgrade to AIX 5.2 ML5
   - Upgrade to latest levels of respective hardware microcode.

Configuration Assistance

1. LPAR is not a factor when determining hardware supportability. Please use the information above to design the solution with respect to CPU, multi-CPU, processor type, and maintenance level (ML).
2. The Telephony server (TS) and TSQS server cannot be deployed on an operating system that is running with multiple Power4 or Power5 CPUs:
   a. TS and TSQS cannot be hosted on a Power4 or Power5 multi-processor server or LPAR (i.e. in a Power4 or Power5 LPAR environment, the partition must be a single processor partition).
   b. With processors other than Power4 or Power5, the TS and TSQS can be deployed in either single or multi-processor configurations.
3. When deploying IC services other than TS and TSQS, the type of CPU, the number of CPUs and LPAR technology are not a determining factor for determining supportability.
4. Avaya is currently evaluating options for supporting these exception cases.

Hardware requirements for Design & Administration Tools

The following table lists the minimum hardware requirements for design and administration workstations in a Windows environment.

These hardware requirements do not include third party components, such as database management, email, telephony, and web-hosting services. For information about requirements for these components, see the manufacturer's documentation.

CAUTION:
Do not run IC Manager on a multi-processor machine.

Component	Microsoft Windows
Hardware Architecture	IBM Compatible
CPU	500 MHz Pentium II

Component	Microsoft Windows
RAM	256 MB
Free Disk Space	400 MB
Load Device	N/A
Recommended Monitor Resolution	1280x1024 (256 colors)
Minimum Monitor Resolution	1024x768 (256 colors)

Required hardware for agent workstations

This section describes the minimum hardware requirements for agent workstations in a Windows environment.

These hardware requirements do not include third party components, such as database management, email, telephony, and web-hosting services. For information about requirements for these components, see the manufacturer's documentation.

This section includes the following topics:

- Required hardware for the Avaya Agent interface on page 204
- Required hardware for the Avaya Agent Web Client interface on page 205

Required hardware for the Avaya Agent interface

The following table lists the minimum hardware requirements for agent workstations installed with Avaya Agent.

If you plan to run additional components on the agent desktop machine, you must allow a minimum of 256 MB of RAM and 400 MB of free disk space for Avaya IC agent applications.

Hardware component	Microsoft Windows
Hardware Architecture	IBM Compatible
CPU	500 MHz
RAM	256 MB

Hardware component	Microsoft Windows
Free Disk Space	400 MB
Load Device	N/A
Recommended Monitor Resolution	1280x1024 (256 colors)
Minimum Monitor Resolution	1024x768 (256 colors)

Required hardware for the Avaya Agent Web Client interface

The following table lists the minimum hardware requirements for the workstations of agents who use Avaya Agent Web Client.

Hardware component	Microsoft Windows
Hardware Architecture	IBM Compatible
CPU	• 700 MHz for voice • 1.4 GHz for voice and email
RAM	512 MB
Free Disk Space	Diskless workstations are not supported.
Load Device	N/A
Recommended Monitor Resolution	1280x1024 (256 colors)
Minimum Ethernet connection	1MBPS

Chapter 8: Avaya IC licensing

You must obtain a license file for your configuration of Avaya Interaction Center (Avaya IC) before you complete your installation and configure your Avaya IC system. Avaya IC cannot function without a valid license file for all components included in your Avaya IC system. The steps you must take to obtain a license file begin when you select and purchase your Avaya IC system.

You must obtain a license for Avaya IC systems, including production, development, and test systems. Licenses for production systems include all of the features and capacities that you purchased for your Avaya IC system. Licenses for non-production systems include up to ten concurrent users.

To obtain an Avaya IC license file, consult your Avaya representative or Avaya Partner representative and perform the steps in the following sections:

- Prerequisites for license files on page 207.
- Identifying a physical address on page 208.
- Requesting a license file on page 209.
- Updating a license file on page 210.
- Requesting a replacement license file on page 211.
- Troubleshooting for license files on page 213.

Prerequisites for license files

The contents of your license file reflect your Avaya IC system. Before you apply for and obtain a license file, you must plan the hardware and software configuration of your Avaya IC system. Your Avaya representative or Avaya Partner representative can assist you with this task.

You need to consider all options in your Avaya IC system to determine the hardware and software configuration for your Avaya IC license file, including:

- Platform architecture, such as how many server machines you require and which, if any, telephony equipment you have.
- Reliability objectives.

- Network topology.
- Avaya IC components required by your system.
- Number and type of media channels.
- Number of Avaya IC sites.
- Number of concurrently logged in agents and supervisors per site.
- Number of concurrently logged in agents and supervisors using each media channel and component.
- Number of Web License Managers and License servers.
- Physical addresses of the computers that will host the License server components for your Avaya IC system. These physical addresses are also known as Host IDs.

Note:

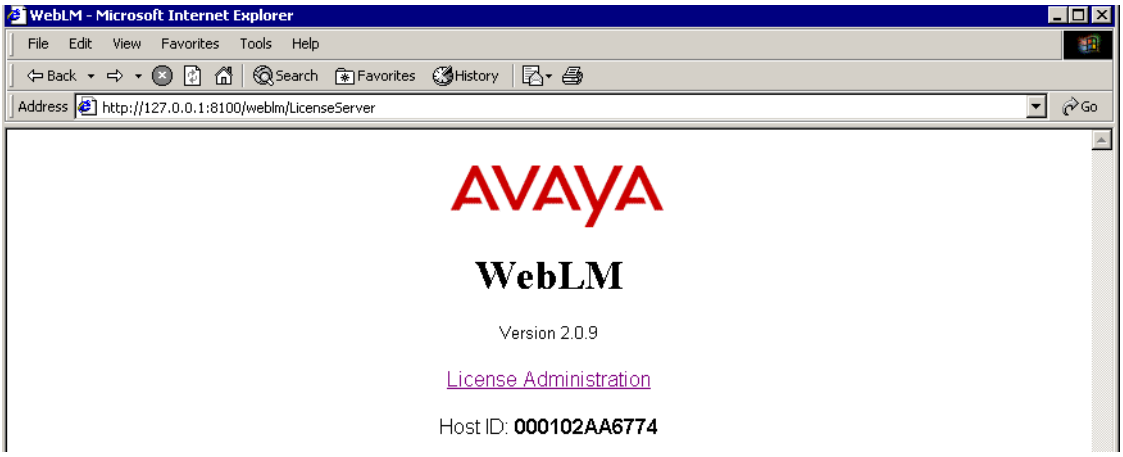
The Dialing Kernel server for Outbound Contact Management has specific requirements for licenses. Each Dialing Kernel server requires one Inbound Agent License and one Total Agent License. Outbound Agent licenses are not affected.

Identifying a physical address

You must provide a physical address for each machine that hosts license components for your Avaya IC system. The physical address is also known as the host ID. If your Avaya IC system includes failover for license components, or multiple sites, you must host the license components on more than one machine, and provide physical addresses for each machine.

The Avaya IC installer automatically identifies the physical address when you install the server files. You do not need to install a license file to install Avaya IC or view the physical address in the Web License Manager (WebLM). To make sure that you identify the physical address for the correct NIC and server, Avaya recommends that you use this method. For more information on how to install Avaya IC and set up the Web License Manager, see *IC Installation and Configuration*.

The WebLM displays the physical address in the Host ID field, as shown in the following figure. For information on how to identify a physical address without the WebLM, see Troubleshooting for license files on page 213.



Requesting a license file

You must request a separate license file for each Avaya IC system. For example, if you plan to create a development system and a production system, you must have a different license file for each system. You must send a separate request for each license file.

To request an Avaya IC license file:

1. Send an email message to icoakeyrequest@avaya.com with the following information about your Avaya IC system:

Required information	Description
SAP order numbers	Avaya assigns one or more numbers to the customer's order in the SAP system.
Avaya sold-to number	Avaya assigns this number to the customer.
Customer name	Name of the customer who purchased the Avaya IC system.

Required information	Description
System purpose	The system purpose must be one of the following: • Production • Development • Test If you need license files for two systems, send two separate email requests.
Return email address	Avaya emails the license file to you. You must provide a secure email address where you want to receive the license file.
Physical addresses	Physical addresses of the computers that will host the Web License Manager (WebLM) and License server components for this particular Avaya IC system. These Physical addresses are also known as Host IDs. For more information, see Identifying a physical address on page 208.

2. You receive an Avaya IC license file from Avaya at the email address designated by your enterprise.
3. Install and activate the license file in your Avaya IC system. For instructions on how to install and activate a license file, see *IC Installation and Configuration*.

Important:
Maintain a copy of your license files in a safe location.

Updating a license file

If your enterprise purchases additional components for your Avaya IC system, or adds more concurrent users, you must update your Avaya IC license file.

Note:
License files for Avaya IC 7.0 releases are valid for all releases of IC 7.0.x. You do not need to update your license files if you upgrade from one Avaya IC 7.0.x release to another unless you purchase new features or capacities.

To update an Avaya IC license file:

1. Send an email message to icoakeyrequest@avaya.com with the following information about your Avaya IC system:

Required information	Description
SAP order numbers	You must provide the original order numbers for your Avaya IC system, and the order numbers for the new components or capacities. Avaya assigns one or more numbers to the customer's order in the SAP system.
Avaya sold-to number	Avaya assigns this number to the customer.
Customer name	Name of the customer that purchased the Avaya IC system.
System purpose	The system purpose must be one of the following: • Production • Development • Test If you need license files for two systems, send two separate email requests.
Return email address	Avaya emails the license file to you. You must provide a secure email address where you want to receive the license file.
Physical addresses	Physical addresses of the computers that will host the Web License Manager (WebLM) and License server components for this particular Avaya IC system. These Physical addresses are also known as Host IDs. For more information, see Identifying a physical address on page 208.

2. You receive an Avaya IC license file from Avaya at the email address designated by your enterprise.
3. Install and activate the license file. For instructions on how to install and activate a license file, see *IC Installation and Configuration*.

Requesting a replacement license file

If you change or upgrade your network, you may need to obtain a replacement license file. Changes that affect the license file include:

- Replacement of the network card on the machine that hosts a Web License Manager

- Transfer of a Web License Manager to a new machine

To obtain a replacement license file:

1. Send an email message to icoakeyrequest@avaya.com with the following information about your Avaya IC system:

Required information	Description
SAP order numbers	You must provide the original order numbers for your Avaya IC system, and any additional order numbers for new components or capacities. Avaya assigns one or more numbers to the customer's order in the SAP system.
Avaya sold-to number	Avaya assigns this number to the customer.
Customer name	Name of the customer that purchased the Avaya IC system.
System purpose	The system purpose must be one of the following: • Production • Development • Test If you need license files for two systems, send two separate email requests.
Return email address	Avaya emails the license file to you. You must provide a secure email address where you want to receive the license file.
Physical addresses	Physical addresses of the computers that will host the Web License Manager (WebLM) and License server components for this particular Avaya IC system. These Physical addresses are also known as Host IDs. For more information, see Identifying a physical address on page 208.

2. You receive an Avaya IC license file from Avaya at the email address designated by your enterprise.
3. Install and activate the license file. For instructions on how to install and activate a license file, see *IC Installation and Configuration*.

Troubleshooting for license files

If you cannot use the WebLM to identify the physical address for one or more machines, perform the steps in one of the following sections to identify a physical address:

- Identifying a physical address in Windows on page 213.
- Identifying a physical address on Solaris on page 213.
- Identifying a physical address on AIX on page 213.

Identifying a physical address in Windows

To identify a physical address on a Windows machine:

1. Open a command window.

   To open a command window, select **Start** > **Run** and enter **cmd** in the **Open** field.

2. At the prompt, enter: **ipconfig /all**
3. Windows displays the physical address on a separate line, such as:

   ```
   Physical Address. . . . . . . . : 00-53-45-00-00-00
   ```

Identifying a physical address on Solaris

To identify a physical address on a Solaris machine:

1. Run the following command: **hostid**
2. Solaris displays the physical address as a list of hexadecimal digits on a separate line, such as:

   ```
   831800e9
   ```

Identifying a physical address on AIX

To identify a physical address on an AIX machine:

1. Run the following command: **uname -m**
2. AIX displays the physical address as a list of hexadecimal digits on a separate line, such as:

   ```
   000C066A4C00
   ```

Chapter 9: Supported operating systems

This section includes the information about how to configure the operating system and install required prerequisite software on machines that host Avaya Interaction Center (Avaya IC) components. For information about supported software, see Chapter 2: Required software components on page 41.

This section includes the following topics:

- Regional settings on page 215
- Microsoft Windows on page 215
- Security for Unix platforms on page 220
- Sun Solaris on page 220
- IBM AIX on page 226
- Citrix on page 231

Regional settings

If you need to change the regional system settings for a machine, make sure that you change the settings for all users, including the local system account.

Microsoft Windows

Note:

Before you install Avaya IC agent applications, configure all agent workstations with restore points. The agent installer replaces some system files. Restore points allow easy rollback after you uninstall Avaya IC if software conflicts arise. Please consult your Windows documentation or third party guides for procedures on how to configure restore points.

To install and configure the following Windows components for Avaya IC, see the documentation provided by Microsoft and the information in the following sections:

- Setting up Windows 2000 Server on page 216.
- Setting up Windows Server 2003 on page 217.
- Setting up Windows XP Professional on page 217.
- Setting up Microsoft Internet Explorer on page 217.

Setting up Windows 2000 Server

Avaya IC components support the following versions of Windows 2000 Server. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Avaya IC component	Supported Windows 2000 versions
Servers	• Windows 2000 Server SP4 • Windows 2000 Advanced Server SP4 • Windows 2000 Datacenter Server SP4
Design & Administration Tools	• Windows 2000 Professional SP4
Avaya Agent Desktop	• Windows 2000 Professional SP4

Installing required service packs for Windows 2000 Server

You must install Windows 2000 Server Service Pack 4 on all machines that run Windows 2000 Server, except machines that run Windows 2000 Datacenter Server. Avaya IC does not support Service Pack 1 or Service Pack 2 for Windows 2000 Server.

To install the Service Pack:

1. Go to the Microsoft Web site at http://www.microsoft.com
2. Navigate to the Downloads section for Windows 2000 Server.
3. Download the following:
   - Windows 2000 Server Service Pack 4
   - Deployment instructions for Windows 2000 Server Service Pack 4

Setting up Windows Server 2003

Avaya IC components support the following versions of Windows Server 2003 for Avaya IC servers. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition

Setting up Windows XP Professional

The following Avaya IC components support Windows XP Professional. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

- Design & Administration tools
- Client applications

Installing required service packs for Windows XP Professional

Avaya supports Windows XP Professional with SP1a or SP2. You must install one of these service packs on all machines that run Windows XP Professional.

To install a service pack:

1. Go to the Microsoft Web site at http://www.microsoft.com
2. Go to the Downloads section for Windows XP Professional, and follow the installation instructions provided by Microsoft.
3. Download:
   - Either Windows XP Service Pack 1a, or Windows XP Service Pack 2
   - Readme and other deployment instructions

Setting up Microsoft Internet Explorer

You must install Internet Explorer 6.0 SP1 on every machine that hosts one or more of the following Avaya IC components:

- Avaya Agent
- Web Management
- Email Management
- Administration tools

All supported versions of Windows typically include Internet Explorer. However, you may need to upgrade to the current version.

This section includes the following topics:

- Downloading Internet Explorer on page 218.
- Installing a Java Virtual Machine plugin for Internet Explorer on page 218.
- Activating the Microsoft JVM on page 219.
- Configuring the Sun JVM on page 219.
- Configuring encoding for localized releases on page 220.

Downloading Internet Explorer

To download Microsoft Internet Explorer 6.0 SP1:

1. Go to the Microsoft Web site at http://www.microsoft.com
2. Click the Internet Explorer hyperlink in the left navigation pane.
3. Download and install Microsoft Internet Explorer 6.0 SP1.

Installing a Java Virtual Machine plugin for Internet Explorer

The version of Internet Explorer that is provided with Microsoft Windows operating systems shipped after December 2003 do not include a Java Virtual Machine (JVM). These operating systems include Windows XP Professional and Windows Server 2003.

The following Avaya IC components require a JVM to function correctly:

- Email Template Administration
- Avaya Agent
- Avaya Agent Web Client
- Customer Chat Applet

Important:
To use the Customer Chat Applet, customers of the Website must have a supported JVM installed to chat with an agent. The Customer HTML Chat Client does not require a supported JVM. For information about the limitations of the Sun JVM 1.4.1 for customers of the Website, see Exceptions to support of Sun JVM for Website customers on page 72. For more information about the Customer Chat Applet and the Customer HTML Chat Client, see *IC Installation and Configuration*.

If you host these components on a machine with Windows XP Professional or Windows Server 2003, you must download and install a JVM on those machines. The following table describes the supported JVMs and where you can obtain copies.

Supported JVM	Download location
Microsoft JVM plugin for Internet Explorer	The Microsoft JVM is no longer available for distribution from Microsoft.
Sun JVM 1.4.1	http://www.sun.com/software/download

Activating the Microsoft JVM

If the machine already includes the Microsoft JVM plugin, you do not need to perform any steps to configure Microsoft Windows and Internet Explorer to use this plugin. However, you do need to disable any other JVM that is activated for Internet Explorer.

To disable an activated JVM:

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. Select the **Advanced** tab of the **Internet Options** dialog box:
3. Scroll down to the section for the currently activated JVMs.

   For example, if a Sun JVM is currently activated, scroll down to the Java (Sun) section.
4. Clear the checkbox to use that JVM.

   For example, for a Sun JVM, clear the **Use Java 2 v1.3.1_15 for <applet>** box.
5. Select **OK**.

Configuring the Sun JVM

If you install the Sun JVM plugin, you must configure Microsoft Windows and Internet Explorer to use this plugin.

To configure the Sun JVM:

1. In the **Windows Control Panel**, select **Java Plug-in**.
2. In the **Java Plug-in** Control Panel:
   a. Select the **Browser** tab.
   b. Confirm that the **Microsoft Internet Explorer** field is checked.
   c. Select **Apply**.
   d. Close the Control Panels.
3. In Internet Explorer, select **Tools** > **Internet Options**.
4. In the **Internet Options** dialog box:

a. Select the **Advanced** tab.
b. In the **Java (Sun)** section, select the **Use Java 2 v1.4.1_*06 for <applet>*** box.
c. In the **Microsoft VM** section, clear the **JIT Compiler for virtual machine enabled** box.
d. Select **OK**.

5. Restart the machine.

Configuring encoding for localized releases

If your Avaya IC system includes Prompter in a supported language other than English, you must configure the encoding in Internet Explorer to match that locale.

For example, if an agent will view Prompter scripts in Thai, you need to perform the following steps to configure the coding in Internet Explorer for Thai:

1. Turn off Auto select
2. Configure the encoding for the Thai locale.

   To configure encoding, select **View** > **Encoding** in Internet Explorer.

Security for Unix platforms

Avaya recommends that users avoid running Avaya software as the root user wherever possible for security reasons. For more information, see User accounts for Solaris on page 225 and User accounts for AIX on page 230.

Sun Solaris

Avaya IC servers supports the following versions of Solaris:

- Solaris 8
- Solaris 9

Important:
Avaya IC does not support Solaris on Intel.

Avaya IC Design & Administration Tools and client applications do not support Solaris.

This section includes information that you need to install and configure a Solaris operating system on machines that host Avaya IC servers or databases. This section includes the following topics:

- Browser requirements for Solaris on page 221.
- Disk space requirements for Solaris on page 221.
- Installing required patches for Solaris on page 222.
- Configuration requirements for Solaris on page 223.
- User accounts for Solaris on page 225.

Browser requirements for Solaris

Avaya IC does not support an internet browser for Solaris. However, you must have an internet browser to install an Avaya IC license. If you host Avaya IC servers on Solaris, install the Avaya IC license from the machine that hosts the Design & Administration Tools or from another machine with a supported Windows operating system.

Disk space requirements for Solaris

A Solaris machine that hosts Avaya IC servers requires the following disk space:

- A minimum of 1 GB of disk space for the server files
- A minimum of 30 GB disk space to store server log files
- A minimum of 360MB extra temp space in the /var/tmp directory for the Avaya IC installer to perform the Java Virtual Machine

These requirements do not include disk space for required third party applications, such as Solaris, Sun ONE server, or the JDK.

Detailed information about how to partition individual Solaris machines is beyond the scope of this manual. The most efficient method to partition a machine depends on many factors, including which Avaya IC servers you plan to host on the machine, and the volume of customer interactions in your contact center. You must consider all of these factors carefully when you determine how to partition each machine in your Avaya IC system.

Installing required patches for Solaris

This section includes information about the patches that you need to install on Solaris machines that host Avaya IC servers. This section includes the following topics:

- Recommended patch cluster on page 222.
- Additional required patches for Solaris 8 on page 222.
- Additional required patches for Solaris 9 on page 222.
- Installing Solaris patches on page 223.

Recommended patch cluster

To avoid potential problems, install the latest Recommended Patch Cluster issued by Sun Microsystems.

Additional required patches for Solaris 8

You must install the latest versions of the patches for Solaris 8 that are shown in the following table.

Tip:

The latest Recommended Patch Cluster may include some of the required patches. Review the list of patches in the cluster before you install any additional patches.

Patch	Dependencies	Description
109147	None	Linker patch
108528	None	Security patch
108434-10	109147 from above	32-bit runtime patch for C++
108435-10	108434 from above	64-bit runtime patch for C++
111721	None	Math lib patch

Additional required patches for Solaris 9

Avaya IC does not require any patches for Solaris 9 except for the latest recommended patch cluster.

Installing Solaris patches

To install Solaris patches:

1. Download the patches from following website:

   http://www.sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

2. Follow the instructions provided by Sun Microsystems in the Readme file for the patch suite.

Configuration requirements for Solaris

This section includes the following topics which describe the recommended configuration parameters for Avaya IC on Solaris:

- Configuration settings for Solaris on page 223.
- ULIMIT parameters on page 224.

Configuration settings for Solaris

The following table describes the configuration settings required on a Solaris machine that hosts Avaya IC servers.

Configuration setting	Notes
DISPLAY	Enable the `DISPLAY` parameter. The Avaya IC installation and Configuration Tool cannot run if you have not enabled the `DISPLAY` parameter.
National character set	UTF8
Oracle Database character set	UTF8

Configuration setting	Notes
Locale	Install the English locale: • English: en_US.UTF-8 You can also install the appropriate locale for the language of your Avaya IC system: • Japanese: ja_JP.UTF-8 • Korean: ko_KR.UTF-8 • Simplified Chinese: zh_CN.UTF-8 • German: de_DE.UTF-8 • French: fr_FR.UTF-8 • Italian: it_IT.UTF-8 • Spanish: es_ES.UTF-8 • Portuguese: pt_BR.UTF-8 • Thai: th_TH.UTF-8 • Russian: ru_RU.UTF-8 **Note:** This setting is case-sensitive.
Port 9010	Solaris runs the HTT Input Method Server (htt_server) on port 9010 by default. This port assignment creates a conflict with any Avaya IC server that you configure to run on port 9010. To avoid the conflict, you can update htt_server to use a different port, or not assign an Avaya IC server to port 9010. In a typical installation, with the primary ORB server on port 9001, IC Manager automatically assigns port 9010 to the Report server.
Space requirements	Make sure that the server machine has sufficient space in the `/var/tmp` directory. For more information, see Disk space requirements for Solaris on page 221.
Windowing environment	Install a Windowing environment such as X Windows.

ULIMIT parameters

The following table describes the minimum required settings for ULIMIT parameters required on an Solaris machine that hosts Avaya IC servers. The superuser must ensure that the hard limits for the ULIMIT parameters are not less than these minimum required settings. For more information, see the UNIX man pages provided by Solaris.

Parameter	Minimum required setting
data	512MB
stack	512MB
memory	512MB

Parameter	Minimum required setting
core dump	1 GB
file descriptors	2000

User accounts for Solaris

You need the following Solaris user accounts when you install and configure Avaya IC:

- Root user on page 225.
- Installation user on page 225.

Root user

You need the root account when you:

- Install Avaya IC on a machine that will host a Telephony server for an Avaya switch with Definity or Communication Manager software.
- Configure the Web applications with the Configuration Tool, including the Website, Email Template Administration, and Web License Manager.

Installation user

Use this account to perform all tasks to install and configure Avaya IC that do not require the root user. The Avaya IC installation directory must be owned by this account.

Important:
If you do not use a root account to install Avaya IC servers on a machine, and need to configure that machine with a Telephony server for an Avaya switch with DEFINITY or Communication Manager software, reinstall the Avaya IC servers under the root account.

Avaya IC does not have any specific requirements for the installation user account. However, Avaya recommends that you:

- Create an installation group named **avaya**.
- Assign the avaya group as the primary group when you create the installation user account.
- Do not assign a secondary group membership to the installation user account.

IBM AIX

Avaya IC servers support AIX 5.1L maintenance level 3 and AIX 5.2. Avaya IC Design & Administration Tools and client applications do not support AIX.

This section includes information that you need to install and configure an AIX operating system on machines that host Avaya IC servers or databases. This section includes the following topics:

- Supported versions of AIX on page 226
- C++ runtime library updates on page 227
- Browser requirements for AIX on page 227
- Disk space requirements for AIX on page 227
- Configuration requirements for AIX on page 229
- User accounts for AIX on page 230

Supported versions of AIX

The following table describes the supported versions of AIX, including maintenance levels and patches. You must install a supported version of AIX to avoid potential problems.

Version requirement	AIX 5.1L	AIX 5.2
Maintenance level	3	2
Required patches	IY34030	Upgrade C++ runtime libraries: xlC.aix50.rte to a version equal or higher to 6.0.0.12 and xlC.rte to a version equal or higher to 6.0.0.0. This can be achieved by installing the latest C++ runtime PTF from IBM support website.
Kernel	32-bit mode	32-bit mode

C++ runtime library updates

The AIX fix pack, "March 2003 C++ Runtime for AIX PTF" is available at the following Website:

http://www-1.ibm.com/support/docview.wss?rs=32&context=SSEP5D&q=&uid=swg24004427&loc=en_US&cs=ISO-8859-1&lang=en

The PTF will update the runtime levels to the correct level. The C++ runtime library levels must be:

```
xlC.aix50.rte        6.0.0.5 COMMITTED C Set ++ Runtime for AIX 5.0
xlC.msg.en_US.rte    6.0.0.0 COMMITTED C Set ++ Runtime
xlC.rte              6.0.0.0 COMMITTED C Set ++ Runtime
```

Browser requirements for AIX

Although, Avaya IC does not support an internet browser for AIX, you must have an internet browser to install an Avaya IC license. If you host Avaya IC servers on AIX, install the Avaya IC license from the machine that hosts the Design & Administration Tools or from another machine with a supported Windows operating system.

Disk space requirements for AIX

An AIX machine that hosts Avaya IC servers requires the following disk space:

- A minimum of 1 GB of disk space for the server files
- A minimum of 30 GB disk space to store server log files
- A minimum of 360MB extra temp space in the `/tmp` directory for the Avaya IC installer to perform the Java Virtual Machine

These requirements do not include disk space for required third party applications, such as AIX or the JDK.

Detailed information about how to partition individual AIX machines is beyond the scope of this manual. The most efficient method to partition a machine depends on many factors, including which Avaya IC servers you plan to host on the machine, and the volume of customer interactions in your contact center. Consider all of these factors carefully when you determine how to partition each machine in your Avaya IC system.

Installing required locales

All installations on IBM AIX require that you install the following locales:

- EN_US locale

  AND

- If the Avaya IC system includes a supported language other than English, one of the following locales, as appropriate:
  - Spanish: ES_CO
  - Portuguese: PT_BR
  - Italian: IT_IT
  - French: FR_FR
  - German: DE_DE
  - Simplified Chinese: ZH_CN
  - Korean: KO_KR
  - Japanese: JA_JP
  - Thai: TH_TH
  - Russian: RU_RU

Configuration requirements for AIX

There are recommended configuration parameters for Avaya IC on IBM AIX. For information about specific operating system and ULIMIT parameters, see Appendix C: Tuning AIX for Avaya IC and Avaya OA on page 413.

Configuration settings

The following table describes the configured settings required on an AIX machine that hosts Avaya IC servers.

Configuration setting	Notes
Locale	Install EN_US and any additional locales, as appropriate for the language of the Avaya IC system: • English: EN_US • Spanish: ES_CO • Portuguese: PT_BR • Italian: IT_IT • French: FR_FR • German: DE_DE • Simplified Chinese: ZH_CN • Korean: KO_KR • Japanese: JA_JP • Thai: TH_TH • Russian: RU_RU **Note:** It is not necessary for EN_US to be the primary locale.
DISPLAY	Enable the **DISPLAY** parameter. The Avaya IC installation and Configuration Tool cannot run if you have not enabled the **DISPLAY** parameter.
Space requirements	Make sure that the server machine has sufficient space in the `/tmp` directory. For more information, see Disk space requirements for AIX on page 227.
Windowing environment	Install a Windowing environment such as X Windows.

User accounts for AIX

You need the following AIX user accounts when you install and configure Avaya IC:

- Root user on page 230.
- Installation user on page 230.

Root user

Avaya IC requires that the root account be in the same group as the database administration login for the Avaya IC databases. For example, include the root user account in the db2admin group.

You need the root account when you:

- Install Avaya IC on a machine that will host a Telephony server for an Avaya switch with Definity or Communication Manager software.
- Configure the Web applications with the Configuration Tool, including the Website, Email Template Administration, and Web License Manager.

Installation user

Use this account to perform all tasks to install and configure Avaya IC that do not require the root user. The Avaya IC installation directory must be owned by this account.

Important:
If you do not use a root account to install Avaya IC servers on a machine, and need to configure that machine with a Telephony server for an Avaya switch with DEFINITY or Communication Manager software, reinstall the Avaya IC servers under the root account.

Avaya IC does not have any specific requirements for the installation user account. However, Avaya recommends that you:

- Create an installation group named **avaya**.
- Assign the avaya group as the primary group when you create the installation user account.
- Do not assign a secondary group membership to the installation user account.

Citrix

Avaya IC provides support for most agent desktop applications in Citrix servers for Windows. For information about which agent desktop applications are not supported, see Limitations on support for Citrix on page 234.

With Avaya IC agent desktop applications in a Citrix environment, the contact center can:

- Administer agent desktop applications from a central location.
- Remotely provide agents and supervisors with access to the agent desktop applications.
- Publish Avaya Agent or another supported agent desktop application on one or more Citrix server machines.
- Use Web browser or Citrix client to access agent desktop applications from agent or admin machines.

This section describes the support for Avaya IC components in Citrix. This section includes the following topics:

- Deployment of Avaya IC components in a Citrix environment on page 231.
- Supported versions of Citrix on page 233.
- Avaya IC components supported in Citrix on page 233.
- Limitations on support for Citrix on page 234.
- Licensing for Avaya IC in Citrix on page 234.
- Citrix Web interface on page 235.
- Citrix client interface on page 235.
- Limitations of integration with Citrix on page 237.

Deployment of Avaya IC components in a Citrix environment

This section provides information about where to deploy Avaya IC components in a Citrix environment, including information about how to deploy more than one configuration of the Avaya IC agent desktop applications.

This section includes the following topics:

- Location of Avaya IC components on page 232.
- Multiple configurations of agent desktop applications on page 232.

Location of Avaya IC components

When you install Avaya IC in a Citrix environment, deploy the Avaya IC components as follows:

Avaya IC servers - Locate the Avaya IC servers on the server machines, following the appropriate deployment scenario for the components in the Avaya IC system. You do not need to change the deployment of Avaya IC servers if you host the agent desktop applications in a Citrix environment.

Design & Administration Tools - Locate the Design & Administration Tools on separate administration machines. You do not need to change the deployment of Design & Administration Tools if you host the agent desktop applications in a Citrix environment.

Web Management Website - Locate the customer Website on a separate machine in the DMZ of the network and the administration Website on an administration machine inside the firewall. You do not need to change the deployment of the Web Management Websites if you host the agent desktop applications in a Citrix environment.

Agent desktop applications - Locate the Avaya IC agent desktop applications on one or more Citrix server machines. Do not install the agent desktop applications on the agent workstations.

Avaya IC Citrix connectors - Locate the Avaya IC Citrix connectors on the agent workstations. These connectors provide agents with access to the agent desktop applications on the Citrix server machines, and ensure that the agent desktop applications resize correctly in the Citrix client.

Citrix clients - Locate the Citrix clients on the agent workstations.

Multiple configurations of agent desktop applications

With the agent desktop applications on Citrix, you can host different configurations of the agent desktop applications on different Citrix servers. For example, you can create a voice only configuration and a multi-channel configuration, as follows:

- Avaya Agent with voice only on ServerA
- Avaya Agent with voice, chat, and email on ServerB

Agents can easily switch from voice only work to multi-channel work by exiting from ServerA and logging in to ServerB.

Supported versions of Citrix

Avaya supports the versions of Citrix listed in the following table. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Location	Supported versions
Citrix server machines - versions of Citrix	• Citrix MetaFrame XP 1.0 • Citrix MetaFrame XP Presentation Server - Feature Release 3
Citrix server machines - operating system	• Windows 2000 Server • Windows Server 2003
Agent machines - operating system	• Windows 2000 Professional • Windows XP Professional

Avaya IC components supported in Citrix

Avaya IC supports the following agent desktop applications in Citrix:

- Avaya Agent with the following features:
  - Inbound voice channel
  - Email channel
  - Chat channel
  - Voice Chat channel
  - Prompter

Avaya IC support for publishing applications in Citrix

Avaya IC supports both of the following methods of publishing applications in Citrix:

- Agent applications accessed as embedded applications in the Citrix Web interface
- Agent applications accessed in a seamless window in the Citrix client interface

Limitations on support for Citrix

For release 7.0 of Avaya IC, Avaya does not provide support for other operating systems that may be supported by Citrix. Avaya also does not provide support for the hosting of Avaya OA components, Avaya Agent Web Client, or other Avaya IC components on the Citrix servers.

The limitations on support for components of Avaya IC and Avaya OA on Citrix server machines, include the following:

- Agent workstation with an operating system that is not Windows 2000 Professional or Windows XP Professional
- Avaya IC Design and Administration Tools, including IC Manager, Workflow Designer, and Database Designer
- Business Advocate administration tools, including Business Advocate Supervisor
- VTel
- Outbound Contact
- Avaya OA
- IP Softphone
- Windows Terminal Services (TSE) without Citrix
- Other Citrix servers, such as UNIX servers
- Wyse Terminals and other terminals, such as the COMPAQ T20

Licensing for Avaya IC in Citrix

If the Avaya IC system includes agent desktop applications in Citrix, the following licenses are required:

- The appropriate number and kind of Citrix licenses
- An Avaya IC license for every agent and supervisor who will be concurrently logged in to Avaya IC.

If an Avaya IC system includes Citrix, there is no reduction in the number of Avaya IC licenses that are required. The Web License Manager monitors the number of agents who log in to Avaya IC. If the number of agents who attempt to log in to Avaya IC exceeds the number of licenses, the Web License Manager denies access to those log in attempts that exceed the licensed number.

Citrix Web interface

The Citrix Web interface is also called “publish as desktop”. The Web interface uses an ActiveX control to exchange information about agent actions with the Avaya IC agent desktop applications published on Citrix server.

Access to agent desktop applications - With the Web interface, agents use a Web browser to log in to the agent desktop applications. After the agent logs in, the Web interface displays a Web page that includes Avaya Agent and other agent desktop applications published on Citrix server.

Configuration for Citrix - You do not have to perform any configuration in Citrix to ensure that agents can access the agent desktop applications through the Web interface.

Citrix client interface

The Citrix client interface is also called “publish as application”. The client interface uses Independent Computing Architecture (ICA) protocol to exchange information about agent actions with the Avaya IC agent desktop applications published on Citrix server.

The Citrix client interface with the seamless window causes issues with the login behavior and the appearance of the Avaya IC agent desktop applications. Avaya provides two tools that prevent these potential issues. For example, these tools ensure that:

- Agents log in to the appropriate agent desktop applications.
- Agent desktop applications, such as screen pops and Web Agent, size properly in the Web interface.
- Avaya Agent does not overlap the other agent desktop applications in the window.

This section includes the following topics:

- Configuring Citrix on page 236.
- Configuring Citrix integration for seamless window applications on page 236
- Web browser tool for the client interface on page 236.
- Executable tool for the client interface on page 236.

Configuring Citrix

You do not have to perform any configuration in Citrix to ensure that agents can access the agent desktop applications through either the Web interface or the agent interface.

Depending upon the environment, you may need to adjust the size of the Avaya Agent framework. For more information on how to customize the framework size, see *Avaya Agent Integration*.

Configuring Citrix integration for seamless window applications

If the Avaya IC system includes access to Avaya IC agent desktop Applications through the Citrix client interface in a seamless window, the Citrix integration can be configured in the following ways:

- Configure and run the Web browser tool to access the agent desktop applications.
- Configure and run the Executable tool to access the agent desktop applications.

Both of these tools require that you install the Avaya Agent INI file (qui.ini). A copy of the INI file is available on Avaya IC CD-ROM 1 for Windows with the other Citrix files. For more information, see IC Installation and Configuration.

Web browser tool for the client interface

The Web interface tool appears as a Web page in Internet Explorer that agents use to log in to the agent desktop applications on Citrix. The Web interface tool ensures that:

- Agents log in to the appropriate agent desktop applications.
- Agent desktop applications size properly in the Web interface.

Configuring the Web browser tool - The only configuration required for this Web interface tool is to update the HTML file with the correct location for the Citrix server that hosts the agent desktop applications.

Customizing the Web browser tool - If desired, you can customize the appearance of the Web page for the Web interface tool.

For information about how to configure the Web browser tool to access a specific agent desktop application on a Citrix server, see *IC Installation and Configuration*.

Executable tool for the client interface

The executable tool is intended for use only in Avaya IC systems where the design precludes a Web browser application. This tool includes an executable and an INI file. This tool appears as a dialog box on the agent desktop.

Agents use the dialog box to access and log in to agent desktop applications published on Citrix server. After the agent logs in, the client interface opens a window that displays Avaya Agent and other agent desktop applications published on Citrix server.

Configuring the executable tool - The only configuration required for the executable tool is update the INI file with the correct location for the Citrix server that hosts the agent desktop applications.

Customizing the executable tool - If desired, you can customize the text on the buttons in the dialog box to meet the needs of the contact center or the corporate style.

For information about how to configure the client interface tool to access a specific agent desktop application on a Citrix server, see *IC Installation and Configuration*.

Limitations of integration with Citrix

With a Citrix integration, agent desktop applications are installed, published, and accessed on Citrix server. Only the interface to the agent desktop applications is installed on the agent workstations.

Before you deploy your Avaya IC agent desktop applications on a Citrix server, consider the following limitations:

- Do not host embedded applications and seamless window applications on the same Citrix server. To use both publishing methods in an Avaya IC system, host the embedded applications on a different Citrix server from seamless window applications.
- Do not use the Web browser tool, the Executable tool, or the Avaya Agent INI file (qui.ini) on a Citrix server that hosts embedded applications.
- Citrix cannot make agent desktop applications look as if they are on agent workstations.
- Citrix does not provide the ability to integrate applications across processor boundaries. For example, you cannot integrate the agent desktop applications on the Citrix server with an application on the agent workstation.
- If the Avaya IC system includes integration with another application, such as PeopleSoft or Siebel, you must integrate the applications on the Citrix server.

Chapter 10: Network configuration

You need to configure your network for Avaya Interaction Center (Avaya IC). To set up your network, perform the steps in the following sections:

- Enabling TCP/IP networking on page 239.
- Verifying DNS resolution on page 240.

For additional network information, see Network topology and configuration guidelines on page 78.

Enabling TCP/IP networking

All Avaya IC servers and client applications use TCP/IP to communicate. You need to enable TCP/IP networking on each machine in an Avaya IC system.

By default, Windows and UNIX operating systems include TCP/IP networking on all machines with network cards. Typically, Avaya IC uses the default TCP/IP settings applied during installation.

However, if you deploy Avaya IC on an existing Novell NetWare network, you may need to take additional steps to configure the TCP/IP networking protocol. You can obtain information on how to install and configure TCP/IP networking on a NetWare network from your IT professionals.

Verifying DNS resolution

Before you install software for Web Management or Email Management, you must verify the domain name system (DNS) resolution on each machine.

Each Web Management server and Email Management server must have a Fully Qualified Domain Name (FQDN) that:

- Has a minimum of three parts, separated with periods

  For example, **bsmith.com** only has two parts and would not qualify. **bsmith.domain.com** has three parts and would qualify.

- Does not contain special characters, except the dash (**-**)
- Has forward and reverse DNS mapping in public DNS records

To verify the DNS resolution on machines in your Avaya IC system, perform the steps in one of the following sections:

- Verifying DNS resolution in Windows on page 240
- Verifying DNS resolution on Solaris and AIX on page 241

Verifying DNS resolution in Windows

The following procedure verifies that DNS is configured properly for Windows. Perform this procedure on every Avaya IC server machine that has a Windows operating system.

To verify DNS resolution in Windows:

1. Open a command prompt window.
2. To find the machine's IP address, type **ipconfig** at the prompt.

   The system returns information about the machine's IP configuration, including the IP address (`254.24.167.211`), as shown in the following example:

```
Windows NT IP Configuration

Ethernet adapter El70x1:

IP Address. . . . . . . . . . : 254.24.167.211
  Subnet Mask . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . :  254.24.167.1
```

3. To verify the “forward” DNS mapping, type the following command with the machine’s FQDN at the prompt:

   nslookup <*machine_name*>.<*domain_name*>

   The system returns information about the machine’s forward DNS mapping, including the machine’s IP address and FQDN. The following example of forward DNS mapping indicates that the FQDN `bsmith.domain.com` is assigned to the IP address `254.24.167.211` in public DNS records.

```
Server:  ns3.domain.com
  Address:  254.24.167.23

Name:    bsmith.domain.com
  Address:  254.24.167.211
```

4. To verify the “reverse” DNS mapping, type the following command with the machine’s IP address at the prompt:

   nslookup <*IP_address*>

   The system returns information about the machine’s reverse DNS mapping, as shown in the following example:

```
Server:  ns3.domain.com
  Address:  254.24.167.23

Name:    bsmith.domain.com
  Address:  254.24.167.211
```

Verifying DNS resolution on Solaris and AIX

The following procedure verifies that DNS is configured properly for Solaris and AIX. Perform this procedure on every Avaya IC server machine with a UNIX operating system.

To verify DNS resolution on Solaris and AIX:

1. Open the **hosts** file and locate the information about the machine’s IP configuration, including the IP address (`254.24.167.211`).
2. To verify the “forward” DNS mapping, type the following command with the machine’s FQDN at the prompt:

   nslookup <*machine_name*>.<*domain_name*>

   The system returns information about the machine’s forward DNS mapping, including the machine’s IP address and FQDN. The following example of forward DNS mapping

indicates that the FQDN `bsmith.domain.com` is assigned to the IP address `254.24.167.211` in public DNS records.

```
Server:  ns3.domain.com
  Address:  254.24.167.23

Name:    bsmith.domain.com
  Address:  254.24.167.211
```

3. To verify the “reverse” DNS mapping, type the following command with the machine’s IP address at the prompt:

   nslookup <*IP_address*>

   The system returns information about the machine’s reverse DNS mapping, as shown in the following example:

```
Server:  ns3.domain.com
  Address:  254.24.167.23

Name:    bsmith.domain.com
  Address:  254.24.167.211
```

Troubleshooting an unresolved DNS entry

If a DNS entry is not set up for a Web Management or Email Management machine, you can temporarily use local host entries.

Note:

This workaround is only temporary. You must establish true DNS resolution as quickly as possible for an easier implementation.

To add local host entries for Avaya IC servers:

1. Open the **hosts** file in a text editor.
   - Windows default location: `\WinNT\System32\Drivers\etc`
   - Solaris default location: `/etc`
   - AIX default location: `/etc`
2. In the **hosts** file, locate the IP entry and name for **localhost**.

   For example, the **localhost** line in the file might read**:**

```
127.0.0.1  localhost
```

3. Add an entry for each Web Management or Email Management machine:
   a. At the end of the **localhost** line, press **Enter** to get a new line.
   b. Type the machine’s IP address.
   c. Press **Tab** or type a few spaces, and type the machine’s FQDN.

d. Press **Tab** or type a few more spaces, and type the machine name.

The machine name and the FQDN resolve to the specified address, as shown in the following example:

```
192.168.0.1  testbox.xyzcorp.com  comhub
192.168.0.2  testbox.xyzcorp.com  sql
```

4. Save the file under its original name (hosts).

Note:

If the IP address changes, you must update the **hosts** file to reflect this change.

Chapter 11: Supported database management systems

A relational database management system (RDBMS) is a required prerequisite for Avaya Interaction Center (Avaya IC). Avaya IC servers and client applications access databases to:

- Store employee, contact, and configuration information
- Deliver statistical information to managers
- Deliver customer contact information to agents

Avaya OA uses data stored in the IC Repository database. Before you install Avaya IC, make sure that you perform all prerequisite steps for Avaya OA. For more information and some guidelines for installing and configuring your database software, see *Avaya OA Installation Planning and Prerequisites*.

This section describes the required databases and optional databases for Avaya IC and Avaya OA, and provides information that you need to configure a relational database management system for Avaya IC. This section includes the following topics:

- About Avaya IC databases on page 246.
- Supported database management systems on page 246.
- Supported mixed operating system combinations on page 247.
- Exceptions to supported database management systems on page 249.
- Requirements for database login on page 249.
- Installing database servers on page 249.
- Installing database client software on page 250.
- Configuring binary sort order for Web Management on page 252.
- SQL Server on page 252.
- Oracle on page 255.
- IBM DB2 on page 261.

About Avaya IC databases

Your Avaya IC databases interact with:

- Avaya IC software
- Avaya IC data store units
- Avaya OA software

At a minimum, your Avaya IC system must include the IC Repository database and the CCQ database. Some Avaya IC applications, such as Outbound Contact, and Business Advocate, also require a separate, dedicated databases. Depending on the components in your implementation, your Avaya IC system may also require one or more of these optional Avaya IC databases.

The Avaya Customer Interaction Repository includes the Avaya IC and Avaya OA database and storage components used by an Avaya IC system.

Supported database management systems

The following table describes the operating system required for Avaya IC and Avaya OA servers and software for each supported RDBMS.

Supported RDBMS	Windows 2000 Server	Windows Server 2003	Solaris 8	Solaris 9	AIX 5.1L	AIX 5.2
SQL Server 2000 SP3a	✔	✔	-	-	-	-
Oracle 8.1.7, patch set 4.0	✔	✔	✔	✔	-	-
Oracle 9.2.0 patch set 4.0	✔	✔	-	✔	-	-
DB2 UDB 8.1 FP5	-	-	-	-	-	✔

Supported mixed operating system combinations

A mixed operating system combination occurs when the databases are on one supported operating system and the Avaya IC servers are on a different supported operating system

Note:

Avaya has not tested the mixed operating system combinations.

This section includes the following topics:

- Mixing operating systems on page 247.
- Examples of mixed operating system combinations on page 247

Mixing operating systems

The Avaya IC databases can be on any Windows, Solaris, or AIX operating system that is supported by Avaya IC *provided that* Avaya IC is on an operating system supported for that database in the supported database combinations described in Supported database management systems on page 246.

Examples of mixed operating system combinations

The following examples show how to determine which mixed operating system combinations are supported and which combinations are not supported.

Supported combination

An Oracle database on AIX with IC servers and OA subsystems on Windows is *supported* because:

- Oracle supports AIX, and AIX is a supported operating system for Avaya IC and Avaya OA.
- Avaya IC and Avaya OA support Oracle/Windows as a database/operating system combination, as shown in Supported database management systems on page 246.

Unsupported combination

An Oracle database on AIX with IC servers and OA subsystems on AIX is *not supported* because:

- Oracle supports AIX, but Avaya IC and Avaya OA do not support software such as the Avaya IC Data server and Avaya OA historical subsystem for Oracle on AIX.
- Avaya IC and Avaya OA do not support Oracle/AIX as a database/operating system combination, as shown in Supported database management systems on page 246.

Mixed operating system combinations

The following table contains examples of mixed operating system combinations.

Avaya IC and Avaya OA software operating system	Examples of mixed operating system combinations
Windows 2000 Server Windows Server 2003	Support for: • SQL Server 2000 on Windows 2000 Server or on Windows Server 2003 • Oracle 8.1.7 on Windows 2000 Server, Solaris 8, or IBM AIX • Oracle 9.2.0 on Windows Server 2003, Solaris 8, Solaris 9, or IBM AIX No support for DB2 databases on any operating system.
Solaris 8	Support for: • Oracle 8.1.7 on Windows 2000 Server, Solaris 8, or IBM AIX • Oracle 9.2.0 on Windows Server 2003, Solaris 9, or IBM AIX No support for SQL Server or DB2 databases on any operating system.
Solaris 9	Support for: • Oracle 8.1.7 on Windows 2000 Server, Solaris 8, or IBM AIX • Oracle 9.2.0 on Windows Server 2003, Solaris 8, Solaris 9, or IBM AIX No support for SQL Server or DB2 databases on any operating system.
AIX 5.2	Support for: • DB2 8.1 on Windows 2000 Server, Windows Server 2003, or IBM AIX 5.2 No support for SQL Server or Oracle databases on any operating system.

Exceptions to supported database management systems

Business Advocate does not support the Business Advocate databases on DB2 and AIX.

If you host your Avaya IC and Avaya IC databases on AIX and DB2, configure a Windows or Solaris machine with a supported SQL Server or Oracle database to host the Business Advocate databases. You must also configure a Data server on a machine that hosts a Resource Manager server to connect to the Business Advocate database.

Requirements for database login

The Avaya IC Data server requires an administrative login with DBA privileges for your database. The administrative login must be a DBA login ID for the database server. Do not use the DBA login for a database client.

Avaya IC and Avaya OA must use the same administrative login. The following table shows typical values for this administrative login. If you choose to use a different administrative login, make sure that login has the same permissions as the logins listed in the table.

Property	SQL Server	Oracle	DB2
Database Administration Login	sa	system	db2inst1
Database Administration Password	*password* for sa	*password* for system	*password* for db2inst1

Installing database servers

Database servers act as a central repository for all the information that Avaya IC stores and retrieves. You can install and configure database servers in a number of ways to provide scalability, fault tolerance, and security to meet the specific requirements of your organization.

Install the database client and any required libraries on every machine that hosts an Avaya IC Data server.

Database server installation and configuration are beyond the scope of this manual. If you have not yet deployed your chosen database platform, consult a qualified Database Administrator (DBA).

Installing database client software

Avaya IC servers communicate with the RDBMS through a database client. You need to install the appropriate database client for the RDBMS.

Avaya IC supports the database clients in the following table. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Database	Database client
IBM DB2 8.1 FP7	IBM DB2 8.1 Administration Client FP7
Oracle 8.1.7	Oracle 8.1.7 client
Oracle 9.2.0	Oracle 9.2.0 client
SQL Server 2000 SP3a	SQL Server 2000 Client

This section includes the following topics:

- Location for database clients on page 251.
- Requirements for database clients on page 251.

Location for database clients

Certain Avaya IC servers and applications require access to a database client. You must install a database client on the same machine as these servers and applications.

You must install the database client on machines that host the Avaya IC servers and applications listed in the following table.

Avaya IC component	Servers and applications that require database client
Core servers	Data server
Web Management	WebACD server, Attribute server, ICM server, CIRS server, and all Websites
Business Advocate	Resource Manager server

The database administrator (DBA) should ensure that the database client can connect to the database server.

Note:

Detailed information about database client installation is beyond the scope of this manual. See the documentation provided by your RDBMS vendor.

Requirements for database clients

Database clients require the following:

Dedicated RAM - Reserve a dedicated amount of RAM to run the database. For more information, see the documentation for your database client.

Connection pool - Ensure there is a connection pool to the Data server. For example, if your Avaya IC includes an Oracle database, calculate the amount of memory required (in megabytes) by multiplying the connection pool size by 3.

Swap space - Reserve two to three times the amount of main memory as swap space, preferably on a raw disk.

Configuring binary sort order for Web Management

Web Management:

- Does not support binary sort order on any database platform
- Cannot differentiate between employee accounts based on case
- Can cause authentication problems in cases where, for example, **Agent1** is not the same user as **agent1**

Binary sort order compares bit by bit and is case sensitive. For example, in Web Management, the SQL command `select * from topic` would not return results from a table named `Topic` if binary sort order is turned on, because `Topic` does not match `topic`.

Note:

DB2 databases do not use binary by default. The sort order for DB2 is set in the configuration of the AIX operating system.

SQL Server

All Avaya IC servers and client components support the following SQL Server 2000 databases:

- Microsoft SQL Server 2000 Standard Edition SP3a
- Microsoft SQL Server 2000 Enterprise Edition SP3a

This section includes the following topics:

- Installing SQL Server on page 253.
- Installing required service packs for SQL Server on page 254.
- Installing the SQL Server 2000 client on page 254.
- Recommended configuration for SQL Server on page 255.

Installing SQL Server

You must install and configure SQL Server 2000 SP3a on all machines that host your Avaya IC databases.

Important:
Do not configure your database to be case-sensitive.

The following table contains recommended values for certain options that you must select during a SQL Server installation. For more information about these options, and about the other options in the SQL Server installer, see the documentation provided with your SQL Server database.

Property	Value
Local Computer	Selection depends upon where you plan to deploy your Avaya OA Historical subsystem: • If Historical subsystem is on same machine as Avaya IC and Avaya OA databases, select **Server and Client Tools**. • If Historical subsystem is a different machine than the Avaya IC and Avaya OA databases, select **Client Tools**.
Database instance name	Enter a name for the database instance that identifies the instance of the RDBMS system in which you will create databases. **Tip:** You need the database instance name to install the Avaya OA Historical subsystem.
Software installation	Select **Custom**. Avaya recommends that you configure SQL Server to store data files, including transaction logs, on a separate disk.
Components to install	Do not install the **Development Tools** option.
Services Accounts	• Select **Use the same account for each service**. • Enter the sa login ID (or a login ID with the same privileges) and the password for that account. **Tip:** You need this login and password when you configure Avaya IC and install the Avaya OA Historical subsystem.
Authentication Mode	• Select **Mixed Mode**. • Enter and confirm the password for the `sa` login ID.

Property	Value
Collation Settings	• Select **collation designator**. • Clear all options under **sort order**. • Select the appropriate locale.
TCP/IP sockets	Enter the port number used to communicate with the database. The default port is 1433 for Avaya IC and Avaya OA. **Tip:** You need this port number when you configure Avaya IC and install the Avaya OA Historical subsystem.

Detailed instructions on the installation and configuration of SQL Server 2000 are beyond the scope of this manual. If you plan to use SQL Server with Avaya IC but have not yet installed SQL Server, consult a qualified SQL Server DBA (Database Administrator) for assistance.

Installing required service packs for SQL Server

Install the SQL Server Service Pack 3a on all machines that host your Avaya IC databases.

To install the SQL Server 2000 Service Pack 3a:

- Download and run Service Pack 3a from

  http://www.microsoft.com/sql/downloads/2000/sp3.asp

For specific information on how to deploy the SQL Server 2000 Service Pack 3a, particularly if you need to install the Service Pack on multiple machines, see the Microsoft document from the following Web site:

http://support.microsoft.com/support/servicepacks/SQL/2000/SP3ReadMe.asp

Installing the SQL Server 2000 client

The SQL Server 2000 client is also known as the Microsoft Data Access Component. You must install the SQL Server 2000 client on every machine that hosts an Avaya IC component that requires access to the client. For more information, see Location for database clients on page 251.

Detailed instructions on the installation and configuration of SQL Server 2000 client are beyond the scope of this manual. If you plan to install SQL Server 2000 client with Avaya IC, consult a qualified SQL Server DBA for assistance.

Recommended configuration for SQL Server

Avaya IC does not have any required or recommended configuration settings for SQL Server.

However, Avaya OA has some recommended configuration settings that you need to set after you configure the Avaya IC databases in Database Designer. For more information, see *Avaya OA Installation Planning and Prerequisites*.

Oracle

All Avaya IC servers and client components support the following releases of the Oracle database:

- Oracle 8.1.7
- Oracle 9.2.0

You must consider the needs of your contact center, the operating system of the machine that hosts your database, and the configuration of your Avaya IC system to determine whether you require the Enterprise Edition or Standard Edition of Oracle.

This section includes the following topics:

- Required version mode for an Oracle 9.2.0 database on page 255.
- Required patches for an Oracle database on page 256.
- Installing Oracle Server on page 256.
- Installing Oracle Client on page 261.

Required version mode for an Oracle 9.2.0 database

You must install Oracle 9.2.0 server and client in 32 bit mode. The Avaya IC Data server for Oracle 9.2.0 uses 32 bit Oracle 9 libraries. The Avaya IC Data server does not function if you install Oracle 9 in 64 bit mode.

Required patches for an Oracle database

The following table describes the patches that Avaya IC requires for an Oracle database.

Oracle version	Required patches
Oracle 8.1.7	Patch set 4.0
Oracle 9.2.0	• Patch set 4.0 • Database client patches: - ODBC 9.2.0.6.0 - patch number 3415990 - ODBC 9.2.0.6.1 - patch number 3434877

Installing Oracle Server

This section contains information you must use when you install and configure Oracle server for use with Avaya IC.

This section includes the following topics:

- Location of Oracle server on page 256
- Recommended values for installing Oracle server on page 257
- Configuration settings for Oracle server on page 259
- Character set configuration for Oracle server on page 260

Location of Oracle server

You must install and configure the Oracle Server on all machines that host your Avaya IC databases.

Recommended values for installing Oracle server

The following table contains recommended values for certain options that you must select during an Oracle installation. For more information about the options in an Oracle installer, see the documentation provided with your Oracle database.

Note:

The following table follows the order of installation and configuration for an Oracle 9.2.0 database. The order and names of properties may be different for Oracle 8.1.7.

Property	Recommended value
Product to install	Oracle 9.2.0 database
Installation types	One of the following: • Enterprise Edition • Standard Edition
Database configuration	Customized
Oracle Services for MTS Transaction Server	Port Number on which the service listens for requests. The default port is 2030.
Directory usage configuration	No, I want to defer this configuration to another time.
Listener configuration	• Listener name: LISTENER • Select Protocols: TCP • TCP/IP Protocol: Use the standard port number of 1521 • Configure another listener: No
Naming methods configuration	No, I do not want to change the naming methods configured.
Database configuration assistant Step 1	Create a database
Database configuration assistant Step 2	New database
Database configuration assistant Step 3	Use a database name and SID that uniquely identifies this as an Avaya IC and Avaya OA database. **Tip:** You need the database name and SID when you configure Avaya IC and install the Avaya OA Historical subsystem.
Database configuration assistant Step 4	For **Database Features**, check all options except **Oracle Label Security**.

Property	Recommended value
Database configuration assistant Step 5	Dedicated Server Mode
Database configuration assistant Step 6	• Memory: Custom - Shared Pool: 48 - Buffer Cache: 24 - Java Pool: 32 - Large Pool: 8 - PGA: 24 • Character Sets: - Choose from the list of character sets: UTF8 - National Character Set: UTF8
Database configuration assistant Step 7	No recommended values.
Database configuration assistant Step 8	Create a database
Summary	Verify that the following characters sets are set to UTF8: • Database character set • National character set
Database configuration assistant	Use different passwords for: • SYS, for example manager • SYSTEM, for example manager1

Detailed instructions on installation and configuration of an Oracle Server are beyond the scope of this manual. If you plan to use Oracle Server with Avaya IC but have not yet installed the Oracle Server, consult a qualified Oracle DBA for assistance.

Configuration settings for Oracle server

When you create the database instance for Avaya IC, you must include the following configurations.

Note:

You cannot change the character set or db_block_size after you create the database instance. If the db_block_size of the Avaya IC database instance is less than 8192, your database will not be able to create some of the large indexes required by Avaya IC.

Configuration	Required settings
db_block_size	8192 or higher
Dedicated connections	A minimum of 115 concurrently dedicated connections
Logging Parameters	Checkpoint Timeout of 0
NLS_CHARACTERSET	UTF8
NLS_NCHAR_CHARACTERSET	UTF8
Redo Log files	50 MB
SGA Parameters	• Shared Pool Size equal to or larger than 100 MB • Block Buffers equal to or larger than 300 MB
Tablespaces	Two tablespaces for each Avaya IC database: one for standard database tables, one for temporary tables. For example, IC Repository and CCQ databases require the following tablespaces: • IC Repository tables – **T_CI** • IC Repository temporary tables – **T_CI_TEMP** • CCQ tables – **T_CCQ** • CCQ temporary tables – **T_CCQ_TEMP**
Rollback segment tablespace size	4000 MB
Temporary tablespace	2000 MB

Configuration	Required settings
For Oracle on Solaris only	• remote_login_passwordfile – true • sort_area_retained_size – 0. **Note:** Avaya recommends that you set sort_area_retained_size to 0, but does not require it. If you do not explicitly set this parameter, Oracle sets this to the same value as sort_area_size.
For Oracle on Windows only	Sort Area Retained Size – 0 **Note:** Avaya recommends this setting but does not require it.

Tip:

Depending upon the deployment of the Avaya IC system, you may need to increase the value for the Oracle shared pool size configuration parameter.

For Avaya OA configuration requirements, see *Avaya OA Installation Planning and Prerequisites*.

Detailed instructions on installation and configuration of an Oracle Server are beyond the scope of this manual. If you plan to use Oracle Server with Avaya IC but have not yet installed the Oracle Server, consult a qualified Oracle DBA for assistance.

Character set configuration for Oracle server

Avaya IC and Avaya OA require that you configure the national character set and character set parameters to UTF8. You set these options when you install the Oracle database.

This section provides you with an overview of how to identify whether the character set configuration has been set correctly for an Oracle database.

Configuring character set parameters - To configure character set parameters:

- For character set, configure NLS_CHARACTERSET as UTF8.
- For national character set, configure NLS_NCHAR_CHARACTERSET as UTF8.

Verifying character set parameters - To verify that these parameters are set to UTF8, execute the following sqlplus statement:

```
Select * from NLS_DATABASE_PARAMETERS;
```

Reconfiguring character set parameters - If the character set parameters were not configured as UTF8 during installation and creation of the initial database, perform the following steps to reconfigure the character set parameters:

1. Export all data from the global database that contains the Avaya IC databases and the Avaya OA historical database.

2. Drop the global database.
3. Reinstall Oracle and configure the character set parameters as UTF8, as described in Recommended values for installing Oracle server on page 257.
4. Reconfigure the Avaya IC database and the Avaya OA Historical database.
5. Reimport the data.

   For more information, see the Oracle documentation.

Installing Oracle Client

You must install the appropriate version of the Oracle client on every machine that hosts an Avaya IC component that requires access to the database. For more information, see Location for database clients on page 251.

You can view complete installation instructions for the Oracle client from the Oracle Technology Network Web site at http://otn.oracle.com

These links require a UserID and password for the Oracle Technology Network. If you do not have an Oracle Technology Network UserID and password, registration is free.

IBM DB2

Avaya IC servers and client components support IBM DB2 UDB version 8.1 with Fix Pack 5.

Important:
The DB2 version and Fix Pack version on the DB2 Server must match the versions on the DB2 Client.

This section includes the following topics:

- Supported versions of DB2 on page 262.
- Location of IBM DB2 Server on page 262.
- Configuring IBM DB2 server for Avaya IC on page 262.
- Installing IBM DB2 Client on page 264.
- Configuring IBM DB2 client for Avaya IC on page 264.

Supported versions of DB2

The following table describes the supported versions of IBM DB2, including maintenance levels and patches. You must install a supported version of IBM DB2 to avoid potential problems.

Version requirement	IBM DB2 8.1
Fix Pack/patches	5
Bits	32-bit mode
Code release	SQL08010
Level identifier	01010106
Informational tokens	• DB2 v8.1.1.8 • s030130 • U486246

Location of IBM DB2 Server

Install and configure the IBM DB2 server on all AIX machines that host the database instance for Avaya IC databases.

Configuring IBM DB2 server for Avaya IC

This section includes the following topics which describe the configuration parameters for IBM DB2:

- DB2 registry variables on page 263.
- Automatic configuration parameters on page 263.
- Manual configuration parameters on page 263.

DB2 registry variables

The following table includes the DB2 registry variables required for Avaya IC.

DB2 registry variable	Recommended entry	IBM DB2 7.2	IBM DB2 8.1
DB2_INDEX_2BYTEVARLEN	yes	✔	-
DB2_STRIPED_CONTAINERS	yes	✔	✔
DB2_RR_TO_RS	YES_OVERRIDE_RI	✔	✔
DB2COMM	tcpip	✔	✔

Manual configuration parameters

The following table includes DB2 configuration parameters required for Avaya IC. You must configure these parameters manually. Database Designer does not automatically configure these parameters.

Configuration parameter	Required minimum setting
APP_CTL_HEAP_SZ	256
MAXLOCKS	22
MAXAPPLS	500

Automatic configuration parameters

Avaya recommends that you use Database Designer to create and configure Avaya IC databases in DB2. Database Designer automatically sets the configuration parameters in the following table.

Configuration parameter	Required minimum setting
Database code set	UTF-8
Territory	US
pagesize	8KB
APPLHEAPSZ	512
bufferpool BUFFERPOOL8K	1000

Configuration parameter	Required minimum setting
tablespace USERSPACE8K	• pagesize: 8k • bufferpool: BUFFERPOOL8K
tablespace TEMPSPACE8K	• pagesize: 8k • bufferpool: BUFFERPOOL8K

Installing IBM DB2 Client

You must install the appropriate version of the IBM DB2 client on every machine that hosts an Avaya IC component that requires access to the client. For more information, see Location for database clients on page 251.

You can install the DB2 Administration Client from the DB2 Server CD-ROM or the DB2 Administration Clients CD-ROM.

Configuring IBM DB2 client for Avaya IC

You must catalog the IBM DB2 client on every machine that hosts a secondary Avaya IC Data server.

You do not need to catalog the IBM DB2 client on the machine that hosts the primary Data server that you used to connect to the database machine to configure the Avaya IC databases. The IBM DB2 client on that machine is catalogued when Database Designer creates the databases.

If you did not use Database Designer to create the databases, you need to catalogue the nodes on all IBM DB2 clients.

For more information about how to catalog the databases on an IBM DB2 client, see the DB2 documentation.

Chapter 12: Supported Telephony switches and software

This section includes the following topics:

- Exceptions for Telephony software and switches on page 266.
- Avaya Definity and Communication Manager products on page 267.
- Aspect CallCenter switches on page 271.
- Nortel Meridian switches and middleware on page 272.
- Ericsson MD110 switches on page 276
- Intel NetMerge Call Processing Software on page 277.
- Interactive Voice Response systems on page 279.

Avaya IC supports these telephony products over various protocols. The supported switches interface with Avaya IC in various ways, including:

- Switch connects directly to the Avaya IC Telephony server. For example, Avaya products and Aspect switches use this interface.
- Switch connects to the Avaya IC Telephony server with Intel NetMerge Call Processing Software as an interface. For example, Nortel Meridian-1 switches use this interface.

Exceptions for Telephony software and switches

The following table contains exceptions for telephony support for certain Avaya IC components.

Avaya IC component	Supported Telephony software and switch
Telephony server	Support for Telephony server on Solaris 8 with Nortel Symposium 4.2 or Meridian Link is only available for existing Avaya IC customers migrating from an earlier release who already have an Avaya IC system with a Nortel TS and an existing installation of IBM DCE 3.1.
Telephony server	No support for Telephony server on Solaris 9 with Nortel Symposium 4.2 or Meridian Link software and switch.
Telephony Queue Statistics (TSQS) server	Support for the TSQS server with Nortel Symposium 4.2 is only available for Windows.
Outbound Contact	No support for Aspect or Nortel software and switches.
Business Advocate	Support for multiple announcements is only available with the following switches: • Avaya Communication Manager 1.2 • Avaya Communication Manager 1.3 • Avaya Communication Manager 2.x • Avaya Communication Manager 3.x

Avaya Definity and Communication Manager products

Avaya IC supports the following Avaya Definity G3 and Communication Manager products. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

- Definity G3 R8.3
- Definity G3 R9
- Definity G3 R10
- Communication Manager 1.1 software
- Communication Manager 1.2 software
- Communication Manager 1.3 software
- Communication Manager 2.x software
- Communication Manager 3.x software

For information about the interface between Avaya products and the Avaya IC Telephony server, see *Telephony Connectors Programmer's Guide*.

This section includes the following topics:

- Supported components on page 268.
- Requirements for Avaya Definity and Communication Manager products on page 268.
- Downloading the CVLAN client on page 270.

Supported components

The following table describes the support for Avaya IC components and features with the supported Avaya Definity and Communication Manager products.

Switch	Supported operating systems for Telephony server	Multisite heterogeneous switch	Protocol
Definity G3: • R8.3 • R9 • R10	• Windows 2000 Server • Windows Server 2003 • Solaris 8 • Solaris 9 • AIX 5.1 • AIX 5.2	Yes	ASAI
Communication Manager releases: • 1.1 • 1.2 • 1.3 • 2.x • 3.x	• Windows 2000 Server • Windows Server 2003 • Solaris 8 • Solaris 9 • AIX 5.1 • AIX 5.2	Yes	ASAI

Requirements for Avaya Definity and Communication Manager products

Install the following prerequisites for Avaya Definity G3 and Communication Manager products. Consult the administrator responsible for the Avaya Communication Manager Call Center at your site for more detailed information about these requirements.

Important:
Avaya IC requires Call Center Elite. Call Center Elite includes Expert Agent Selection. Telephony in Avaya IC uses Expert Agent Selection to improve the synchronization between the agent desktop telephone and the Avaya Agent Softphone. These improvements were made available through tighter linkages with ASAI Agent States.

Install CVLAN Client version 8.2.5 or later to use the Service Observer feature of your Avaya Definity G3 and Communication Manager products. Do not use version 8.2.1 of the CVLAN Client. Version 8.2.1 can cause the Telephony server to fail under a moderate load.

The following table describes the requirements for the supported versions of Avaya Definity G3 and Communication Manager products.

Switch	Requirements
Definity G3: • R8.3 • R9	• CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 8.2.5 or later. • ADJLK Adjunct Link (not asai link) configured on the switch. • Call Center Elite with EAS for ASAI Agent States For Business Advocate only: • Increased Adjunct Route Capacity
Definity G3 R10	• CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 8.2.5 or later. • ADJLK Adjunct Link (not asai link) configured on the switch. Order of an Avaya IC ACD connector configures the RFA file on the switch appropriately. • Call Center Elite with EAS for ASAI Agent States For Business Advocate only: • Increased Adjunct Route Capacity
Communication Manager: • 1.1 • 1.2	• CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 8.2.5 or later. • ADJLK Adjunct Link (not asai link) configured on the switch. Order of an Avaya IC ACD connector configures the RFA file on the switch appropriately. • Call Center Elite with EAS for ASAI Agent States For Business Advocate only: • Increased Adjunct Route Capacity

Switch	Requirements
Communication Manager: • 1.3 • 2.x	• CVLAN Server 9 or 8.2.5 or later, mode 6 or 8, on MAPD. • CVLAN Client 8.2.5 or later. • ADJLK Adjunct Link (not asai link) configured on the switch. Order of an Avaya IC ACD connector configures the RFA file on the switch appropriately. • Call Center Elite with EAS for ASAI Agent States For Business Advocate only: • Increased Adjunct Route Capacity
Communication Manager 3.x	• AE Services 3.0 CVLAN Service (new implementations) • MAPD based CVLAN Server (existing implementations upgrading to 3.x). • CVLAN Client 8.2.5 or later. • ADJ-IP Adjunct Link (not asai link) configured on the switch. Order of an Avaya IC ACD connector configures the RFA file on the switch appropriately. • Call Center Elite with EAS for ASAI Agent States For Business Advocate only: • Increased Adjunct Route Capacity

Downloading the CVLAN client

To download the current version of the CVLAN client:

1. With your Web browser, navigate to the Avaya Technical Support website at:

   http://www.avaya.com/support/
2. Select the link for software downloads.
3. Select the link for CVLAN Client.
4. Select the link for CVLAN Client software.
5. Select the newest version of CVLAN Client. At this time, the current CVLAN version is 8.2.5.
6. Follow the instructions provided on the Web page, and select the appropriate CVLAN Client for your environment.

Aspect CallCenter switches

Avaya IC supports the following Aspect CallCenter switch with the Aspect Contact Server. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

- Aspect CallCenter 8.3 with Contact Server V4

The Aspect Contact Server is part of the Aspect Portal.

For information about the interface between the Aspect CallCenter switch and the Avaya IC Telephony server, see *Telephony Connectors Programmer's Guide*.

This section includes the following topics:

- Supported components on page 271.
- Requirements for Aspect CallCenter switches on page 271.

Supported components

The following table describes the support for Avaya IC components and features with Aspect CallCenter switches.

Switch	Supported operating systems for Telephony server	Multisite heterogeneous switch	Protocol
Aspect CallCenter 8.3	• Windows 2000 Server • Windows Server 2003	Yes	Aspect

Requirements for Aspect CallCenter switches

Avaya IC requires the following additional software for supported Aspect CallCenter switches:

- Aspect Contact Server (Portal)
- Aspect CMI server version 4.x, installed and available via an Ethernet connection to enable the Telephony server to establish a connection to the Aspect CallCenter System
- Aspect Real-time Receiver Custom Control runtime version, installed on the same machine as the TSQS server
- Aspect App Bridge Admin tool

Nortel Meridian switches and middleware

Avaya IC supports the Nortel Meridian-1 option 11, 61 and 81 switches, with X11 Release with V2111 patch (core patch 9MP05182), Version 5.42. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Nortel switches connect to Avaya IC through the Telephony server using NetMerge 6.0. For more information, see Intel NetMerge Call Processing Software on page 277.

For information about the interface between Nortel Meridian-1 switches and the Avaya IC Telephony server, see *Telephony Connectors Programmer's Guide*.

This section includes the following topics:

- Limitations on support for Nortel Meridian switches on page 272
- Supported links on page 273.
- Supported packages on page 273.
- Supported components on page 274.
- Requirements for Nortel Meridian switches on page 274.
- Intel NetMerge Call Processing Software on page 277.

Limitations on support for Nortel Meridian switches

Due to platform limitations with NetMerge and IBM DCE, Avaya IC provides only the following support for Nortel Meridian switches with Symposium 4.2 or Meridian Link:

- For all Avaya IC customers, Telephony server on either Windows 2000 Server or Windows Server 2003.
- For existing Avaya IC customers migrating from an earlier release who already have an Avaya IC system with a Nortel switch and an existing installation of IBM DCE 3.1, Telephony server on Solaris 8.

Note:

If existing Avaya IC customers use Nortel Symposium 4.2 with a TSQS server, the TSQS server is supported only on Windows 2000 Server and Windows Server 2003. The TSQS server for Nortel Symposium is not supported on Solaris.

Avaya IC does not support Nortel Meridian switches with Symposium 4.2 or Meridian Link on the following platforms:

- Solaris 9
- IBM AIX 5.1
- IBM AIX 5.2

Supported links

Avaya IC supports Nortel switches with the following links:

- Meridian Link
- Symposium Call Center Server 4.2
- Symposium Call Center Server 5.0

Supported packages

Avaya IC supports these products with the following packages:

- Integrated Message System (35)
- Command Status Link (77)
- Application Module Link (153)
- Meridian Link Module (209)
- Custom Controlled Routing (215) if your system uses the Workflow server to route calls
- Call ID (247)

Supported components

The following table describes the support for Avaya IC components and features with Nortel Meridian-1 switches. Limited support is available with the Telephony server on Solaris 8, as described in Limitations on support for Nortel Meridian switches on page 272.

Link	Supported operating systems for Telephony server	Multisite heterogeneous switch	Protocol
Meridian Link	• Windows 2000 Server • Windows Server 2003	Yes	MLP
Symposium Call Center Server 4.2	• Windows 2000 Server • Windows Server 2003	Yes	MLS
Symposium Call Center Server 5.0	• Windows 2000 Server • Windows Server 2003	Yes	MLS

Requirements for Nortel Meridian switches

Avaya IC requires the components listed in the following table for Nortel Meridian-1 switches.

Switch	Required software	Installation location
Meridian Link	Link 5c	Switch
	Nortel Meridian 1 X11, Release 24B, version 5.42	Switch
	Intel NetMerge Call Processing Software 6.0	Telephony server machine
	IBM DCE 3.1 with patch 6 (Solaris only)	Telephony server machine
	Meridian MAX version 9 with MSI	TS Queue Statistics server machine

Switch	Required software	Installation location
Symposium Call Center Server 4.2	Symposium Server 4.2	Symposium server machine
	Symposium Client 4.2	Symposium client machine
	Nortel Meridian 1 X11, Release 24B, version 5.42	Switch
	Intel NetMerge Call Processing Software 6.0	Telephony server machine
	IBM DCE 3.1 with patch 6 (Solaris only)	Telephony server machine
	Real Time Data Interface Toolkit	TS Queue Statistics server machine
Symposium Call Center Server 5.0	Symposium Server 5.0	Symposium server machine
	Symposium Client 5.0	Symposium client machine
	Nortel Meridian 1 X11, Release 24B, version 5.42	Switch
	Intel NetMerge Call Processing Software 6.0	Telephony server machine
	IBM DCE 3.1 with patch 6 (Solaris only)	Telephony server machine
	Real Time Data Interface Toolkit	TS Queue Statistics server machine

Ericsson MD110 switches

Avaya IC supports the Ericsson MD110 switch release BC10 or above running Ericsson Application Server 4.0. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

The Ericsson MD110 uses the Ericsson Application Link Server (via Intel NetMerge Call Processing software) to communicate with the Avaya TS.

For information about the interface between the Ericsson MD110 switch and the Avaya TS, see *Telephony Connectors Programmer's Guide*.

This section includes the following topics:

- Supported components on page 271.
- Requirements for Ericsson MD110 switches on page 276.
- Intel NetMerge Call Processing Software on page 277.

Supported components

The following table describes the support for Avaya IC components and features with the Ericsson MD110 switch.

Switch	Operating system	Multisite hetero switch	Protocol
Ericsson MD110, release BC10 or above	• Windows 2000 Server • Windows Server 2003	Yes	CSTA

Requirements for Ericsson MD110 switches

Avaya IC requires the following additional software for Ericsson MD110 switches:

Required software	Installation location
Ericsson MD110 release BC10 or above	Switch
Ericsson Application Link Server 4.0	ApplicationLink server
Intel NetMerge Call Processing Software 6.0	Telephony server

Intel NetMerge Call Processing Software

If your Avaya IC system includes a Nortel Meridian-1 switch or an Ericsson switch, you must install Intel NetMerge Call Processing Software 6.0. You can purchase the Intel NetMerge Call Processing Software 6.0 CD-ROM and documentation with Avaya IC. The Intel NetMerge Call Processing Software 6.0 CD-ROM includes Windows and Solaris versions.

You can view product information for Intel NetMerge Call Processing Software 6.0 from the following Web site:

http://www.intel.com/network/csp/products/ctconnect/index.htm

Note:

If you install the Intel NetMerge Call Processing Software server on a different machine than the machine that hosts the Telephony server, install the Intel NetMerge Call Processing Software client libraries on the machine with the Telephony server.

To set up Intel NetMerge Call Processing Software for Avaya IC with a Nortel Meridian-1 or an Ericsson MD110 switch:

1. Install Intel NetMerge Call Processing Software with the default settings for a typical installation.
2. Set the following value in the Intel NetMerge Call Processing Software PBX: **`dialby_equipment=true`**
3. Configure Intel NetMerge Call Processing Software for the switch protocol, using the values in the following table.

Configuration window	Symposium	Ericsson MD110
Configuration	• Enter a logical identifier, such as **`symposium`**. • Click **Add**.	• Enter a logical identifier, such as **`ericsson`**. • Click **Add**.
Switch Type for Link	• Select **Nortel Meridian with Symposium** • In the **Transport** field, select **TCP/IP**. • Click **Next**.	• Select **Ericsson MD110 BC9 and BC10** • In the **Transport** field, select **TCP/IP**. • Click **Next**.

Configuration window	Symposium	Ericsson MD110
Configuring TCP/IP Link	Enter the following values for the Symposium Module (SM): • **Switch IP Address** – SM IP address. Do not enter the host name. • **Port Number** – SM port (default 3000). • **Maximum Monitors** – Maximum number of channels to monitor simultaneously (default 1000). • **Application ID** – Host name of machine that runs Intel NetMerge Call Processing Software server. • **Machine ID** – Type of SM (default SL16). This field is case sensitive. • **Customer Number** – Customer number for MLM (default 0). • **Host name** – Host name of SM (default Lanlink). This field is case sensitive. • **Auto Start Link** – Check. • **Auto Restart Monitors** – Do not check. • **Switch Timestamp** – Do not check. • Press **Advanced**.	Enter the following values for the Ericsson Module (EM): • **Switch IP Address** – EM IP address. Do not enter the host name. • **Port Number** – EM port (default 3000). • **Maximum Monitors** – Maximum number of channels to monitor simultaneously (default 1000). • **Auto Start Link** – Check. • **Auto Restart Monitors** – Do not check. • **Switch Timestamp** – Do not check. • Press **Advanced**.
Advanced Settings for Link	• Select the Server Application Data checkbox. • Press **Save**. • Press **Save** again at the **Configuring TCP/IP Link** window.	• Select the Server Application Data checkbox. • Press **Save**. • Press **Save** again at the **Configuring TCP/IP Link** window.
Configuration	• Select the Logical Identifier is in the Existing Link list. • Click **Server Options**.	• Select the Logical Identifier is in the Existing Link list. • Click **Server Options**.
Server Options	Select the checkboxes for the following Server Interfaces: • Enable DCE/RPD Interface • Enable Java RMI Interface • Press **Save**.	Select the checkboxes for the following Server Interfaces: • Enable DCE/RPD Interface • Enable Java RMI Interface • Press **Save**.

Interactive Voice Response systems

Avaya IC supports the following interactive voice response systems (IVRs). For more information, see the documentation provided with the IVR.

IVR	Supported version
CONVERSANT System for Interactive Voice Response	• 8.0 • 9.0
Avaya Interactive Response	• 1.0 • 1.2
Edify Interactive Voice Response	8.0
Periphonics IVR	5.4
IBM WebSphere Voice Response	2.3 and greater
Intervoice TRM	510

For information on how to configure the CONVERSANT System for Interactive Voice Response, see *External Function Library for Avaya IVR Programmer's Guide*.

Note:

IBM WebSphere and Intervoice require connectors that are only available from the IVR manufacturer. Contact IBM or Intervoice for current information on their support for Avaya IC and to acquire the required software to integrate their IVRs with Avaya IC

Chapter 13: Supported Web servers

This section provides information about supported Web servers and Java SDK. This section includes the following topics:

- Components that require a Web server on page 281
- Supported Web server versions on page 282
- Microsoft Internet Information Server on page 283.
- Sun Java System Web Server on page 286.
- IBM HTTP Server on page 290.
- Java SDK on page 291.
- IBM Websphere Application server on page 293.

Components that require a Web server

The following Avaya Interaction Center (Avaya IC) components require a Web server:

- Web Management external website with chat and ICM server
- Web Management administration website
- Email Management Template Administration
- Agent Installer
- Web License Manager
- Avaya Agent Web Client (IBM Websphere only)

Supported Web server versions

Avaya supports the versions listed below. For more details about the definition of supported versions and about subsequent updates or services packs of the software, see About the supported versions on page 42.

Web server	Windows 2000 Server	Windows Server 2003	Solaris 8	Solaris 9	AIX 5.1	AIX 5.2
Microsoft Internet Information Server (IIS) 5.0	✔	-	-	-	-	-
Microsoft Internet Information Server (IIS) 6.0	-	✔	-	-	-	-
Sun Java System Web Server 6.0 SP5	-	-	✔	-	-	-
Sun Java System Web Server 6.1 SP1	-	-	-	✔	-	-
IBM HTTP Server 1.3.28	-	-	-	-	✔	✔
IBM Websphere 6.0 (Avaya Agent Web Client only)	✔	✔	-	✔	-	✔

Note:

The Voice Media Manager (VMM) service required for Voice Chat does not support AIX. You must host the VMM on a Windows or Solaris machine. Voice Chat does not function with the VMM on AIX.

Microsoft Internet Information Server

If your system uses a supported Windows Server operating system to host the Avaya IC servers, you must use Microsoft IIS as your Web server.

Microsoft IIS is part of the Windows Server operating system. For information on how to configure and use Microsoft IIS, see the documentation for the Windows Server operating system.

This section includes the following topics:

- Supported versions of Microsoft IIS on page 283.
- Security patches and hot fixes for Microsoft IIS on page 283.
- Security considerations for Microsoft IIS 5.0 on page 284.
- Security considerations for Microsoft IIS 6.0 on page 284.
- Configuring IIS 6.0 for Avaya IC on page 284

Supported versions of Microsoft IIS

The following table describes the versions of Microsoft IIS that Avaya IC supports for each supported version of Windows.

Windows version	Microsoft IIS version
Windows 2000 Server	Microsoft IIS 5.0
Windows Server 2003	Microsoft IIS 6.0

Security patches and hot fixes for Microsoft IIS

You need to check the Microsoft Web site for security bulletins and hot fixes for Microsoft IIS that describe possible security issues and solutions. Review these security bulletins after you install Microsoft IIS, make any required configuration changes, and apply the required patches.

You can find a listing of current security bulletins, patches, and hot fixes for Microsoft IIS from the following Web site: http://www.microsoft.com/technet/security/current.aspx

Continue to monitor the Microsoft security bulletins and apply all future hot fixes when they are made available.

Security considerations for Microsoft IIS 5.0

The IIS Lockdown Tool increases the security of a Microsoft IIS 5.0 deployment for Avaya IC and Avaya OA and reduces the risk of intrusion. The IIS Lockdown Tool can help you close several security risks that can occur with IIS. However, the IIS Lockdown Tool cannot completely remove all risk of intrusion.

Note:

Microsoft creates and maintains the IIS Lockdown Tool. Avaya recommends that you review and follow the security guidelines outlined by Microsoft for IIS. Avaya does not make security recommendations for IIS or Windows.

Install the most recent security patches and hot fixes for Microsoft IIS 5.0 before you install and run the IIS Lockdown Tool.

You can download a copy of the IIS Lockdown Tool version 2.1 from the following Web site:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC

For specific recommendations and instructions on how to configure security with the IIS Lockdown Tool, see Appendix B: IIS Lockdown Tool on page 411.

Security considerations for Microsoft IIS 6.0

The default configuration settings in Microsoft IIS 6.0 meet or exceed the security configuration settings made by the IIS Lockdown Tool. You do not need to install the IIS Lockdown Tool if your Avaya IC system uses Microsoft IIS 6.0.

For more information about security considerations for Microsoft IIS 6.0, see the documentation provided with Microsoft IIS 6.0.

Configuring IIS 6.0 for Avaya IC

If you host your Avaya IC servers on Windows Server 2003, you need to configure IIS 6.0 to ensure that the Avaya IC system functions correctly.

This section includes the following topics:

- Configuring IIS 6.0 for Avaya IC plugin and Tomcat ISAPI extensions on page 285.
- Configuring MIME types for IIS 6.0 on page 286.

Configuring IIS 6.0 for Avaya IC plugin and Tomcat ISAPI extensions

To be able to access the WebLM and the Web Management Website, you must configure IIS 6.0 to recognize and allow the ISAPI extensions used by the Avaya IC plugin and by Tomcat. To do this, you can either configure IIS 6.0 to allow All Unknown ISAPI Extensions, or you can add the extensions for the Avaya IC plugin and Tomcat to IIS 6.0.

Configuring IIS 6.0 to allow All Unknown ISAPI Extensions - To configure IIS 6.0 to allow All Unknown ISAPI Extensions:

1. In the **Computer Management** window for Windows 2003, expand the following in the left pane: **Services and Applications** > **Internet Information Service** > **Web Service Extensions**.
2. In the right pane for Web Service Extensions, make sure that the status of **All Unknown ISAPI Extensions** is **allowed**.

   If you cannot see **All Unknown ISAPI Extensions** in the **Computer Management** window, make sure that you have installed all required components of IIS 6.0. For more information about the IIS 6.0 components that are required, see the IIS documentation provided with Windows 2003.

Adding the Avaya IC plugin and Tomcat extensions to IIS 6.0 - To add the Avaya IC plugin and Tomcat extensions to IIS 6.0:

1. In the **IIS Management** window, right-click on the **Web Service Extensions** folder and select **Add a new Web service extension**.
2. Add the extensions and files in the following table and enable Set extension to Allowed for each extension.

Extension name	File to add for the extension
IC plugin	*IC_INSTALL_DIR*\IC70\comp\icws\isplugin.dll
Tomcat	*IC_INSTALL_DIR*\IC70\tomcat\modules\ isapi_redirect.dll

3. Set the execute permission flag for the IIS anonymous user account. The IIS anonymous user account is usually IUSR_*machinename* on the IIS plugins:
   - isapi_redirect.dll
   - ISPlugin.dll
4. Stop and restart IIS Admin.

Configuring MIME types for IIS 6.0

If your Avaya IC system includes Voice Chat, and you host your Avaya IC servers on Windows Server 2003, you must configure the MIME types for IIS 6.0.

Configure the MIME types in the following table on the **HTTP Headers** tab of the **Default Website Properties** dialog box and of the properties dialog boxes for the virtual directory that is used for the agent installation.

Extension	MIME type
.dll	application/x-msdownload
.ini	text/html
.imp	text/html
.txt	text/html

Sun Java System Web Server

The type of Web server required for Avaya IC servers depends upon the version of Solaris. This section provides information specific to Avaya IC that you need to install and configure a supported version of Sun Web Server.

This section includes the following topics:

- Supported versions of Sun Java System Web server on page 287.
- Limitations on Sun Java System Web Server support on page 287.
- Sun Java System Web Server 6.0 configuration parameters on page 287.
- Sun Java System Web Server configuration parameters on page 288.

Supported versions of Sun Java System Web server

The following table describes the versions of Sun Java System Web server that Avaya IC supports for each supported version of Solaris.

Solaris version	Sun Web Server	Download location
Solaris 8	Sun Java System Web Server 6.0 SP5 (formerly Sun ONE Web Server 6.0 SP5)	http://wwws.sun.com/software/download/products/3e3add06.html
Solaris 9	Sun Java System Web Server 6.1 SP1	http://wwws.sun.com/software/download/products/4000635d.html

Limitations on Sun Java System Web Server support

Avaya IC support for the Sun Java System Web servers has the following restrictions.

- Avaya IC does not support the Windows versions of either the Sun ONE Web Server 6.0 or Sun Java System Web Server 6.1.
- The Administrative Web Server may have some Javascript compatibility problems with Internet Explorer 5.0. If the Web page does not display correctly or **Apply** is not active, open the Administrative Web server with a Netscape 7.0 browser.

Sun Java System Web Server 6.0 configuration parameters

A detailed guide to installing and configuring a Sun Java System Web Server is beyond the scope of this document. For more information about the Sun Java System Web Servers, see the documentation provided by Sun and the following Web site:

http://wwws.sun.com/software/download/products/3e3add06.html

The following table includes some recommended values when you install Sun ONE Web server to use with Avaya IC.

Parameter	Value
Installation staging directory	iplanet_install
Installation type	Typical installation
Installation components	• All • Server Core and Java Support (1, 3)

Parameter	Value
Host name	Default (if correct)
User and group	Nobody (or a user without general privileges)
iWS Administration server “run-as” user	root
Admin login	Admin
Admin password	admin
Port	8888
Port	80
Docs	Default
JDK	Use own JDK
libs	Default
classpath	Default

Sun Java System Web Server configuration parameters

A detailed guide to installing and configuring a Sun Java Web Server is beyond the scope of this document. For more information about the Sun Web Servers, see the documentation provided by Sun and the following Web site:

http://wwws.sun.com/software/download/products/4000635d.html

The following table includes some recommended values when you install Sun Java Web server to use with Avaya IC.

Parameter	Value
Installation type	Typical installation
Installation components	• All • Server Core • Java Development Kit
Computer name	Default

Parameter	Value
System User / Group	Choose a UNIX user and group to represent the Sun Web Server in the user directory. The Web Server will run as this user. Avaya recommends that this user should have no privileges in the computer network system. The Administration Server will give this group some permissions in the server root to perform server-specific operations. If you have not yet created a user and group for the Web Server, create this user and group using your native UNIX system utilities.
Run Web Server Administration Server user	The Web Server Administration Server is different from other Web servers on the system. Avaya recommends that the Web Server Administration Server run with a different user id than those used by the other Web servers on the machine. The Administration Server user is the only user able to write Web server configuration files. **Note:** If the Web Server Administration Server is run as "root", you can use the administration interface to start and stop the other Web servers.
Web Server Admin User Name/ Password	The Web Server Administration Server requires its own administrative user name and password for GUI access. When you access the Web Server Administration Server interface, it will prompt you for the administrative user name and password. Please select a user name and password now. For example, select admin/admin
Web Server Admin Server Port	8888
Web Server Port	80
Web Server Content Root	Default

IBM HTTP Server

This section provides information specific to Avaya IC that you need to install and configure the supported version of IBM HTTP Server.

Tip:

Avaya Agent Web Client also uses the IBM HTTP Server provided with IBM WAS. For information about the supported version of IBM HTTP Server used by Avaya Agent Web Client, see IBM Websphere Application server on page 293.

This section includes the following topics:

- Supported version of IBM HTTP server on page 290.
- Restriction on the deployment of IBM HTTP Server on page 290.
- IBM HTTP Server configuration parameters on page 291.

You can obtain more information about IBM HTTP Server 1.3.28 from the following Web site:

http://www-3.ibm.com/software/webservers/httpservers/

Supported version of IBM HTTP server

If your system uses AIX 5.1 or AIX 5.2 as the operating system for the Avaya IC servers, you must use IBM HTTP Server, release 1.3.28, as your Web server.

Restriction on the deployment of IBM HTTP Server

Avaya recommends that you install IBM WAS on a machine that is separate from the Avaya IC server and Avaya OA server. The HTTP Server can reside on the same machine as IBM WAS, but this is not recommended. For more information about installing Avaya OA, see *Avaya OA Installation Planning and Prerequisites*.

IBM HTTP Server configuration parameters

A detailed guide to installing and configuring IBM HTTP Server is beyond the scope of this document. See the installation guide for IBM HTTP Server.

When you install and configure IBM HTTP Server, use the following parameters:

Parameter	Value
ServerName Property is in the following file: `<IBMHttPServer_installation_root>/conf/httpd.conf`	Fully-qualified domain name of the machine that hosts the IBM HTTP Server. **CAUTION:** Do not use `localhost` for the value. A value of `localhost` for `ServerName` causes an infinite redirection loop when you access the Administration Website.

Java SDK

You must install and configure the Java SDK on the machines that host certain Avaya IC components. This section includes the following topics.

- Supported versions of the Java SDK on page 292.
- Components that require the Java SDK on page 292.
- Installing the JDK for Windows and Solaris on page 292.
- Installing the JDK for AIX on page 293.

Supported versions of the Java SDK

The following table shows the version of the Java SDK that you need to install for each supported operating system:

Operating system	Java SDK version
Windows	Sun JDK 1.3.1_15
Solaris	Sun JDK 1.3.1_15
AIX	IBM JDK 1.3.1, 32 bit

Components that require the Java SDK

The following table describes the Avaya IC components which require the Java SDK.

Avaya IC component	Description
Website	For systems with Web Management, runs the customer-facing website and the administration website for Web Management.
Email Template Administration	For systems with Email Management, lets you create, customize, and maintain templates for responses to email contacts and outbound email contacts to customers.
Web License Manager	For all Avaya IC systems, hosts the Avaya license for your Avaya IC system.

Installing the JDK for Windows and Solaris

To install the Java JDK for Windows or Solaris:

1. Go to http://java.sun.com and navigate to the product archive.
2. Download JDK release 1.3.1_15, including the optional Java 2 Runtime Environment.
3. Install the JDK on all required machines.

Installing the JDK for AIX

To install the Java JDK for AIX:

1. Go to http://www.ibm.com and navigate to the product archive.
2. Download IBM JDK 1.3.1, 32 bit, build ca131-20030329.

   http://www-106.ibm.com/developerworks/java/jdk/aix/index.html
3. Install the JDK on all required machines.

IBM Websphere Application server

Avaya Agent Web Client requires IBM Websphere Application server (IBM WAS).

This section provides information specific to Avaya IC that you need to configure the supported version of IBM WAS.

This section includes the following topics:

- Supported version of IBM WAS on page 293.
- Installing IBM WAS on page 294.
- Installing IBM WAS on page 294.
- Configuring IBM WAS for Avaya Agent Web Client on page 294.

Supported version of IBM WAS

For all Avaya IC systems with Avaya Agent Web Client, you must use IBM WAS 6.0 as the Application server for Avaya Agent Web Client.

Installing IBM WAS

For Avaya Agent Web Client, use the instructions and configuration recommendations provided in the IBM documentation to install the following IBM WAS components:

IBM WAS 6.0 - Install IBM WAS 6.0 on all machines that will host the Avaya Agent Web Client application.

IBM WAS Application Server Kit (AST) - Install IBM AST with the default configurations on a Windows machine, as described in the following table.

Location of IBM WAS	Location of IBM AST
Windows machine	You can install IBM AST: • On the same machine as IBM WAS • On a different Windows machine than IBM WAS
Solaris or AIX machine	Install IBM AST on a separate Windows machine.

IBM HTTP server and plug-in - Install the versions of IBM HTTP Server and the IBM HTTP Server plug-in provided with IBM WAS:

Configuring IBM WAS for Avaya Agent Web Client

This section describes the mandatory configuration changes that you must make to the IBM WAS server that hosts Avaya Agent Web Client. These configuration changes are required for IBM WAS on all supported operating systems.

This section includes the following topics:

- Changing the JVM heap size on page 295.
- Changing Web Container thread pool size on page 295.
- Disabling the Dynamic Cache Service on page 296.

Changing the JVM heap size

To change the JVM heap size:

1. In the left pane of the IBM WAS Administrative Console, select **Servers > Application Servers**.
2. In the **Application Servers** pane, select the IBM WAS application server that hosts Avaya Agent Web Client.

   For example, if you will host Avaya Agent Web Client on the default application server, select Server1.
3. In the **Configuration** tab, select **Server Infrastructure** > **Java And Process Management** > **Process Definition** > **Java Virtual Machine**.
4. Under **Configuration**, set the following values:
   - Initial Heap Size: 512
   - Maximum Heap Size: 1024.
5. Save the changes to the IBM WAS Master Configuration:
   a. Select **Save to the Master Configuration**.
   b. On the next page, select **Save**.

Changing Web Container thread pool size

To change the Web Container thread pool size:

1. In the left pane of the IBM WAS Administrative Console, select **Servers > Application Servers**.
2. In the **Application Servers** pane, select the IBM WAS application server that hosts Avaya Agent Web Client.

   For example, if you will host Avaya Agent Web Client on the default application server, select Server1.
3. In the **Configuration** tab, select > **Additional Properties** > **Thread Pools** > **WebContainer**.
4. Under **Configuration**, set the following values:
   - Minimum Size: 150
   - Maximum Size: 512
   - Check the **Is Growable** box.
5. Save the changes to the IBM WAS Master Configuration:
   a. Select **Save to the Master Configuration**.
   b. On the next page, select **Save**.

Disabling the Dynamic Cache Service

To disable the Dynamic Cache Service:

1. In the left pane of the IBM WAS Administrative Console, select **Servers > Application Servers**.
2. In the **Application Servers** pane, select the IBM WAS application server that hosts Avaya Agent Web Client.

   For example, if you will host Avaya Agent Web Client on the default application server, select Server1.
3. Select **Container Settings** > **Container Services** > **Dynamic Cache Service**.
4. In the **Configuration** tab, make sure that **Enable service at server start up** is unchecked.

Chapter 14: Supported email servers

Certain components of Avaya Interaction Center (Avaya IC) require access to email servers that support the following protocols:

POP3 - Post Office Protocol - RFC-1725, required to receive email contacts.

SMTP - Simple Mail Transport Protocol - RFC - 821, required to send email contacts

SMTP and POP3 are standard Internet email protocols. Most common mail servers, such as Microsoft Exchange and Lotus Notes, support these protocols. You need to install or configure your enterprise email server to support SMTP and POP3 services.

CAUTION:
Turn off Microsoft Word Autocorrect features if you use Word as the editor for Outlook. The Autocorrect features can causes application errors in the Avaya IC agent desktop.

Configuring SMTP and POP3 servers

Email Management works closely with other servers and applications on your Local Area Network.

To configure your email system:

1. Configure your mail server to allow POP3 and SMTP access.

   The Avaya Email Server uses a POP3 server to retrieve incoming messages, and uses an SMTP server to send outgoing messages.

2. Define an email address for your email system that matches the following configuration. You will set this configuration in the Notification server:
   - Email server name
   - Domain name
   - Default email sender name, for example user@xyzcorp.com

3. Verify the email system on the machine, as described in the following table.

Operating system	Verification step
Windows	Notification server verifies the ability to send a simple email contact to the default email sender name. The Notification server will not start if the email address is invalid.

Solaris	You must verify that the default email sender name is accessible from the mail daemon on the machine that hosts the Notification server.
	Execute the following command from any directory to send a simple text message:
	`mail <email_address>`
	`test`
	`.`
	Where <*email_address*> is the default email sender name. For example, enter `user@xyzcorp.com`

AIX	You must verify that the default email sender name is accessible from the mail daemon on the machine that hosts the Notification server.
	Execute the following command from any directory to send a simple text message:
	`mail <email_address>`
	`test`
	`.`
	Where <*email_address*> is the default email sender name. For example, enter `user@xyzcorp.com`

4. Remove all aliases and distribution lists from the mail accounts that Email Management handles.

   To avoid potential mail loops, do not include mail accounts that are polled by Email Management in any distribution lists or aliases.

5. Configure your firewall for Email Management:
   - To send messages to the SMTP server on port 25
   - To retrieve messages from the POP3 server on port 110
   - To allow agent machines to communicate with the Email server on port 19113
   - To allow administrators to communicate with Mail Template Administration on port 19114
6. Create mail accounts for the following roles in your contact center:
   - Bounce (rejected) message

- Support message

Email Management handles these accounts as POP3 mailboxes not IMAP mailboxes.

7. Do not store email messages on a mail server after they have been retrieved and archived. Email Management does not support IMAP. Email Management stores incoming and outgoing messages in IC database.
8. Enable SMTP relaying if Email Management will send replies to customers outside the local domain.

Chapter 15: Supported third party applications

Avaya Interaction Center (Avaya IC) works with several third party applications from other vendors. These applications support various functions within the product, such as database management and reports.

This section includes the following topics that describe third party applications:

- Adobe Acrobat Reader on page 302
- Compilers for Avaya IC Server SDK on page 302
- Lotus Sametime on page 303
- Tomcat on page 303
- IBM WebSphere on page 303

The following topics in other sections provide information about supported third party applications and the requirements of Avaya IC:

- Chapter 2: Required software components on page 41.
- Operating systems, see Chapter 9: Supported operating systems on page 215.
- Database management systems, see Chapter 11: Supported database management systems on page 245.
- Telephone switches, see Chapter 12: Supported Telephony switches and software on page 265.
- Intel NetMerge Call Processing Software, see Intel NetMerge Call Processing Software on page 277.
- Web servers, see Chapter 13: Supported Web servers on page 281.
- Java SDK, see Java SDK on page 291.
- Email servers, see Chapter 14: Supported email servers on page 297.

For more information about Avaya OA and its prerequisites, see *Avaya OA Installation Planning and Prerequisites*. For detailed information about Avaya IC for Siebel 7, see *Avaya IC for Siebel 7 Integration*, which is available on the Avaya IC for Siebel 7 installation CD-ROM.

Adobe Acrobat Reader

Avaya IC requires the Adobe Acrobat Reader 5.0 (or later version) to view the Avaya IC PDF documentation and access the cross-document indexing and search capabilities of the Avaya IC documentation.

The PDF documents are available:

- On the Avaya IC CD-ROM
- On the Avaya IC Documentation CD-ROM
- On all machines that host Avaya IC components

You can download the free Acrobat Reader and the separate Search functionality from a link on the splash screen of the Avaya IC documentation CD-ROM or directly from the Adobe Web site at http://www.adobe.com/

Compilers for Avaya IC Server SDK

If you build custom Avaya IC servers with the SDK, you must install the appropriate compiler for the Avaya IC server operating system. The following table shows the compiler for each supported operating system.

Server operating system	Supported SDK compiler
AIX	AIX VisualAge C++ Professional / C for AIX Compiler, Version 5
Solaris	Sun Forte Developer 6, Update 2
Windows	Microsoft Visual Studio 6, SP 5

Lotus Sametime

Sametime 2.5 is a product of Lotus/IBM that can be integrated with Avaya IC. Sametime allows your agents to share a session with customers. The Sametime session provides application sharing, whiteboarding, and chat and IP audio and video capabilities.

If you integrate Sametime with Avaya IC, agents in your contact center can initiate a Sametime session when they are in a chat and collaboration session. Your customer can join the Sametime session after the agent initializes the session.

For information about Sametime, see the following Web site:

http://www.lotus.com/products/lotussametime.nsf/wdocs/homepage

Tomcat

Avaya IC installs Tomcat 3.3.1-A with the Avaya IC servers. Tomcat is the servlet container of the Jakarta Project. Tomcat is developed in an open and participatory environment and released under the Apache Software License.

IBM WebSphere

Avaya Agent Web Client requires IBM WebSphere software. The WebSphere Application Server Kit (AST) packages the Avaya Agent Web Client sources so the Avaya Agent Web Client software can be deployed to IBM WAS. IBM WAS hosts the Avaya Agent Web Client software. The Avaya Agent Web Client software provides the user interface and dynamic content that is accessed by agents through a Web browser. You must meet the minimum hardware and software requirements for Avaya IC and IBM WAS.

For more information about supported software for Avaya Agent Web Client, see Requirements for Avaya Agent Web Client on page 66. For more information about supported software for IBM WAS, refer to the documentation provided by IBM.

Chapter 16: Business Advocate

You must configure the operating system and database for Business Advocate before you install Avaya Interaction Center (Avaya IC). The configuration steps are different for each supported operating system and database.

This section describes the operating systems and databases supported by Business Advocate and the configuration steps for each supported platform. This section includes the following topics:

- Exceptions to platform support for Business Advocate on page 305.
- Configuring Windows for Business Advocate on page 306.
- Configuring SQL Server for Business Advocate on page 312.
- Configuring Oracle for Business Advocate on page 315.

Exceptions to platform support for Business Advocate

The following table describes the exceptions to platform support for Business Advocate for Avaya IC. For information about which platforms are supported by Business Advocate, see Required software for Business Advocate on page 60.

Platform	Exception
Operating system	Resource Manager servers support only Windows. No AIX or Solaris support for Resource Manager servers. Business Advocate does not function with the Resource Managers servers on AIX or Solaris.
Database	Advocate database supports only SQL Server or Oracle. No DB2 support for the Advocate database. Agent administration for Business Advocate does not function with the Advocate database on DB2. You can use DB2 for the other Avaya IC databases.

Configuring Windows for Business Advocate

If your Avaya IC system includes Business Advocate, you must install Message Queuing service (MSMQ) support on the machine that hosts the Resource Manager server. This machine serves as your MSMQ client for Business Advocate.

You need a Windows CD-ROM for these steps.

To install the MSMQ service, perform the steps in the following sections:

- Configuring Windows Server 2003 for Business Advocate on page 306.
- Configuring Windows 2000 Server for Business Advocate on page 309.
- Configuring Windows for Thai (optional) on page 311.
- Troubleshooting the installation of MSMQ on page 311.

Configuring Windows Server 2003 for Business Advocate

This section describes the specific configurations required to run Business Advocate servers on Windows server 2003. This section includes the following topics:

- Configuring the Windows Server 2003 application server role on page 306
- Setting up the Active Directory domain for Windows Server 2003 on page 307
- Installing the MSMQ service for Windows Server 2003 on page 308

Configuring the Windows Server 2003 application server role

Business Advocate requires an application server role on Windows Server 2003 If you host the Resource Manager servers on a Windows 2003 machine, you must configure the application server role.

If you do not configure Windows Server 2003 with an application server role, Business Advocate cannot install and function correctly. The Business Advocate installer displays an error message and cannot complete the installation. If you receive an error during the installation, perform the following steps and reinstall Business Advocate.

Tip:

Use the **Manage Your Server** wizard to configure the application server role to ensure that Distributed Transaction Coordinator (DTC) access is enabled. If you use **Add/Remove programs** to configure the application server role, Windows Server 2003 does not enable DTC access.

To configure Windows Server 2003 with an Application Server role:

1. Select **Start** > **Manage Your Server**.

2. In the **Manage Your Server** window, select **Add or remove a role**.
3. In the first window of the **Configure your server** wizard, select **Next**.
4. In the second window of the **Configure your server** wizard:
   a. Select **Application Server** from the **Server Role** column.
   b. If the **Configured** column displays:
      - **Yes** – select **Cancel**.
      - **No** – select **Next**.
5. Select **Next** on all remaining windows of the **Configure your server** wizard.

Setting up the Active Directory domain for Windows Server 2003

The MSMQ server requires Active Directory services. You must join all Windows machines that host Business Advocate servers to an Active Directory domain. If your Avaya IC system includes servers on Solaris or AIX, you need to join all Windows machines that host Resource Manager servers to an Active Directory domain.

If your network does not include an Active Directory domain, you must create a new Active Directory domain. A machine that hosts one or more Business Advocate servers can serve as the Active Directory domain controller.

You must join all Windows machines that host Business Advocate servers to the same Active Directory domain as the machine that hosts the Resource Manager server.

To create an Active Directory domain:

1. Select **Start** > **Manage Your Server**.
2. In the **Manage Your Server** window, select **Add or remove a role**.
3. In the first window of the **Configure your server** wizard, select **Next**.
4. In the second window of the **Configure your server** wizard:
   a. Select **Domain Controller (Active Directory)** from the **Server Role** column.
   b. If the **Configured** column displays:
      - **Yes** – select **Cancel**.
      - **No** – select **Next**.
5. Make the configuration selections in the following table. If no selection is specified, select **Next** in that window to accept the default.

Configuration parameter	Recommended entry
Domain controller type	Select **Domain controller for a new domain**.
Create new domain	Select **Domain in a new forest**.

Configuration parameter	Recommended entry
Full DNS name for new domain	Type fully-qualified name for the domain. For example, `advocate.xyzcorp.com`.
Domain NetBIOS name	Accept the name shown, or type a new name. For example, `ADVOCATE`.
Database folder	Type the folder path or browse to the folder where the database will be stored.
Log folder	Type the folder path or browse to the folder where the log files will be stored.
Shared system volume	Type the folder path or browse to the folder on an NTFS volume where the server will store a copy of the public files for the domain.
Permissions	Select Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems.
Directory services restore mode administrator password	Type and confirm the password for the Administrator account to be used in Restore mode.

Installing the MSMQ service for Windows Server 2003

After you have joined a machine to an Active Directory domain, you must install the MSMQ service. If you host Resource Manager servers on a Windows 2000 Server machine, see Installing the MSMQ service for Windows 2000 Server on page 310.

> **Important:**
> If the MSMQ service is already installed and configured before you join a machine to the Active Directory domain, you have to re-install the service on that machine after you join the machine to the domain.

To install the MSMQ service:

1. If you have not already done so, log into the machine with a Windows Active Directory Domain account that has domain and local administrator privileges.

   By default, the Administrator account for the domain has the required privileges.
2. From the **Start** menu, select **Windows Control Panel** > **Add or Remove Programs**.
3. Select **Add/Remove Windows Components**.
4. In the **Windows Components** Wizard:
   a. Select the **Application Server** entry.
   b. Select **Details**.

5. In the **Application Server** window:
   a. Verify whether there is a check mark in the box next to **Message Queuing Service**.
   b. If there is no check mark, select the box to add a checkmark.
   c. Select **Details**.
6. In the **Message Queuing Type** window:
   a. Under **Subcomponents of Message Queueing**, make sure that the following boxes are checked. You do not need to check the remaining boxes in this section.
      - Active Directory Integration
      - Common
   b. Select **Details**.
7. In the **Common** window:
   a. Under **Subcomponents of Common**, make sure that the following boxes are checked:
      - Core functionality
      - Local Storage
   b. Select **OK**.
8. Select **OK** in each window until you return to the **Windows Components** Wizard.
9. In the **Windows Components** Wizard, select **Next**.

   Windows Server 2003 installs and configures the MSMQ service. If prompted, enter the DNS or NetBIOS name of a supporting server in the local site.
10. Select **Finish** to complete the setup.

Note:

The MSMQ service cannot send or receive messages until a connection with a Message Queuing server is established.

Configuring Windows 2000 Server for Business Advocate

This section describes the specific configurations required to run Business Advocate servers on Windows 2000 Server. This section includes the following topics:

1. Setting up the Active Directory domain for Windows 2000 Server on page 310.
2. Installing the MSMQ service for Windows 2000 Server on page 310.

Setting up the Active Directory domain for Windows 2000 Server

The MSMQ server requires Active Directory services. You must join all Windows machines that host Business Advocate servers to an Active Directory domain.

If your network does not include an Active Directory domain, you must create a new Active Directory domain. A machine that hosts one or more Business Advocate servers can serve as the Active Directory domain controller.

You must join all Windows machines that host Business Advocate servers to the same Active Directory domain as the machine that hosts the Resource Manager server.

To create an Active Directory domain:

1. On the machine that will be your Active Directory domain controller, open the Windows Control Panel.
2. Select **Administrative tools** > **Configure Your Server** > **Active Directory**.
3. In the right pane, select **Start the Active Directory wizard**.
4. Follow the prompts in the wizard to update your machine to an Active Directory Domain Controller.

Installing the MSMQ service for Windows 2000 Server

After you have joined a machine to an Active Directory domain, you must install the MSMQ service. If you host Resource Manager servers on a Windows Server 2003 machine, see Installing the MSMQ service for Windows Server 2003 on page 308.

> **Important:**
> If the MSMQ service is already installed and configured before you join a machine to the Active Directory domain, you have to re-install the service on that machine after you join the machine to the domain.

To install the MSMQ service:

1. If you have not already done so, log into the machine with a Windows Active Directory Domain account with local administrator privileges on that machine.
2. In the Windows Control Panel, select **Add or Remove Programs** > **Add/Remove Windows Components**.
3. In the Windows Components Wizard, confirm whether there is a check mark in the box next to **Message Queuing Service**.
4. If there is no check mark:
   a. Select the box to add a checkmark.
   b. Select **Next**.
5. In the **Message Queuing Type** window:
   a. Select **Independent client**.

b. Select **Next**.

6. In the **Message Queuing Server** window:

   a. Select **Message Queuing service will access a directory service**.

   b. In the **Domain controller** field, enter the IP address of the Active Directory domain controller.

   c. Select **Next**.

   Windows 2000 Server installs the MSMQ service.

Configuring Windows for Thai (optional)

If you install Windows with an English CD-ROM, and then configure for Thai, you must configure Windows to display the Thai characters. If you do not configure Windows correctly:

- Business Advocate Supervisor displays Thai characters as question marks when creating qualifiers.
- Avaya OA events for updating qualifiers do not function correctly.

Important:
You must configure Windows for Thai before you install the SQL Server database. You will see problems if either the database or Business Advocate is installed before the operating system is changed to Thai.

To retrieve and display Thai characters correctly in an English version of Windows:

1. Change the value of the **Default Locale** configuration parameter to Thai.
2. Change the value of the **System Locale** configuration parameter to Thai.
3. Change the value of the **User Locale** configuration parameter to Thai.

   After you configure the English version of Windows for Thai, install SQL Server on the machine.

Troubleshooting the installation of MSMQ

The installation of MSMQ can fail if the login ID and the computer that hosts MSMQ do not meet specific criteria. For example, you may receive a Message Queue Server Setup Failure error message with a message similar to the following:

> Setup failed to create the MSMQ Configuration (msmq) or MSMQ Settings object in Active Director. Please add the "Create All Child Objects" and "Delete all Child Objects" permission for your logon account to the following objects:

To resolve an MSMQ installation failure:

1. Verify that you are logged in to the Active Directory domain with an account that has Administrator privileges.
2. If the login account has the correct privileges, perform the following steps to rebuild the computer objects:
   a. Remove the machine from the domain and assign it to a workgroup.
   b. Restart the machine.
   c. Remove the machine from the domain controller.
   d. Reassign the machine to the domain.
   e. Restart the machine.
3. If neither of these solutions work, consult the documentation for MSMQ provided by Microsoft.

Note:

According to Microsoft, this problem will be resolved in Service Pack 1 of Windows Server 2003. To resolve this issue, install Service Pack 1 when it becomes available.

Configuring SQL Server for Business Advocate

Business Advocate does not use Database Designer to create and configure the Advocate database. You must create and configure the Advocate database before you install the Business Advocate components.

To configure SQL Server for Business Advocate, perform the steps in the following sections:

- Creating a database for Business Advocate on page 313
- Creating the Nethome directory on page 313
- Configuring the SQL Server client on page 313
- Configuring a user to run Business Advocate services on page 314
- Configuring SQL Server for Thai (optional) on page 315

Creating a database for Business Advocate

With SQL Server Enterprise Manager, create a database with the properties in the following table.

Property	Value
Database name	advocate Note: You can use a different name if desired. However, Avaya recommends that you name this database "advocate" for easy identification.
Main schema size	10 MB or more
Log size	20 MB or more

Creating the Nethome directory

On the machine that will host the first Logical Resource Manager for Business Advocate, do the following:

1. Create a directory called “Nethome”.
2. Share the Nethome directory as `Nethome`.

Configuring the SQL Server client

On every machine that hosts one or more Business Advocate servers, do the following:

1. Install the SQL Server Client, Microsoft Data Access Component.
2. Upgrade each machine to the Microsoft Data Access Component 2.7.
3. Configure the Client to access the machine that hosts your Advocate databases with TCP/IP protocol, using the correct server port, as follows:
   a. Run the SQL Server Client Network Utility.

      If you installed the SQL Server Client in the default location, you can find the Client Network Utility in the following folder: `C:\WINNT\System32\cliconfg.exe`

b. On the **Alias** tab page, add an alias with the properties in the following table.

Property	Value
Server alias	Name of the machine that hosts SQL Server. **Note:** You can use a different name if desired. However, Avaya recommends that you use this naming convention for easy identification.
Network libraries	TCP/IP.
Server name	Name of the machine that hosts your Advocate database.
Dynamically determine port	Do not check this box.
Port number	Enter the port number that the client uses to communicate with the Advocate database.

Configuring a user to run Business Advocate services

Create and configure a user to run Business Advocate services:

1. In Active Directory, create a user for Business Advocate
2. Configure the Business Advocate user account with the following rights and permissions:
   - Read, write, and execute permissions to the Nethome network share.
   - Create, delete, and access permissions for MSMQ queues.
   - Send and receive rights for MSMQ events.
   - Logon as a service permissions on every machine that hosts Business Advocate servers.
   - Local administrative rights on every machine that hosts Business Advocate servers.

   For information about how to assign these rights and permissions to the user account, see the documentation provided by Microsoft.

Configuring SQL Server for Thai (optional)

If you install Windows with an English CD-ROM, then configure for Thai, you must configure SQL Server to display the Thai characters. If you do not configure SQL Server correctly:

- Business Advocate Supervisor displays Thai characters as question marks when creating qualifiers.
- Avaya OA events for updating qualifiers do not function correctly.

Important:
You must configure Windows for Thai before you install the SQL Server database. For more information, see Configuring Windows for Thai (optional) on page 311. You must configure SQL Server for Thai before you install Business Advocate.

To retrieve and display Thai characters correctly for SQL Server on an English version of Windows:

1. Open Enterprise Manager for SQL Server.
2. Verify that the value of the Collation parameter is Thai:
   a. Right-click on the Advocate database and select **Properties**.
   b. On the **General** tab, confirm that the value of the Collation name field in the **Maintenance** group is Thai.

   After you complete this configuration, you can install Avaya IC and Business Advocate components.

Configuring Oracle for Business Advocate

Business Advocate supports Oracle 8.1.7 and Oracle 9.2.0 on Windows and Solaris. The steps to configure both versions of Oracle are almost identical. The only difference is that you do not have to disable NTS authentication for Oracle 9.2.0.

If your Avaya IC system includes Business Advocate and an Oracle database, do the following steps:

- Location of Oracle components for Business Advocate on page 316
- Creating tablespaces for the Business Advocate database on page 316
- Creating Oracle users for Business Advocate on page 317
- Disabling NTS authentication on page 318

- Installing the Oracle Client on page 319
- Completing the Net8 configuration on page 319

Location of Oracle components for Business Advocate

The following table shows which Oracle components you need to install for Business Advocate. For more information, see the documentation provided with your Oracle database software.

Machine	Required Oracle components
Machine that hosts your Business Advocate database	Install the following components: • Supported operating system: - Windows 2000 Server SP4 with recent updates and MDAC 2.7 - Windows Server 2003 with recent updates and MDAC 2.7 - Solaris 8 with all required patches - Solaris 9 with all required patches • Supported Oracle database: - Oracle Enterprise Server 8.1.7 with all required patches - Oracle Enterprise Server 9.2.0 with all required patches
On every machine that hosts a Resource Manager server	Install the Oracle Client with all required patches.

Creating tablespaces for the Business Advocate database

You must create a tablespace for every machine that hosts Business Advocate servers. Create these tablespaces on the machine that hosts your Business Advocate database.

To create a tablespace:

1. Open the Oracle DBA Studio standalone.

2. Create a tablespace with the properties described in the following table.

Window	Property	Recommended value
Database Connection Information	Username	internal
	Password	oracle
	Connect as	SYSOPER
General tab of Create Tablespace	Name	Enter a name for the tablespace. For example, enter ADVOCATETBS.
	Drive used for directory	E If possible, use drive E for the Business Advocate tablespace, and use drive D for the system tablespace. This configuration reduces the I/O burden on the drive for the system tablespace.
	Size	Enter an appropriate size. The minimum tablespace size is 100 MB.

Creating Oracle users for Business Advocate

You must create a unique Oracle user for every Logical Resource Manager in the Business Advocate system. Create these Oracle users on the machine that hosts the Business Advocate database.

Important:
To ensure that Business Advocate can create the schema in Oracle, the user name must start with a letter, and can contain only letters, digits, and underscore characters

To create an Oracle user:

1. Open the Oracle DBA Studio standalone.

2. Create a user with the properties described in the following table.

Window	Property	Recommended value
General tab of Create User	Name	Enter a name for the user. For example, enter advocate. **Caution:** To ensure that Business Advocate can create the schema in Oracle, the user name must: • Start with a letter. • Contain only letters, digits, and underscore characters
	Password	Enter a password for the user. For example, enter advocatepw.
	Confirm	Re-enter the password.
	Tablespaces Default	Enter the name of the Business Advocate database. For example, enter ADVOCATEDB.
Role tab of Create User	Available roles	Select the following role and move to the **Granted** column: • DBA
System Privileges tab of Create User	Available system privileges	Select the following system privilege and move to the **Granted** column: • UNLIMITED TABLESPACE

Disabling NTS authentication

CAUTION:

For all systems that include Oracle 8.1.7, you must disable NTS authentication on all machines that host the Business Advocate servers and the Business Advocate database.

You do not need to perform this step if the Business Advocate database is hosted on Oracle 9.2.0.

To disable NTS authentication:

1. Open the sqlnet.ora file.

   If you installed Oracle in the default directory, you can find this file in the following location: `..\oracle\ora81\network\admin\sqlnet.ora`

2. Confirm that the file includes the following setting, which disables NTS authentication:

   ```
   SQLNET.AUTHENTICATION_SERVICES = (NONE)
   ```

   Add this setting to the file, if it does not already exist.

Installing the Oracle Client

When you install the Oracle Client, install the Oracle ODBC connector on the machine that hosts your Oracle database server.

Important:
Do not install the Microsoft Oracle ODBC connector.

Completing the Net8 configuration

After you install the Oracle Client, the Oracle Universal Installer automatically runs the Net8 Configuration Assistant.

To complete the Net8 configuration:

1. Complete the windows in the Net8 Configuration Assistant with the properties described in the following table.

Window and property	Recommended value
Welcome	Confirm that **Perform typical configuration** is not selected.
Directory Service Access	Select **No, I want to defer directory service access configuration to another time**.
Naming Methods Configuration, Select Naming Methods	Verify that **Local** is the only selected naming method.
Net Service Name Configuration, Database Version	Select **Oracle8i database or service**.
Net Service Name Configuration, Service Name	For **Service Name**, type the Oracle SID value.
Net Service Name Configuration, Select Protocol	Verify that **TCP** is the only selected network protocol.

Window and property	Recommended value
Net Service Name Configuration, TCP/IP Protocol	Do the following: ● For **Host Name**, type the host name of the machine that hosts the Oracle Enterprise Server. ● Verify that the standard port number of 1521 is selected.
Net Service Name Configuration, Net Service Name	For **Net Service Name**, type the Oracle SID value.

2. After you complete the Net8 Configuration Assistant, exit the Oracle Universal Installer.

Appendix A: Switch administration

This appendix provides configuration and administration information for each of the switches supported by the Avaya Telephony server (TS) in IC 7.0.

This section includes the following topics:

- Avaya Communication Manager administration on page 322
- Aspect CallCenter administration on page 357
- Meridian-1 administration: Symposium Server on page 389
- Meridian-1 administration: Meridian Link on page 398
- Ericsson MD110 Administration on page 405

Important:
To display the calling party's number on the Softphone when an agent receives a call, the switch must be configured to provide an ANI. If there is no ANI, the Softphone displays the agent ID.

Avaya Communication Manager administration

This section describes how to configure the Avaya DEFINITY/Communication Manager for use with the Avaya TS. Refer to the appropriate Avaya DEFINITY documentation for more details on administering the switch to accommodate the goals of this section.

Avaya IC supports the RONA (Redirect on No Answer) switch feature that redirects calls sent to an agent that are not answered by that agent. The agent must be configured on the switch for RONA. Refer to the administration documentation for your switch for RONA configuration instructions.

Important:

The Avaya DEFINITY/Communication Manager switch sends the default reason code value 0 when it puts an agent on AUX work when a switch generated RONA occurs. This precludes the Avaya Agent from issuing a TS.BusyWithReason because the agent has already been placed into AUX work by the switch.

Configuration for IC 7.0

The Avaya DEFINITY/Communication Manager must be configured with a license file that activates the Call Center Deluxe features. Call Center Deluxe activates Call Vectoring (Basic), Call Vectoring (Prompting), etc., and the Call Center Elite package (provides Expert Agent Selection “skills”, Reason Codes, etc.), Computer Telephony Adjunct Links (in addition to ASAI Link Core and ASAI Link Plus Capabilities) and Agent States.

The Co-Res DEFINITY LAN Gateway is required for the Avaya S8100 or S8300 Media Servers. IC can interface with Communication Manager 3.x in two ways: via a MAPD with CVLAN software or via a C-LAN board and a separate server running AEServices 3.0. The ASAI links must be configured either as ADJLK (for MAPD connectivity) or ADJ-IP (for co-resident DLG or C-LAN connectivity). The ASAI links must also have IC Adjunct Routing active (with Communication Manager 1.2 or later configured on the CTI Link form) to support multiple announcement/wait/loop back goto commands following the adjunct routing command.

Important:

When the switch administrator makes a change to be sent to an agent's station on the switch while that agent is being monitored by the TS, the TS receives a C_PROV_ABT packet with a cause value of 19. When the TS receives this event, it assumes the CTI Link is down and the TS shuts itself down.

Do not make changes that cause a C_PROV_ABT packet with a cause value of 19 to an agent's station on the switch while the agent is being monitored by the TS.

Best Services Routing (BSR) option

If you are using the Best Services Routing (BSR) option on your Avaya DEFINITY switch to transfer IC related calls, you must ensure that you have ISDN trunk lines configured between each switch and that you are passing UUI (User to User Information) on the D Channel to the remote switch. Avaya IC uses the UUI field to send and receive the EDUID of the call at each endpoint.

Refer to Chapter 10 in the *Telephony Connectors Programmer Guide* for more information.

For more information about Best Services Routing, see *DEFINITY ECS Vectoring/EAS Guide (555-230-521)*.

Timed ACW

Timed After Call Work (TimedACW) is a switch based feature supported by the Avaya Agent on the Avaya DEFINITY/Communication Manager switch. With TimedACW, when an ACD call or queue is disconnected, the agent is placed into Wrapup (After Call Work) for a pre-defined period of time, which is configured on the switch. Once this period of time elapses, the agent is made available to receive the next call. TimedACW requires agents to use Auto-In functionality, not Manual-In.

Support Limitations

Given the complexity of Avaya Agent, there are limitations to Timed ACW support, which are listed on the following table:

Not supported with...	Not supported when...	Call types are...
Avaya Agent Wrapup	PBX TimedACW set to FALSE on the switch.	Outbound calls
Selective Wraup (customized by PSO)	Client TimedACW set to Y in the VTel.ini file.	Direct calls dialed by equipment
VTel standalone	Client Wrapup property in IC Manager set to TRUE.	Calls that are conferenced or transferred
Agent events turned off at the switch	-	Calls that are received by an agent that were previously RONA'd
-	-	RONA or RONA'd calls
-	-	Abandoned calls

Call vectoring adjunct routing request

Adjunct routing is the process by which an ACD informs the Avaya TS that a call has arrived and the Avaya TS informs the ACD that the call should be routed to a particular destination.

There are several steps involved in adjunct routing, as outlined below. Each step is explained more fully in the following sections.

1. Incoming call is identified by Dialed Number Identification Service (DNIS).
2. DNIS is mapped to a Vector Directory Number (VDN).
3. VDN identifies the vector to be executed.
4. Vector identifies the ASAI link to which the call is to be routed using an adjunct routing vector command.
5. Vector executes an adjunct route request on the ASAI link and waits for a return.
6. Avaya TS responds with a route select.

The following sections trace a call from its arrival at the switch to its eventual transfer to an agent.

Note:

The interaction of the Avaya TS and the Avaya DEFINITY/Communication Manager can be affected by many switch parameter settings that are not described in this chapter. For example, when configuring the switch for outbound dialing, you may have to set the “Answer Supervision by Call Class” parameter to Y. Refer to your Avaya DEFINITY documentation for a complete description of switch parameters.

Defining Vector Directory Numbers (VDNs)

When a call arrives at the switch, the DNIS (Dialed Number Identification Service) is mapped to a Vector Directory Number (VDN).

The VDN table associates each VDN with a vector (script) to be executed when a call arrives on that VDN. The following illustrates a VDN table. In this example, a call arriving on VDN 26001 would cause Vector 1 to be executed.

```
Allow VDN              Vec       Orig     Event     Skills
Ext Name               Override  COR TN   Num Meas  Annc   Notif Adj   1st

26001 route to ASAI    n         1   1    1    none
26002 Route to LAN     n         1   1    2    none
26003 Rt LAN thn ASAI  n         1   1    3    none
```

Defining vectors

Vectors are scripts that contain a series of steps to be executed when the vector is run.

The following illustrates the definition of vector 1 (which, following the previous example, is the vector executed when a call arrives on VDN 26001). In this example, vector 1 causes calls to be adjunct routed to a link defined by extension 24961.

Defining links via station extensions is different on Avaya DEFINITY before release 1.1 from Avaya Communication Manager release 1.1 or later. On versions prior to release 1.1, a station extension number is used to reference the ASAI link. On versions 1.1 or later, one or two digit link number is defined for each link.

- For information on defining link stations on Avaya Communication Manager before release 1.1, refer to Defining ASAI link station extensions (before 1.1) on page 327.
- For information on defining link numbers on Avaya Communication Manager on release 1.1 or later, refer to Defining link numbers (on 1.1 or later) on page 328.

The Avaya Communication Manager will execute step 02, and then will pause as specified below in step 3 until one of the following occurs:

- Avaya TS requests a route (response to route request). The Avaya Communication Manager would then leave the vector and make the route to an available agent or wait treatment VDN.
- More than 10 seconds pass. The Avaya DEFINITY/Communication Manager would then execute the next command in the vector, in this case, routing to the failover VDN defined by extension 24183.
- If the ASAI link is not operational, the Avaya DEFINITY/Communication Manager will automatically proceed to step 4 in the vector without waiting the 10 seconds.

```
CALL VECTOR

    Number: 1              Name VECTOR 1
Multimedia? n
     Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? y   ASAI
Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? n   CINFO? n   BSR? y  Holidays? y

01 wait-time 0 secs hearing ringback
02 adjunct     routing link 24961
03 wait-time 10 secs hearing ringback
04 route-to number 24183 with cov n if unconditionally
```

Step 01 starts ringback and introduces a slight delay to prevent timing issues.

Blind transfer

When an agent initiates a blind transfer to the queue of a second agent, the call is connected to the second agent but it is not disconnected from the first agent. The call goes into the Hold state.

This happens because the call was moved from the VDN before the call merge could be completed. When the call is moved from the VDN and when the call merge takes place are operations controlled by the switch.

To correct this problem, you need to allow for enough time for the call merge to be completed before starting the adjunct route. To accomplish this, set a "wait-time 1 sec" step at the start of the vector.

Defining ASAI link station extensions (before 1.1)

This section describes how to define ASAI link station extensions on a release version of Avaya Communication Manager prior to 1.1.

A station is any physical device, such as a teleset or telephony link, that has an extension number and has a physical connection to a port on a telephony card. This section describes how to define station extensions on systems running a version of an Avaya DEFINITY switch prior to Avaya Communication Manager 1.1.

For instructions on defining a link number on a system running Avaya Communication Manager 1.1 or later, refer to Defining link numbers (on 1.1 or later) on page 328.

The following List Station report illustrates a list of stations on an Avaya DEFINITY. In this example, the 8410D telephone sets are digital telephones, the 602A1 are CallMaster sets, the 8510T telesets are ISDN phones, the ASAI LINE 1 is the telephony link (physical) to the Avaya TS, and the ASAI LAN 01 is the LAN gateway which replaces the ASAI direct-connect link with an ethernet connection.

You must configure either an ASAI link or an ASAI LAN for an Avaya TS connection.

Following the example, calls routed to station 24961 are routed to ASAI link 1.

Ext	Port	Type	Data Name	Cv	COR/ Room	Ext	Pth	COS	Cable
24141	01A0803	8410D	STATION		24141			1	1
24142	01A0804	8410D	STATION		24142			1	1
24181	01A0801	602A1	AGENT		1			1	1
24182	01A0802	602A1	AGENT		2			1	1
24183	01A0402	8510T	STATION		24183			1	1
24184	01A0403	8510T	STATION		24184			1	1
24185	01A0805	602A1	Agent		5			1	1
24186	01A0806	602A1	Agent		6			1	1
24187	01A0807	602A1	Agent		7			1	1
24188	01A0808	602A1	Agent		8			1	1
24961	01A0401	ASAI	ASAI LINE		1			1	1
24962	01A1501	ASAI	ASAI LAN		01			1	1

Defining link numbers (on 1.1 or later)

This section describes how to define link numbers on a release version of Avaya Communication Manager of 1.1 or later.

A new CTI link form was added on Avaya Communication Manager 1.1 to define ASAI links. This new CTI link form replaces use of the "add station" form for assignment of station extensions to define ASAI links. This new form captures the same information that was administered on the station form for ASAI with the exception that a port number is no longer needed for a co-resident DLG link, an ADJ-IP link, or an ASAI-IP link. The port number is still required for a traditional ASAI link. When adding a link using this new form, a CTI link number is assigned. It is also necessary to enter an extension for the new link on the form.

The extension on the CTI link form is a station extension. An extension is still required because the switch architecture is based on extensions. Therefore, station extensions are used throughout the code for the internal ASAI implementation. However, externally on the SAT screens, ASAI links are referenced by their CTI link numbers. The CTI link number (between 1 and 16) is now used, instead of the ASAI extension, in the "adjunct routing link" vector step to define the link. Upgrades from an earlier release automatically add the new

CTI link form and move the existing ASAI link assignments to the CTI Link form and the station extension numbers are converted to link numbers in all references to ASAI links in existing vectors.

Each ASAI link for use with IC is defined using two pages. The following screens illustrate page 1 for different links.

For earlier DEFINITY CSI/SI/R and the S8700 Media Servers (link type ADJLK):

```
add cti-link next                                                Page   1 of 2
LINK
   CTI Link: 01
   Extension: 40001                                               BCC: 0
        Type: ADJLK                                                TN: 1
        Port: 1C0501                                              COR: 1
        Name: ADJLK CTI Link 1                                    COS: 1
                                          Hunt-to Station

   STATION OPTIONS
                Loss Group: 3


   BRI OPTIONS
                XID? y     Fixed TEI? n
         MIM Support? n
                         CRV Length: 2
```

For S8100 or S8300 Media Servers

```
add cti-link next                                                Page   1 of 2
LINK
   CTI Link: 01
   Extension: 40001                                               BCC: 0
        Type: AD-IP                                                TN: 1
                                                                  COR: 1
        Name: ADJLK CTI Link 1                                    COS: 1
                                          Hunt-to Station

   STATION OPTIONS
                Loss Group: 3
```

The following is assigned to page 2 for all types of links:

```
add cti-link next                                                Page   2 of 2
LINK
   FEATURE OPTIONS

        Event Minimization? n



                                    Special Character for Restricted Number? N
```

For Communication Manager 3.x (link type ADJ-IP):

```
add cti-link next                                                Page   1 of 2
                                CTI LINK
   CTI Link: 4
   Extension: 77004
        Type: ADJ-IP
                                                                  COR: 1
        Name: CM100 (7.0 CI Windows)




--- ADJLK link, p. 1 ---

add cti-link next                                                Page   1 of 2
                                CTI LINK
   CTI Link: 5
   Extension: 77005
        Type: ADJLK
        Port: 1C1105                                              COR: 1
        Name: CM101 (7.0 CI Windowx)

   BRI OPTIONS
                XID? n     Fixed TEI? y     TEI: 3
         MIM Support? n
                         CRV Length: 2

--- ADJLK, ADJ-IP link, p. 2 ---
```

The following is assigned to page 2 for all types of links:

```
add cti-link next                                                Page   2 of 2
                                CTI LINK
   FEATURE OPTIONS

        Event Minimization? n     Special Character for Restricted Number? N
        IC Adjunct Routing? y     Send Disconnect Event for Bridged Appearance? n
```

The following tables illustrates the valid link numbers for the various Avaya DEFINITY switch configurations:

Switch Configuration	Valid Link Numbers
Avaya DEFINITY One Release 5 and S8100	1 to 8
Avaya DEFINITY CSI	1 to 8
Avaya DEFINITY SI	1 to 8
Avaya DEFINITY R, S8700, and S8300	1 to 16

Involvement of the telephony server

Continuing with the above example:

1. The Avaya TS will be notified of a new call arrival and will request that an EDU be created by the EDU server.
2. The Avaya TS will pass the call to the Workflow server to determine the call's final destination.
3. The Workflow server will make a request of the Avaya TS (TS.Route) to route the call to a station or queue.
4. When the Avaya TS gets the request, it will send the commands to the Avaya DEFINITY/Communication Manager over the ASAI link to route the call.

Defining hunt and skill groups

The Avaya DEFINITY/Communication Manager supports two environments for defining agents and assigning them to queues: EAS (Expert Agent Selection) and non-EAS.

Both non-EAS and EAS has agents defined in hunt groups and the AAS parameter should be set to N (for no). The AAS setting is only used for IVR ports, not live agents.

With non-EAS, the hunt group is defined as an ACD split. In this case each agent is pre-assigned (when administered) to the hunt group (split) to which the agent will be a member. If an agent is to be a member of more than one split, the agent needs a separate set of work buttons for each of the splits because the agent must log into each split individually.

With EAS, the hunt group is defined as a skill and the agent becomes a member of the skill when they log in, not when they are administered. Each EAS agent has a LoginID form assigned, which list the skills they become members of when they log in. An agent only needs one set of work buttons because once the agent logs in, the system automatically makes them a member of all their assigned skills (hunt groups). The agent LoginID form also has an AAS field (for use as an IVR port), which also should be set to N (for no) for live agents.

In both an EAS and non-EAS environment, agents are defined in hunt groups. When agents log in, they must identify the queue with which they are associated. They are not affiliated with a specific skill. The Auto Available Split (AAS) parameter in the Hunt Group must be set to N (for no).

EAS agents are associated with skill groups. If a caller needs to speak with an agent that has a specific skill, such as understanding a foreign language or having knowledge of a specific procedure, the caller is routed to a queue associated with the required skill. The next available agent with the appropriate skill takes the call and IC Telephony is notified that the call was transferred to an agent.

Depending on your environment, you must identify agents by either skill groups or hunt groups.

Grp No.	Grp Ext.	Name	Grp Typ	ACD/ MEAS	Vec	MCH	Que Size	No. Mem	Cov Path	Notif/ Ctg Adj	Dom Ctrl	Message Center
1	24301	Skill	1	ucd	y/N	SK	none	5	0	n		n
2	24302	Skill	2	ucd	y/N	SK	none	5	0	n		n
16	24316	Skill	16	ucd	y/N	SK	none	5	0	n		n
17	24317	Skill	17	ucd	y/N	SK	none	5	0	n		n

Summary of adjunct routing requirements

The following summarizes the items that must be configured for adjunct routing to take place. Refer to Configuration for IC 7.0 on page 322 for more details.

1. Stations - phones connected and configured, ASAI Link or ASAI LAN gateway configured to a station extension. For MultiVantage 1.1 or later, a specific link number between 1 and 16.
2. Network DNIS mapped to a VDN on the switch.
3. VDN assigned to a vector number.
4. Vector script performing adjunct route to the ASAI ink extension or link number.
5. Agent logins defined with associated skills.
6. Skill queues (hunt groups) defined to route calls from Avaya Computer Telephony.
7. In the definition of the ASAI link, event minimization must be set to N.
8. To allow calls to be sent to an “agentid”, the “Direct Agent Calling” parameter of the “Class of Restriction” for both the sending and receiving parties (i.e., the Agent ID and the incoming VDN) must be set to “Y”. If not set to “Y” the call could be delivered to the agent as a personal call rather than an ACD call.

Note:

An agent's profile can be set to either Auto In mode or Manual In mode. This setting affects VTel's ability to control the agent's availability. Refer to the *VTel Programmer's Guide* for additional information on this setting.

Configuring MAPD CVLAN server software

You must configure the MAPD CVLAN server software to enable IC 7.0 special features over the adjunct link. Before you begin, ensure the link you intend to use is set as Adjunct Links on both the switch and on MAPD.

- Check the station type for each of the clients assigned to the switch. The station type must be set to ADJLK.
- Contact your switch administrator to determine if your MAPD is configured as Adjunct. If your MAPD is configured for ASAI only, contact Avaya Technical Support for assistance.

Once you determine the station types are set to ADJLK, you can configure MAPD. You must complete the following procedures in order to configure MAPD to enable special features on Avaya IC.

- Add the client(s) to the host table
- Assign the client(s) to a signal

To add a client in the Host Table:

1. Start the **Standard MAPD Interface** if it is not already running.
2. Select the **TCP-IP Administration** option at the **Main Menu**.
3. Select the **Local Host Table** option at the **TCP-IP Administration** screen.
4. Select **ADD** to display the **Host Table** screen where you can add new clients.
5. Enter the IP address and host name of the client where the TS is installed at the **Add Host** screen.
6. Select **ENTER** to add the client and return to the **Host Table** screen.
7. Repeat steps 4 through 6 for any additional clients you wish to add.
8. Select **CANCEL** to return to the **TCP-IP Administration** screen after adding all of the clients.
9. Select **EXIT** at the **TCP-IP Administration** screen to return to the **Main Menu**.

To assign a client to a signal:

1. Select the **Port Administration** option at the **Main Menu**.
2. Select the **CV/LAN Administration** option at the **Port Administration** screen.
3. Select the desired "signal" using the arrow keys.
4. Select **CLIENT** to display a list of clients assigned to that signal.
5. Select **ADD** to display the **Add Client** screen.
6. Type the client name or IP address of a client you added to the host table.
7. Select **ENTER** to display the **Clients for Node** screen with the client added.
8. Repeat steps 3 through 7 to assign additional clients to a signal.
9. Select **CANCEL** to return to the **CV/LAN Administration** screen after assigning all of the clients.
10. Select **CANCEL** at the **CV/LAN Administration** screen and again at the **Port Administration** screen to return to the **Main Menu**.
11. Select the appropriate option at the **Main Menu** to continue MAPD administration tasks or to exit and close the **Standard MAPD Interface**.

Configuring redundant CTI links

Installing two or more Avaya TSes allows for failover in the event of a malfunction of the server or ISDN line.

There are two approaches available for configuring redundant ASAI links:

- Configure each link to connect with a different physical computer, each with its own Avaya TS.
- Configure each link to connect with a single computer running multiple Avaya TS processes on that machine. (Remember to set the “Signal Number” configuration parameter to specify signal numbers for the ASAI links.)

Avaya DEFINITY/Communication Manager setup

Regardless of whether the primary and backup Avaya TSes are installed on either the same or different hardware, two separate VDNs and vectors are required in the Avaya DEFINITY or Communication Manager, one for each Avaya TS. The division of work between ASAI links (and thus servers) is determined by the number of calls that are processed by each vector.

The following illustrates vectors that are configured to fail over to alternate ASAI links and finally, if both links fail, to a default routing. If either Avaya TS is disabled or the ISDN connection is broken, subsequent calls to the corresponding vector are immediately channeled through the alternate ASAI link to the working Avaya TS. When the Avaya TS is re-enabled (or the ISDN connection is restored) subsequent calls to that vector are processed via their usual path with no operator intervention.

```
display vector 7
Page   1 of 2
CALL VECTOR

    Number: 7              Name Troy Link 1
Multimedia? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? y   CINFO? n   BSR? y  Holidays? y

01 wait-time  0 secs hearing ringback
02 adjunct    routing link extension 5100
03 wait-time  4 secs hearing ringback
04 adjunct    routing link extension 5113
05 wait-time  4 secs hearing ringback
06 route-to number 4000 if unconditionally

display vector 13
Page   1 of 2
CALL VECTOR

    Number: 13              Name Troy Link 2
Multimedia? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? n   BSR? y  Holidays? y

01 wait-time  0 secs hearing ringback
02 adjunct    routing link extension 5113
03 wait-time  4 secs hearing ringback
04 adjunct    routing link extension 5100
05 wait-time  4 secs hearing ringback
06 route-to number 4000 if unconditionally
```

The wait time (in steps 03 and 05 of the sample vectors) should be configured to allow adequate time for the adjunct route to process normally when the link is functioning properly. If the link fails because the physical link, the Avaya TS or the Workflow server fails, the vector will skip the “wait” and immediately execute the next step in the vector. The time-out will occur only if the link, Avaya TS and the Workflow server are up and assigned, but network traffic or database access is so slow that the route does not reach the switch in time.

Configuring the switch in an ACD environment

When configuring the switch for non-EAS agents, certain parameters must be set. Note that the default setting of these parameters, and even whether or not they are displayed, varies depending on whether the switch was ever set up for EAS use.

The following notes are specific to the menus displayed by the Avaya DEFINITY G3V6 or higher. The wording and location of these parameters may vary slightly for other versions.

1. Log on to the **Avaya DEFINITY** console using an account with appropriate security, such as the unit account.
2. Enter the **Change System Customer Options** command.
3. On page 3 of the menu, the BCMS/VuStats loginIDs parameter should be set to N and the EAS parameter must be set to N. Note that, in some circumstances, the BCMS parameter can be set to Y. The switch will display a message indicating if it must be changed.
4. Log off for the changes to take effect.
5. Log on again (using the init account is optional for the following command).
6. Enter the **Change System Parameter Features** command.
7. On page 7 of the menu, the **EAS Enabled** parameter must be set to **N**.
8. On page 8 of the menu, **Auxwork Reason Code** and **Logout Reason Code** must both be set to **None**.

When defining hunt groups, note that the Auto Available Split (AAS) parameter must be set to “N” and the skill for the hunt group (if this option is displayed) must also be set to “N”. Agent phone extensions must be included in the hunt group as group members.

Service Observing

Service Observing is an Avaya DEFINITY/Communication Manager feature that allows a specified user on Avaya IC (such as a customer service supervisor or a calling group supervisor) to observe the calls of another user (an agent) on Avaya IC. This gives the contact center the capability to ensure their customers are receiving quality service from their agents. Service Observing allows an observer with a hardphone to observe (listen to) calls at extensions within a Service Observing group. Observing means that the service observer can only listen and cannot be heard by either party on the call.

Important:
Avaya IC supports Service Observing activation through the hardphone only. The service observer must use a hardphone to observe the call of another user on Avaya IC.

The following scenario illustrates service observing on Avaya IC:

1. A call comes into the agent triggering a TS.IncomingCall and a TS.Connect event.
2. The recording application that is monitoring the station is notified about the service observing audio connection to this call with the TS.ObserverConnect event.
3. When the agent puts the call on hold, a TS.Hold event is triggered for the agent and a TS.ObserverDropped event is generated to the recording application, indicating that the audio connection is no longer active.
4. When the agent reconnects a held call, a TS.HoldReconnect event is triggered for the agent and a TS.ObserverConnect event is generated on the recording application, indicating that the audio connection is again active.
5. When the agent hangs up the call, a TS.ObserverDropped event is triggered for the agent and a TS.Disconnect is sent to the client application.

Predictive call properties

This section provides configuration information pertaining to the Predictive Dialing Kernel (PDK) functionality available to the Avaya DEFINITY/Communication Manager in IC 7.0. The following table describes the configuration parameters that must be set on the Avaya DEFINITY/Communication Manager to enable predictive (outbound) dialing functionality.

Parameter Name	Description
Predictive Route Point	Predictive Dialing uses Call Adjunct Routing also. The configuration of the Call Adjunct Routing for Predictive Dialing is very similar to the Call Adjunct Routing described above. There needs to be one VDN (Predictive Route Point) for this purpose. With Predictive Dialing, a DNIS is not mapped to this VDN. Other than that, the configuration for the VDN, and vector is the same as described. An ASAI station needs to be defined as an Adjunct Link.
Predictive Drop Point	Predictive Dialing needs a place to send calls that are to be dropped if specified to do so in the job configuration. This is done by routing the call to a VDN (Predictive Drop Point) that points to a vector with one step: 01 disconnect after announcement none.
Call Classified Card	The Call Classified Card is required and the use of the Call Classifier Card needs to be configured on the Telephony Services for Avaya DEFINITY. Refer to the Avaya DEFINITY/Communication Manager documentation for instructions.

Call Coverage

Call Coverage provides automatic redirection of calls to a designated destination (VDN or extension number) in a Call Coverage path. Call Coverage enables you to:

- Establish coverage paths with multiple answering options.
- Establish redirection criteria that govern when a call redirects.
- Redirect calls to a local switch station.

In Avaya IC 7.0, the following Call Coverage functions are supported on the Avaya DEFINITY/ Communication Manager switch:

- Coverage Path
- Call Forward All Calls (Call Forward/All)
- Call Forward Busy/Don’t Answer (Call Forward Busy/DA)

The Avaya DEFINITY/Communication Manager switch can be configured to leave a Bridged Call Appearance for the call following the Coverage Path or Call Forward. This option is not supported by Avaya IC because the Avaya TS does not support Bridged Call Appearance.

Important:
Call Coverage functionality is not supported on IC systems using Avaya Business Advocate. A conflict would exist because Advocate must control where the calls are routed and Call Coverage allows the switch to make call routing decisions.

Coverage Path

Coverage Path is a list of alternate answering options that are accessed, in sequence, when the dialed agent is not available to answer the call. Switch system administrators can configure Coverage Paths in one of the following ways:

- On stations (hardphones)
- By ACD Agent IDs (agent IDs)

The Coverage Path setup cannot be modified by agents.

The switch routes the call based on the configuration set for the Dialed Number (DN).

For example:

- If the hardphone extension number is dialed, the call follows the "station" call coverage information.
- If the dialed number is the agent ID (in an EAS environment), the call follows the "agent ID" call coverage information.

If the agent does not have a Coverage Path configured, direct agent calls are queued to the agent on the agent's primary queue with a higher priority than any other call.

Note:

If Coverage Path is routed to a VDN by the Workflow server, additional routing hints should be defined on the default routing queue (DefaultVoiceQueue@DefaultTenant) is used to route the call.

Call Forwarding

Call Forwarding allows agents to specify a destination to redirect calls when they are not available to take calls. These destinations can be either a VDN or an extension number. Call forwarding is set up by the agent before logging into Avaya IC.

Avaya IC 7.0 supports the following Call Forwarding functions:

- Call Forward All Calls (Call Forward/All) - Limited support
- Call Forward Busy/Don't Answer (Call Forward Busy/DA) - Limited support

With either of these Call Forwarding functions, the TS does not receive information from the switch until the call is answered and the agent does not see the Softphone ring.

Before logging into Avaya Agent, the agent must manually perform call forwarding on the hardphone to initiate call forwarding functionality for the session.

Call Forward All

Only hardphones can forward calls with the Call Forward/All (CFA) function. If an agent logs into a hardphone with Call Forward/All activated, calls made to that hardphone are automatically forwarded to the designated destination. The agent is not notified about these calls.

Calls made to the agent ID either:

- follow the agent configuration if the agent's Class of Restriction (COR) allows Direct Agent Calls (DAC).
- or are forwarded to the designated destination if the agent's COR does not allow DAC.

Limitation:

Calls made to the agent through the queue are delivered to the agent as usual.

Call Forward Busy/DA

Only hardphones can set the Call Forward Busy/DA (CFN B/A) function. The hardphone must be authorized to allow Call Forward Busy/DA in its Class of Service (COS) before it can be set up for Call Forward Busy/DA.

The following scenario illustrates a call to a hardphone with Call Forward Busy/DA:

1. The phone rings a number of times, based on the configuration setting in System-Parameters Coverage-Forwarding.
2. The call is re-routed to the designated call forward destination.
3. When the calls rings on the hardphone, the TS is not notified by the switch that the hardphone is ringing and one of the following occurs:
   a. If the call is not answered, the TS is unaware the call was ever there, so the Report server and OA do not report this step of the call.
   b. If the call is answered, the TS tries to "catch up" and send the appropriate alerting and connecting events to the client assigned to the hardphone.

Calls made to the agent ID follow the same rules as Call Forward All.

Calls that are made to the agent ID that are not allowed to receive DAC are forwarded to the call forwarding destination without ringing.

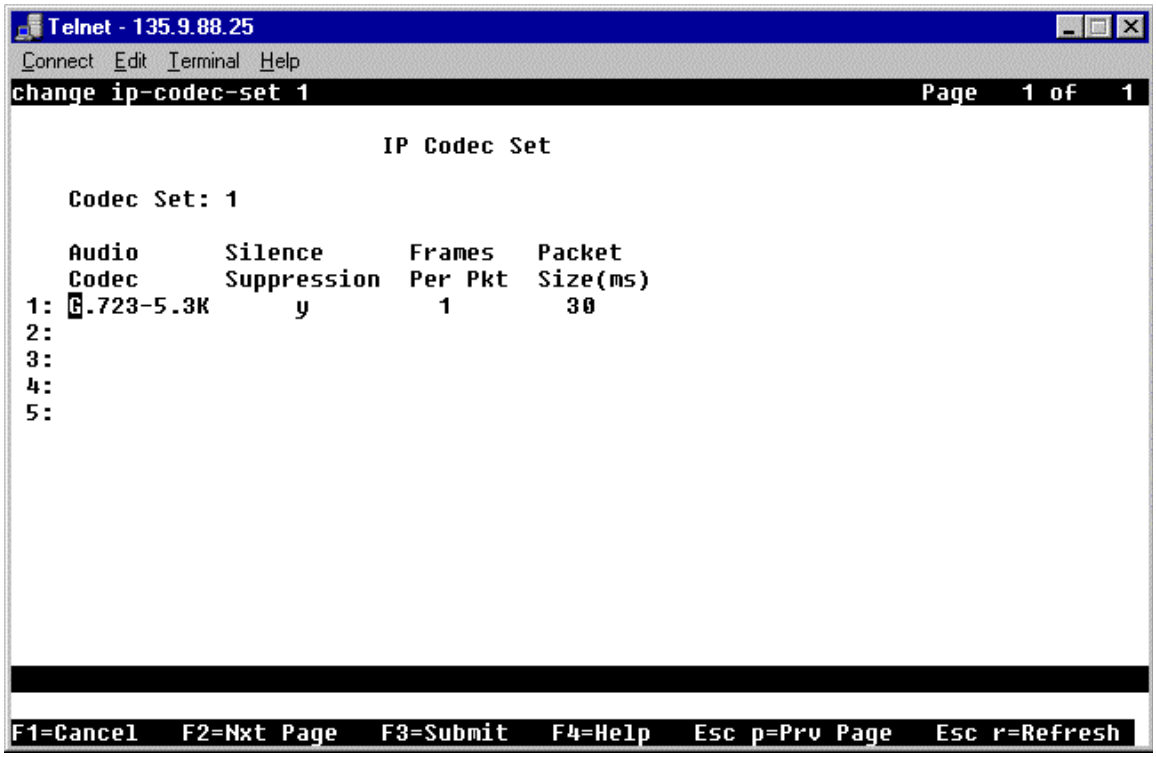
VoIP configuration

This section explains how to configure the Avaya DEFINITY/Communication Manager switch to enable the Voice channel to handle VoIP calls.

Define Codec Set

To define the Codec Set:

1. Type **change ip-codec-set 1** on the command line to open the **IP codec set 1** form.



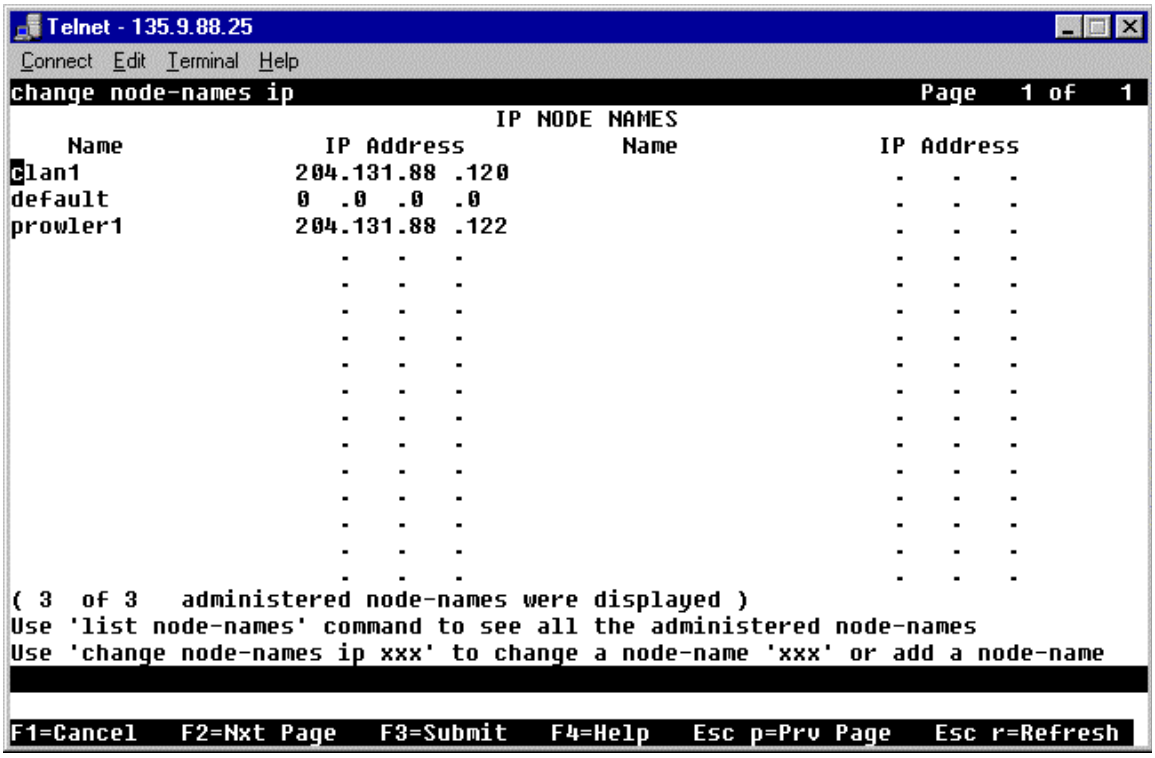
2. Type **G.723-5.3K** in the **Audio Codec** field.
3. Type **Y** in the **Silence Suppression** field.
4. Type **1** in the **Frames Per Pkt** field.
5. Type **30** in the **Packet Size(ms)** field.
6. Press **F3** to submit this form.

Assign node name

You need to add a node name for the C-LAN and Prowler circuit packs.

To assign the node name:

1. Type **change node-names ip** on the command line to open the **node names ip** form.

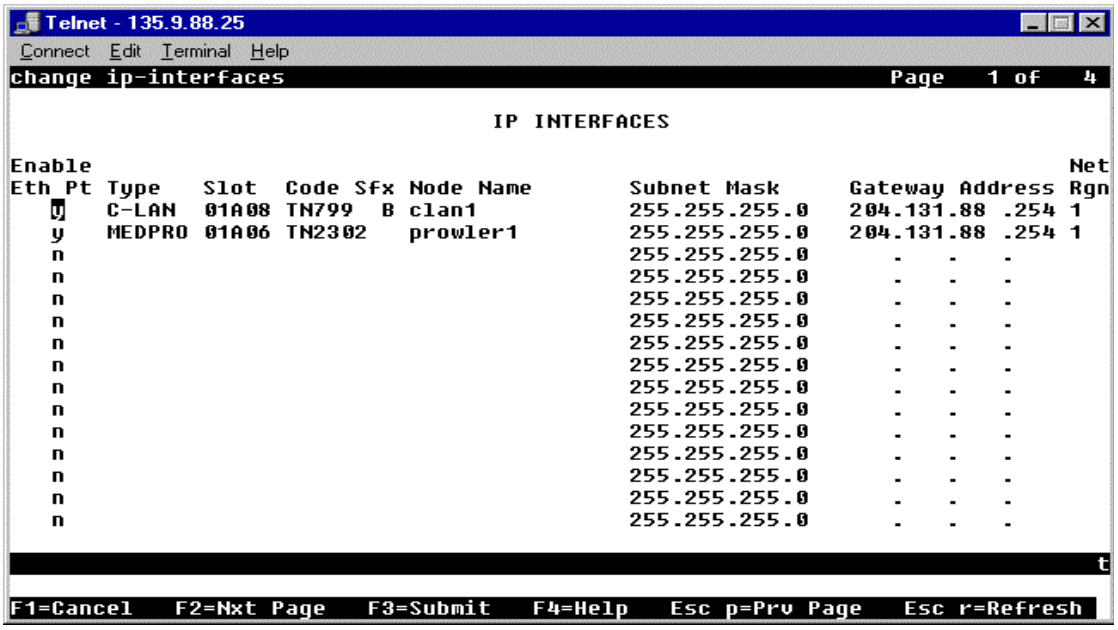


2. Type the unique name for each C-LAN and for each Prowler circuit pack in the **Name** field.
3. Type the unique IP address for each of the corresponding C-LAN and Prowler circuit packs in the **IP Address** field.
4. Press **F3** to submit this form.

Define the IP interface

To define the IP interface:

1. Type **change ip-interfaces** on the command line to open the **IP interfaces** form.



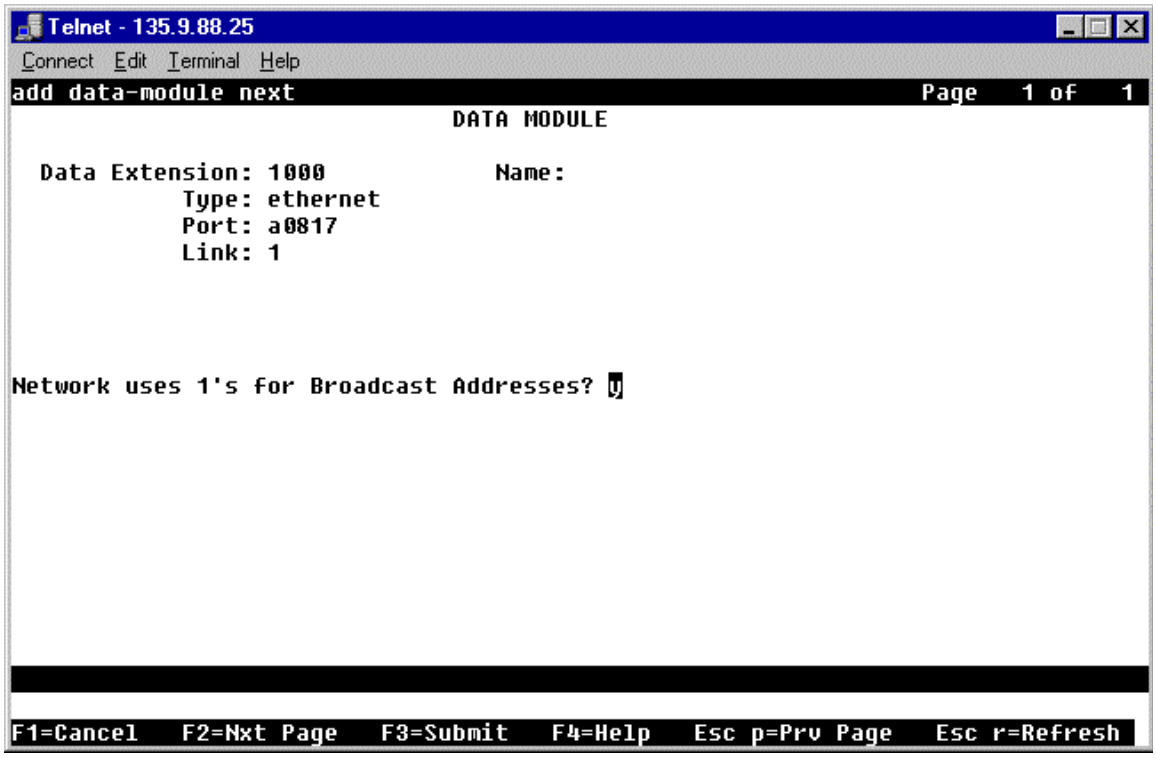
2. Type **y** in the **Enable Eth Pt** field.
3. Type **C-LAN** for the C-LAN circuit pack in the **Type** field.
4. Type the slot location for the C-LAN circuit pack in the **Slot** field.
5. Type the node name that you created for the C-LAN circuit pack in Assign node name on page 343 in the **Node Name** field.
6. Type the IP address of the gateway for the ip interface for the C-LAN circuit pack in the **Gateway Address** field.
7. Type **1** in the **Net Rgn** field for the C-LAN circuit pack.
8. Navigate to the next **Enable Eth Pt** field and type **y**.
9. Type **MEDPRO** for the Prowler circuit pack in the **Type** field.
10. Type the slot location for the Prowler circuit pack in the **Slot** field.
11. Type the node name that you created for the Prowler circuit pack in Assign node name on page 343 in the **Node Name** field.
12. Type the IP address of the gateway for the ip interface for the Prowler circuit pack in the **Gateway Address** field.
13. Type **1** in the **Net Rgn** field for the Prowler circuit pack.
14. Press **F3** to submit this form.

Assign a link to the LAN

You must assign a link to the LAN using the ethernet data module.

To assign a link to the LAN via the ethernet data module.

1. Type **add data-module next** on the command line to open the **data module** form.

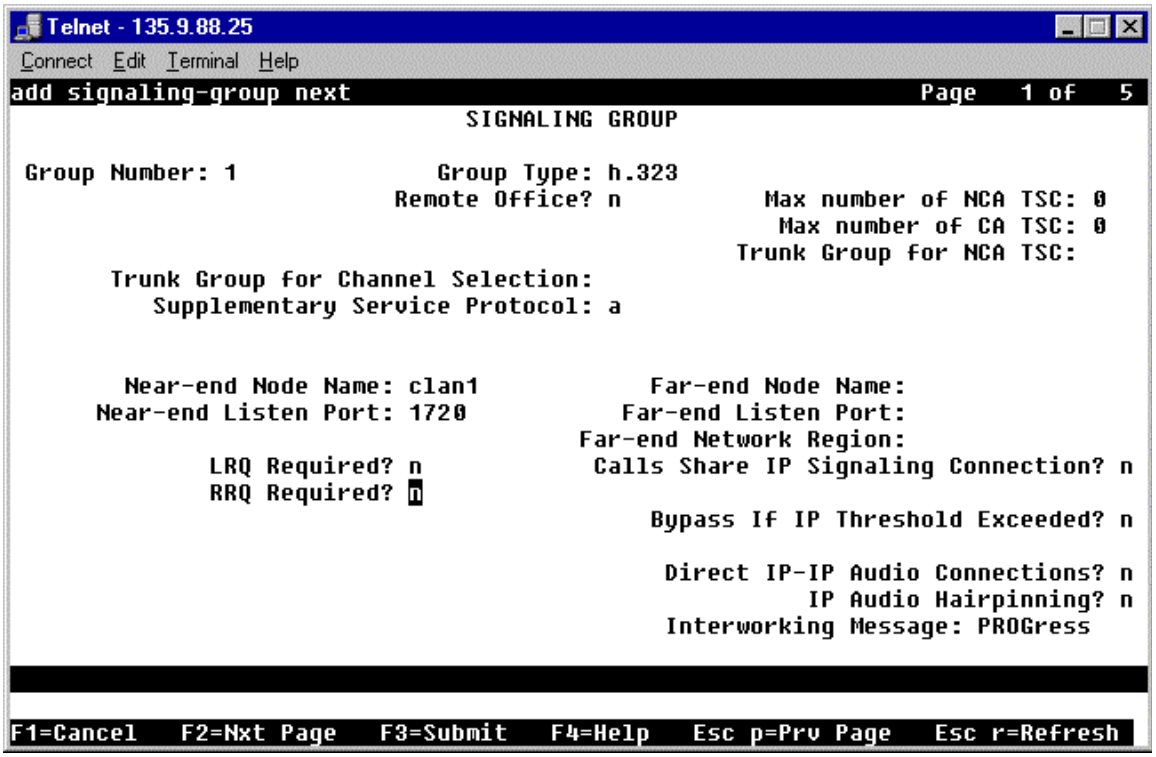


2. Type **Ethernet** in the **Type** field.
3. Type the port number to be used by the circuit pack in the **Port** field. Ethernet connections must be assigned to port 17 on the C-LAN circuit pack.
4. Type the link number to assign to the circuit pack in the **Link** field. Link numbers 1-25 not previously assigned on this switch.
5. Press **F3** to submit this form.

Create an IP signaling group

To create a signaling group:

1. Type **add signaling-group next** on the command line to open the **signaling group** form for the next available signaling group.

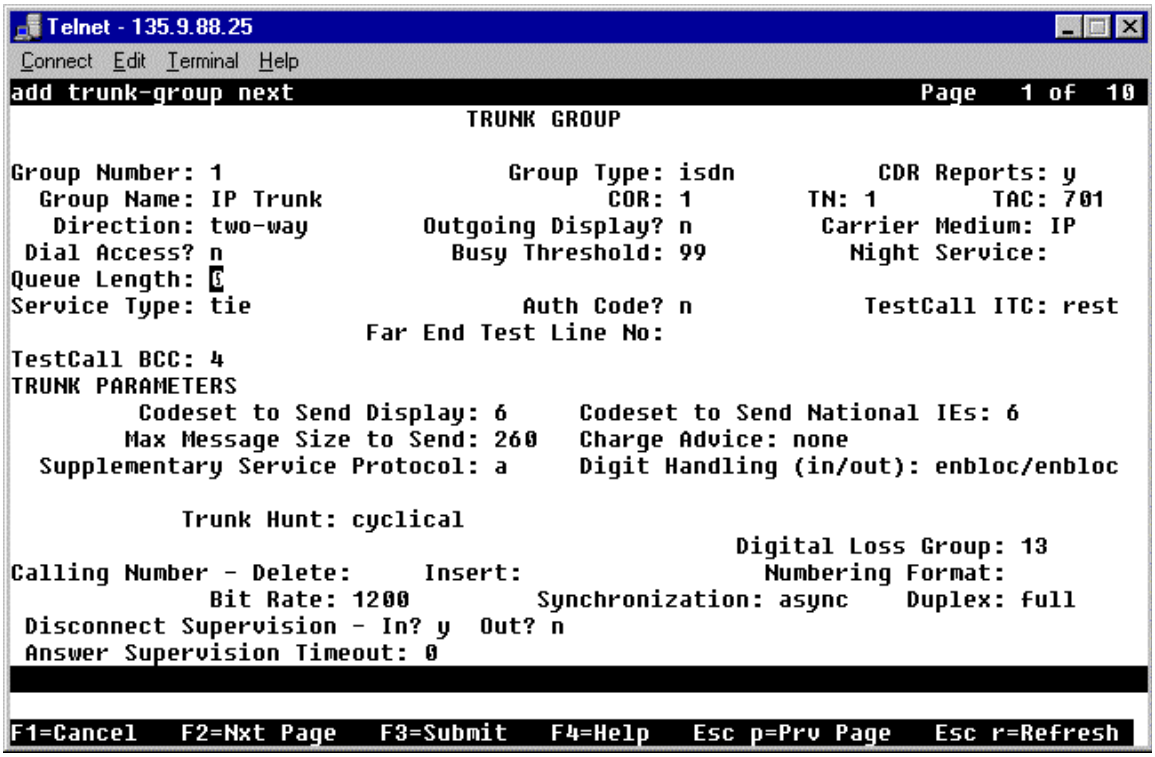


2. Type **h.323** in the **Group Type** field.
3. Leave the Trunk Group for Channel Selection field blank until you create a trunk group in the next task. Once you have created the trunk group, type change signaling group at the command line and enter the trunk group number in this field.
4. Type the node name that you created for the C-LAN IP interface in Assign node name on page 343 in the **Near-end Node Name** field.
5. Press **F3** to submit this form.

Create IP trunk group

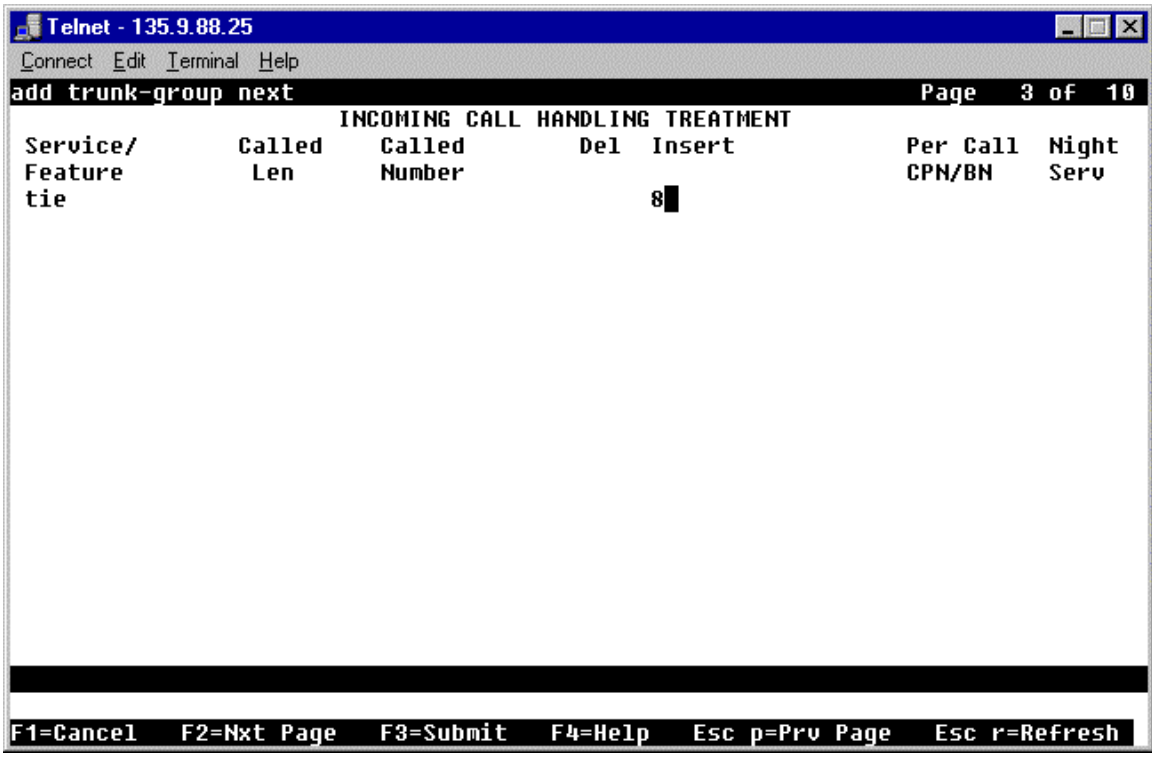
To create a trunk group:

1. Type **add trunk-group next** on the command line to open the **trunk group** form for the next available trunk group.



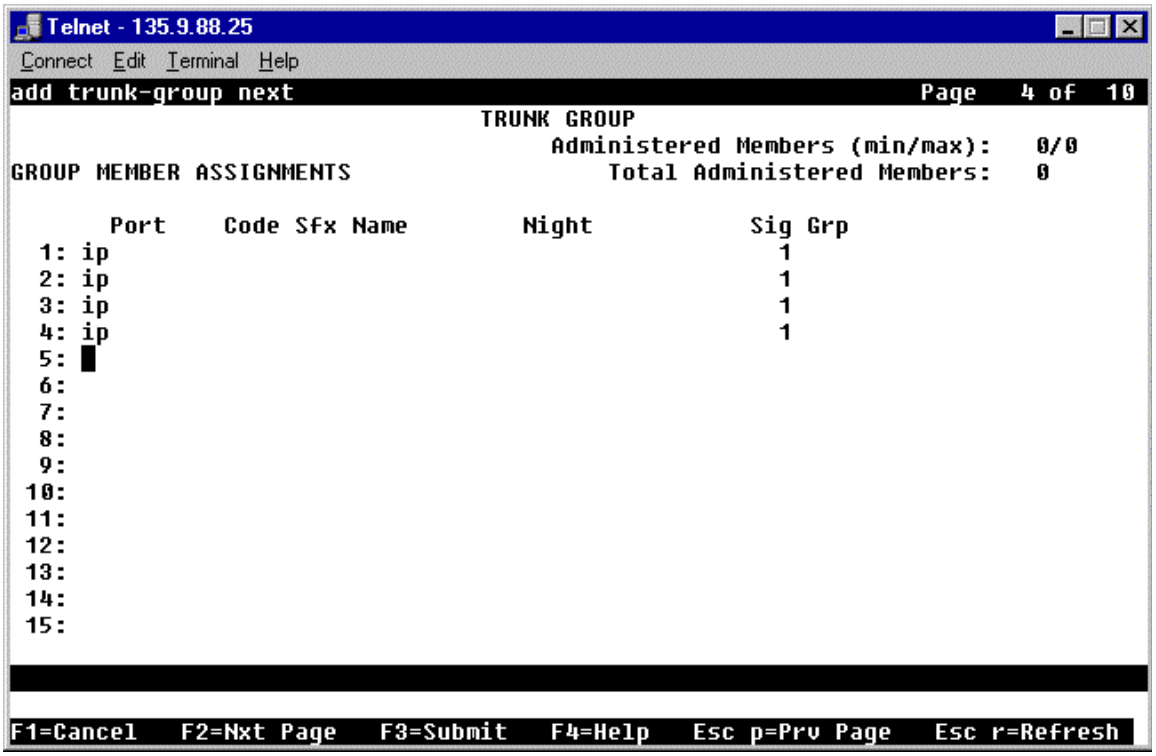
2. Type **IP Trunk** in the **Group Name** field.
3. Type **701** (the trunk access code) in the **TAC** field.
4. Type **IP** in the **Carrier Medium** field.
5. Type **Tie** in the **Service Type** field.

6. Press **F2** two times to display page 3 of this form.



7. Type **Tie** in the **Service Feature** field
8. Type **8** in the **Insert** field. This is the AAR feature access code to called number of all incoming calls on this trunk that forces them to go through AAR routing.

9. Press **F2** to display page 4 of this form.

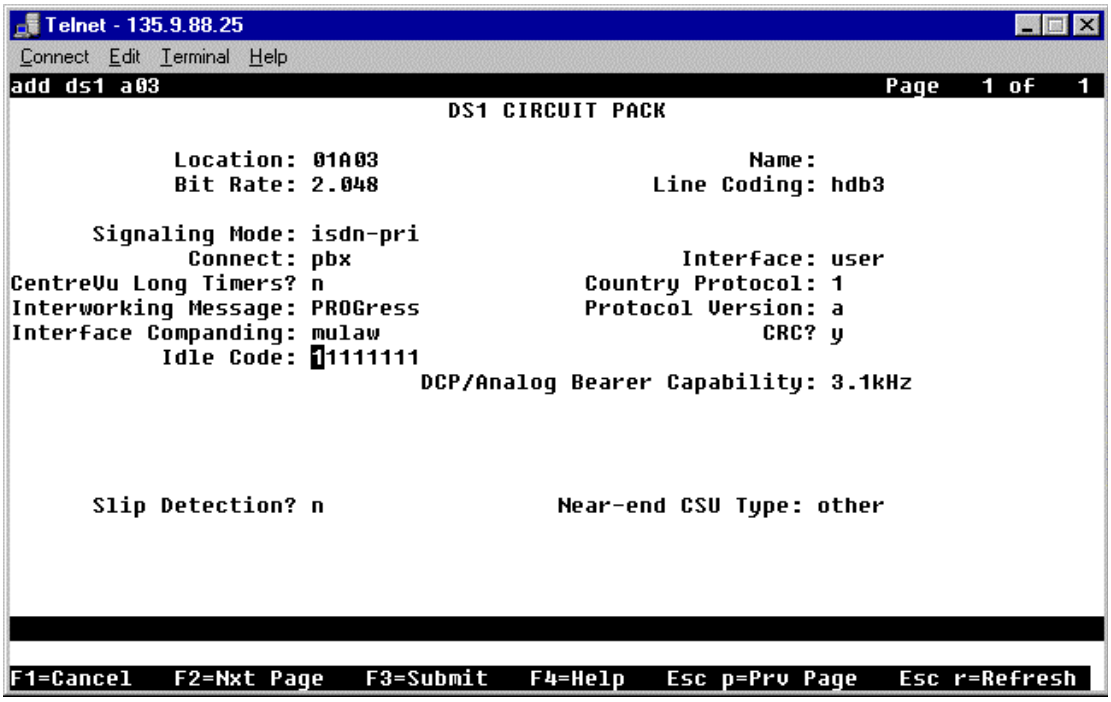


10. Enter **ip** in the **Port** field for this trunk. The maximum number of IP trunks for a signaling group is 31.
11. Enter the number of the signaling group from the previous task, Create an IP signaling group on page 346 in the **Sig Group** field.
12. Press **F3** to submit this form.

Create a DS1

A DS1 is only needed if the incoming VoIP call is not terminated on the switch and needs to be routed to a different switch.

1. To create a DS1:
2. Type **add ds1 a03** on the command line to open the **ds1** form.

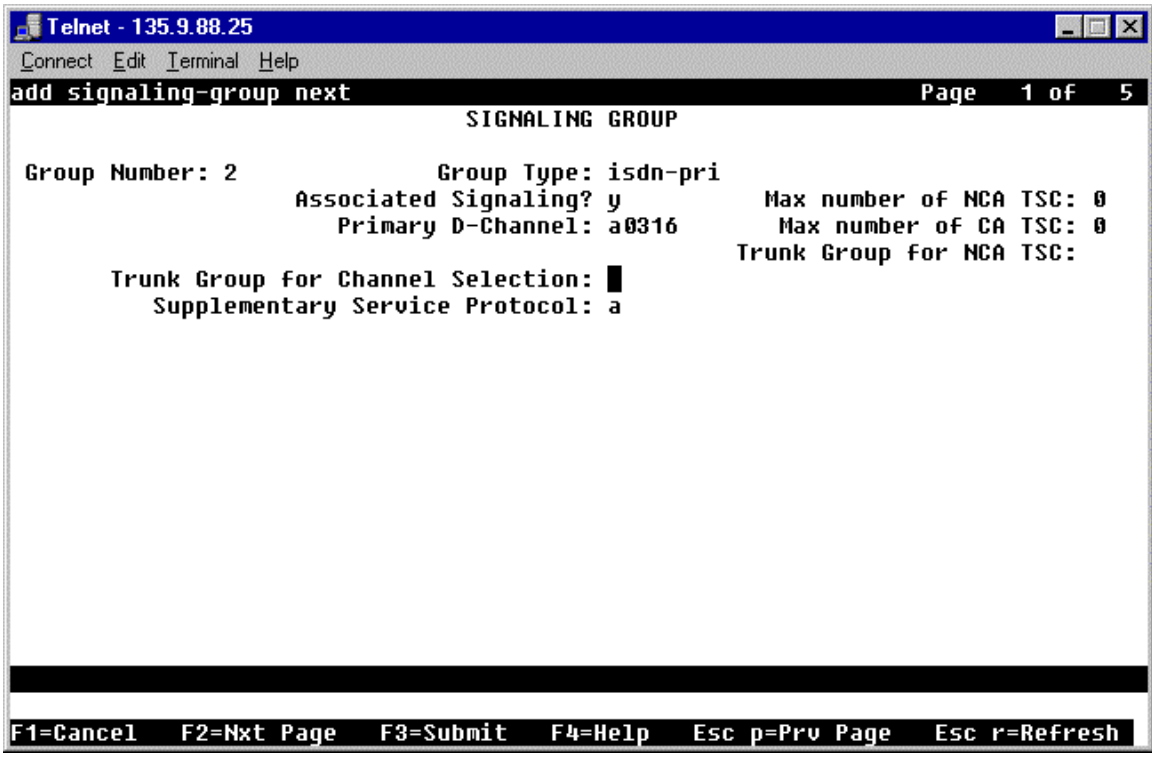


3. Enter one of the following in the **Bit Rate** field based on your system configuration:
   a. Enter **1.544** for a T1 connection.
   b. Enter **2.048** for an E1 connection.
4. Enter one of the following in the **Line Coding** field:
   a. Enter **b8zs** for a T1 connection.
   b. Enter **hdb3** for an E1 connection.
5. Enter **Isdn-pri** in the **Signaling Mode** field.
6. Enter **Pbx** in the **Connect** field.
7. Enter **User** in the **Interface** field.
8. Enter one of the following in the **CrC** field based on your system configuration:
   a. Enter **n** for a T1 connection.
   b. Enter **y** for an E1 connection.
9. Press **F3** to submit this form.

Create a PRI signaling group

A PRI signaling group is only needed if the incoming VoIP call is not terminated on the switch and needs to be routed to a different switch.To create a signaling group (PRI):

1. Type **add signaling-group next** on the command line to open the **signaling group** form for the next available signaling group.

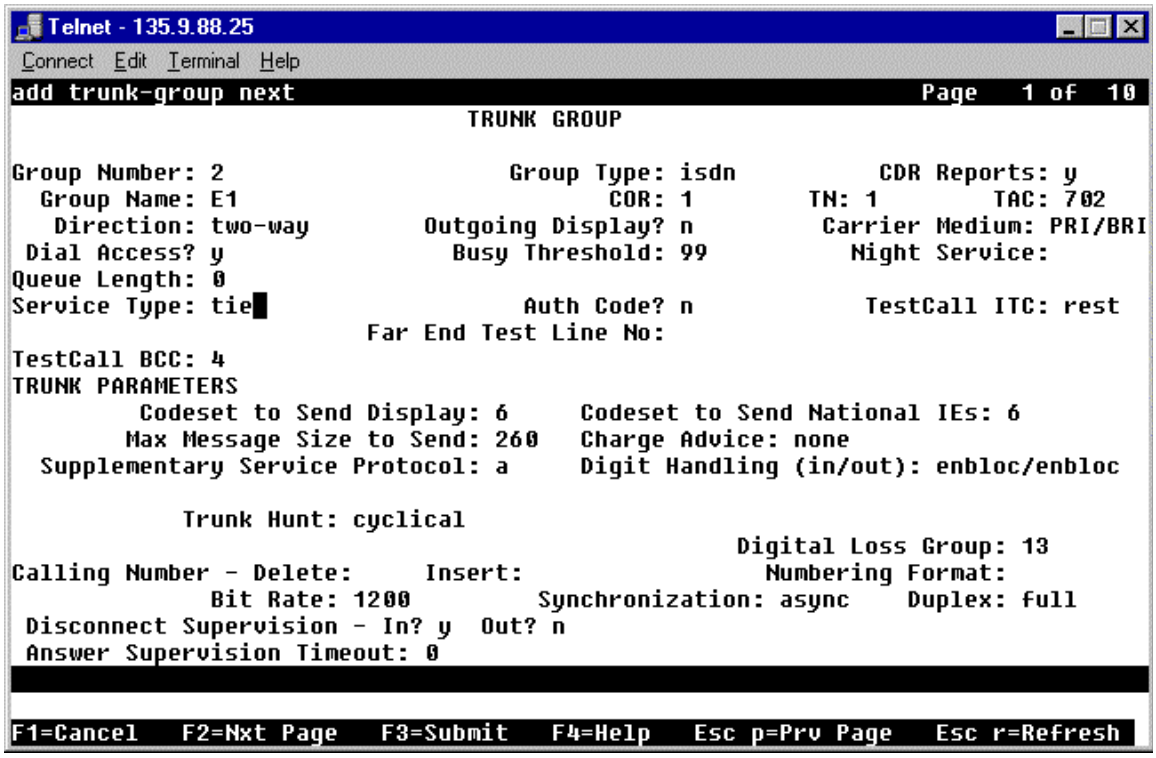


2. Enter **Isdn-pri** in the **Group Type** field.
3. Enter one of the following in the **Primary D-Channel** field based on your system configuration:
   a. Enter port **24** of the DS1 circuit pack for a T1 connection.
   b. Enter port **16** of the DS1 circuit pack for an E1 connection.
4. Leave the **Trunk Group for Channel Selection** field blank until you create a trunk group in the next task. Once you have created the trunk group, type change signaling group at the command line and enter the trunk group number in this field.
5. Press **F3** to submit this form.

Create a PRI trunk group

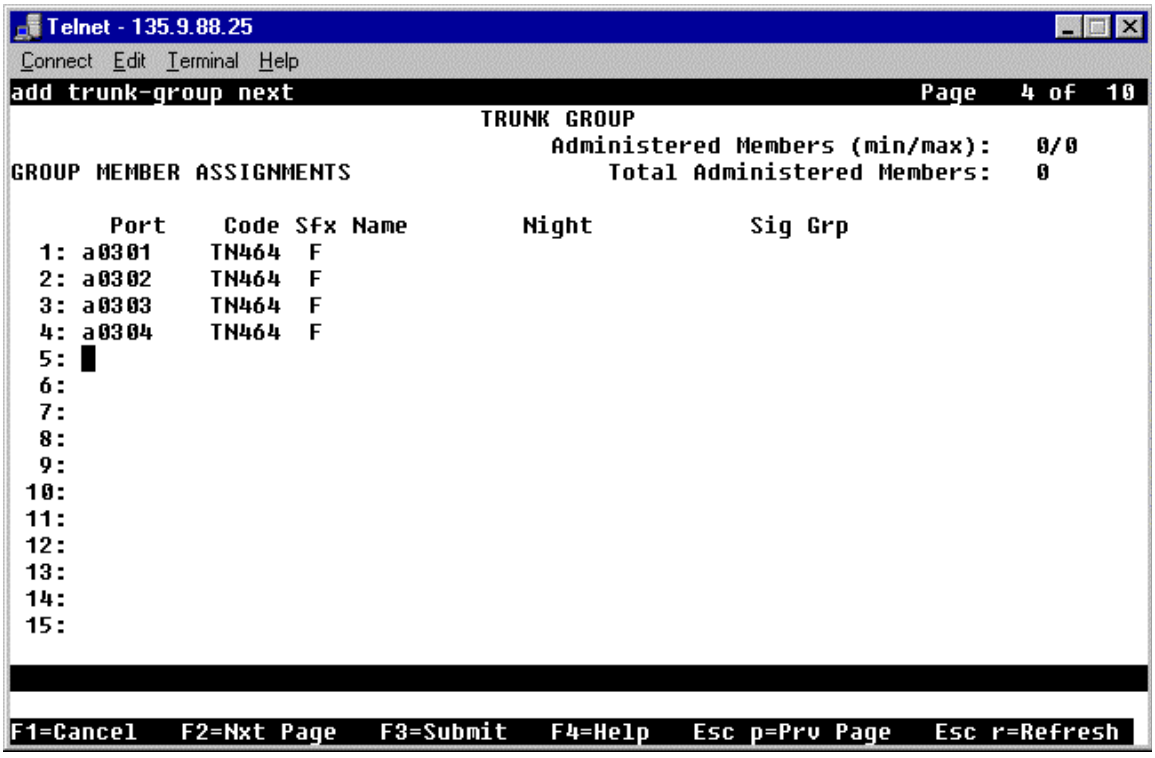
A PRI trunk group is only needed if the incoming VoIP call is not terminated on the switch and needs to be routed to a different switch.To create a trunk group (PRI):

1. Type **add trunk-group next** on the command line to open the **trunk group** form for the next available trunk group.



2. Enter one of the following in the **Group Name** field based on your system configuration:
   a. Enter **T1** for a T1 connection.
   b. Enter **E1** for an E1 connection.
3. Type **702** (the trunk access code) in the **TAC** field.
4. Enter one of the following in the **Carrier Medium** field based on your system configuration:
   a. Enter **PRI** for a T1 connection.
   b. Enter **BRI** for an E1 connection.
5. Type **Tie** in the **Service Type** field.

6. Press **F2** two times to display page 4 of this form.

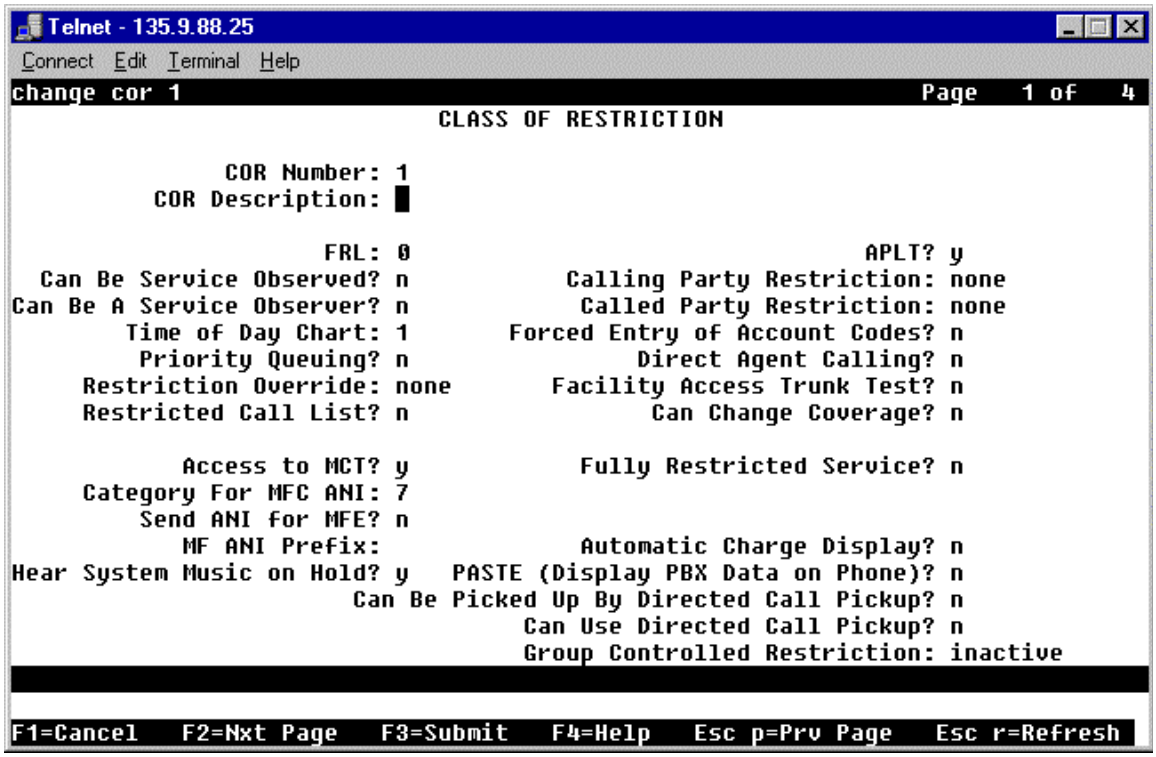


7. Enter the port number of the DS1 circuit pack in the **Port** field.
8. Enter the number of the signaling group from the previous task, Create a PRI signaling group on page 351 in the **Sig Group** field.
9. Press **F3** to submit this form.

Define the class of restriction

To define the class of restriction 1:

1. Type **change cor 1** at the command line to open the **cor 1** form which is used by all trunk groups.

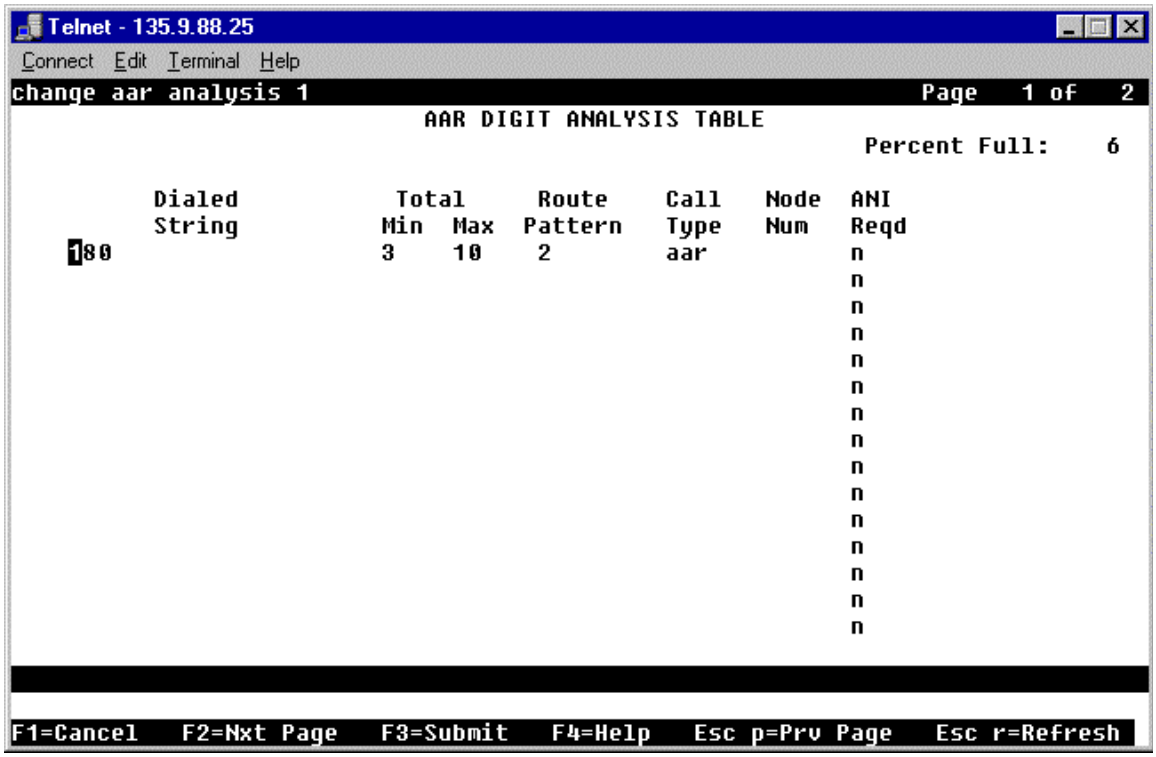


2. Enter **0** (zero) in the **FRL** field.
3. Enter **none** in the **Calling Party Restriction** field.
4. Enter **none** in the **Called Party Restriction** field.
5. Press **F3** to submit this form.

Define the AAR analysis

AAR analysis is only needed if the incoming VoIP call is not terminated on the switch and needs to be routed to a different switch.To define AAR analysis:

1. Type **change aar analysis** on the command line to open the **aar analysis** form.

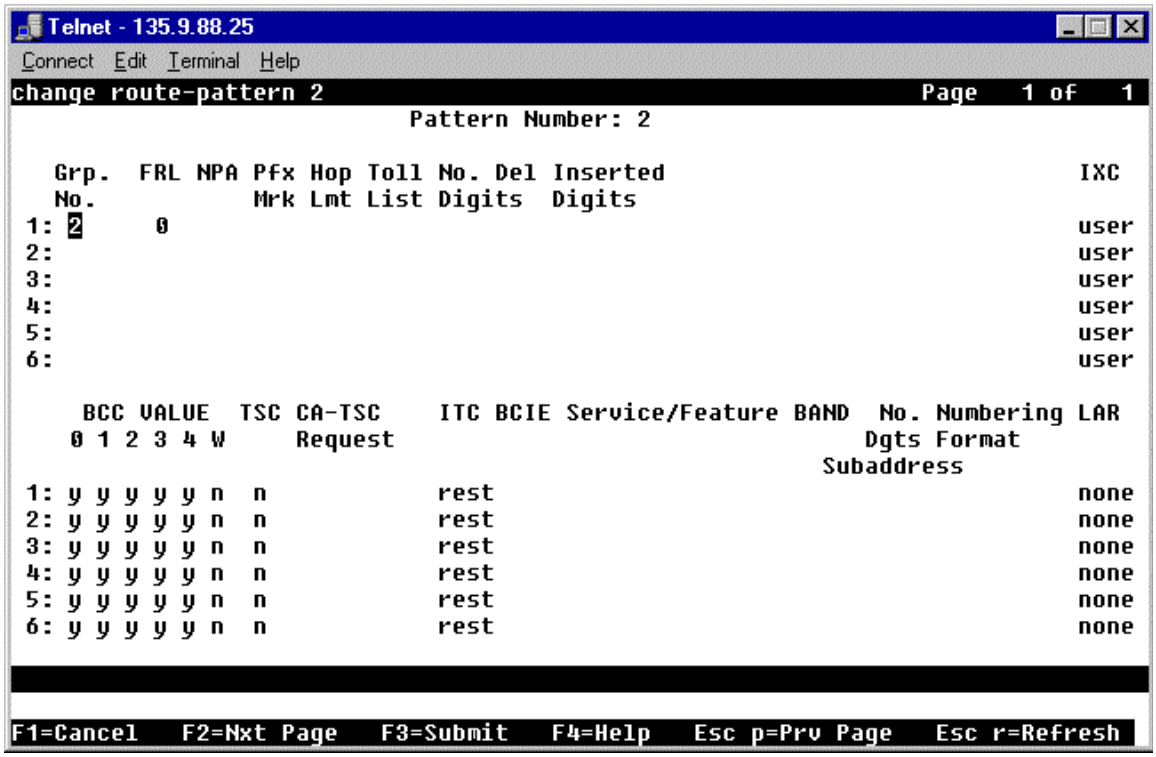


2. Enter the customer specific VDN in the **Dialed String** field.
3. Enter the length of the customer specific VDN in the **Total Min** field.
4. Enter the length of the customer specific VDN plus 7 (the length of the call ID) in the **Total Max** field.
5. Enter the route pattern that includes the ISDN-PRI trunk setup in the **Route Pattern** field.
6. Enter **aar** in the **Call Type** field.
7. Press **F3** to submit this form.

Define the routing pattern

A routing pattern is only needed if the incoming VoIP call is not terminated on the switch and needs to be routed to a different switch.To define the routing pattern:

1. Type **change route-pattern 2** on the command line to open the **route pattern** form.



2. Enter the ISDN-PRI trunk number in the **Grp. No.** field.
3. Enter **0** (zero) in the **FRL** field.
4. Press **F3** to submit this form.

Universal Call ID (UCID)

The Universal Call ID (UCID) is a unique 8-byte binary tag assigned by DEFINITY ECS MultiVantage to each call upon call origination or upon entry into DEFINITY, if the call is not already associated with a UCID. UCID allows tracking of calls from cradle to grave within a private network of DEFINITY systems when they are connected via ISDN trunks.

Products such as Call Management System (CMS), Avaya IVR, and CentreVu Computer Telephony support UCID. For more information on using UCID in custom applications, please refer to *CallVisor ASAI Protocol Reference.*

Aspect CallCenter administration

This section provides the configuration information required for the Aspect CallCenter switch to interface with the Avaya TS and the Avaya TSQS. Refer to the appropriate Aspect CallCenter System switch documentation for details on administering the switch to accommodate the goals of this section.

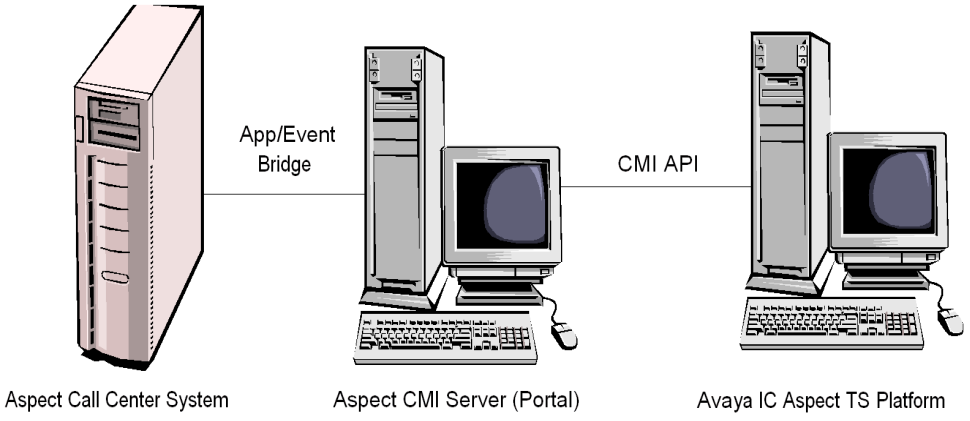
Perform these procedures in the following order:

1. Configure the Aspect CallCenter ACD
2. Configure the Aspect CMI server
3. Configure the Call Control Tables (CCTs)
4. Configure the Avaya Telephony server as described in *Telephony Server Programmer's Guide*.

Important:
The Aspect CallCenter System must have a DataInterlink directed at the machine where the Aspect CMI server is installed.

Aspect server topology

The following diagram illustrates the components that makeup the Aspect CallCenter System Topology including an Aspect CMI server component:



Configure Aspect CallCenter for the TS

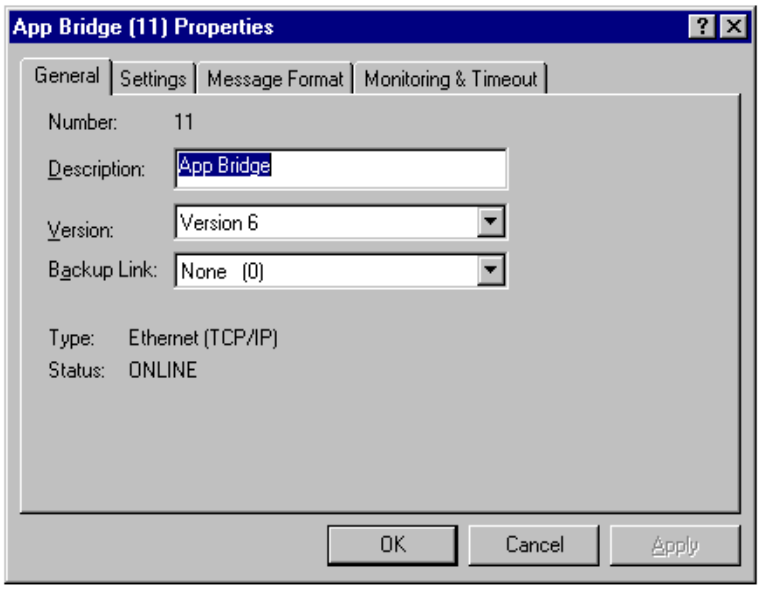
This section describes how to configure the Aspect CallCenter switch for the Avaya TS.

The Aspect CallCenter switch is configured from the App Bridge Properties feature in the Aspect CallCenter System Hardware Administrator. Access the App Bridge Properties dialog box using the instructions provided in the *Aspect CallCenter Administration Guide*.

General tab

Enter the following parameters at the **General** tab:

1. Enter **App Bridge** in the **Description** field.
2. Select the **Version 6** option from the drop down menu in the **Version** field.
3. Select the **None** (0) option from the drop down menu in the **Backup** Link field.

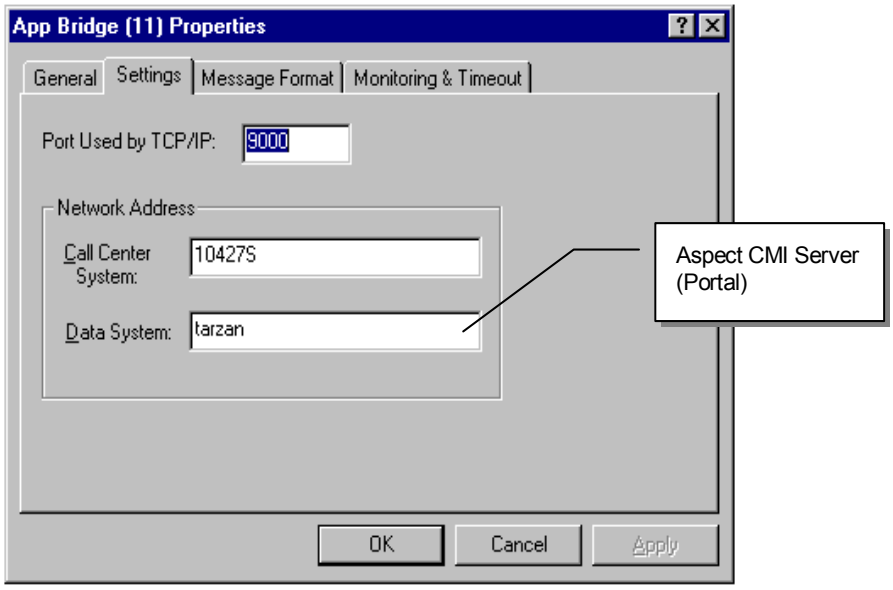


Settings tab

Enter the following parameters at the **Settings** tab:

1. Enter the port number, default is 9000, to be used by the TCP/IP connection in the **Port Used by TCP/IP** field.
2. Enter the call center system name in the **Call Center System** field.

3. Enter the name assigned to the Aspect CMI server (Portal) in the **Data System** field.

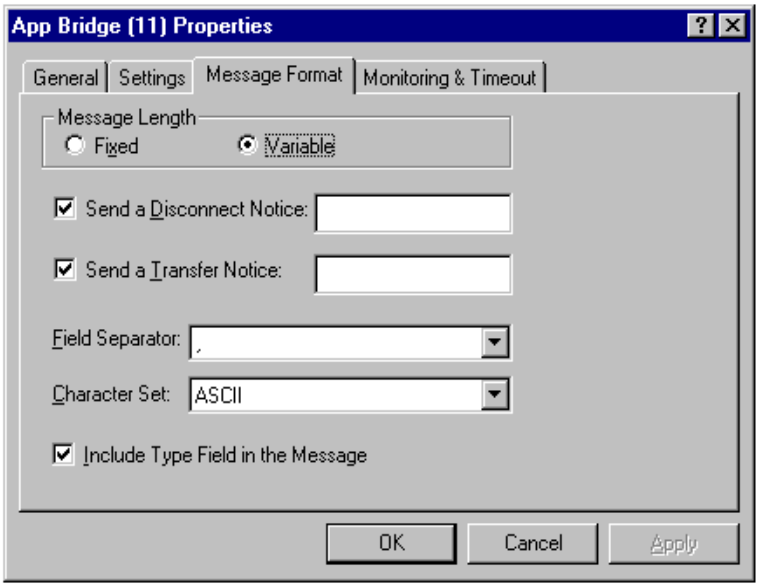


Message Format tab

Enter the following parameters at the **Message Format** tab.

1. Select the **Variable** option in the **Message Length** field.
2. Check the check box for the **Send a Disconnect Notice** field.
3. Check the check box for the **Send a Transfer Notice** field.
4. Leave the **Field Separator** field "," (comma) as it is.
5. Select the **ASCII** option in the **Character Set** field.

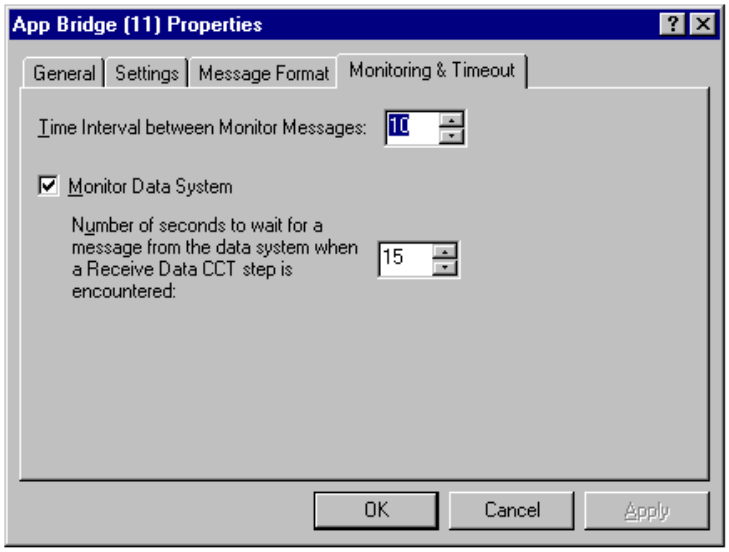
6. Check the check box for the **Include Type Field in the Message** field.



Monitoring & Timeout tab

Enter the following parameters at the **Monitoring & Timeout** tab.

1. Select **10** in the **Time Interval between Monitor Messages** field.
2. Check the check box for the **Monitor Data System** field.
3. Select **15** in the **Number of seconds to wait for a message from the data system when a Receive Data CCT step is encountered** field.

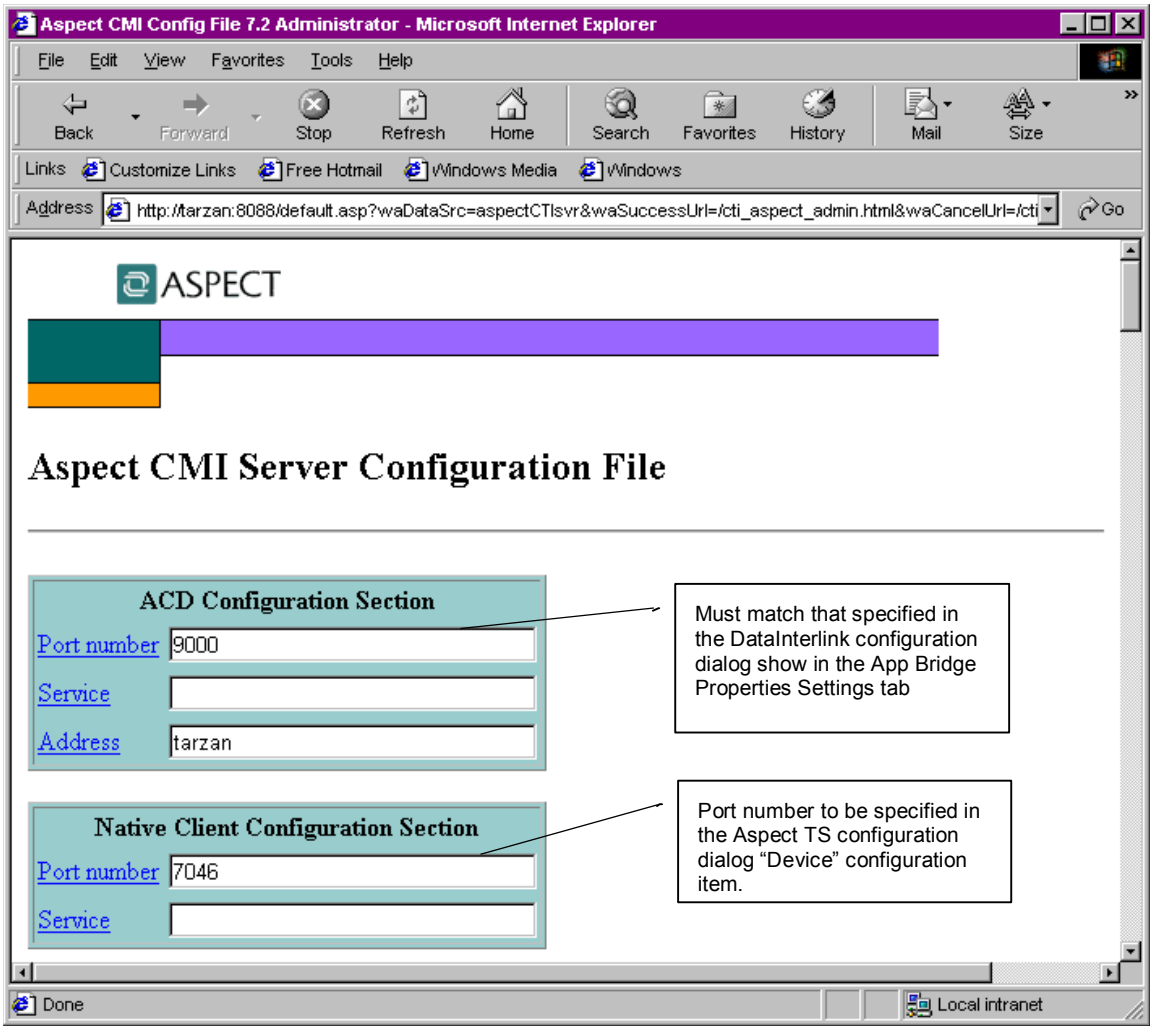


4. Click **OK** to save the settings and close the **App Bridge Properties** dialog box.

Configure the Aspect CMI server

This section describes how to configure the Aspect CMI server for the Avaya TS.

The following configuration parameters must be set on the Aspect CallCenter System to establish a connection with the Aspect CMI server.



Call control tables configuration

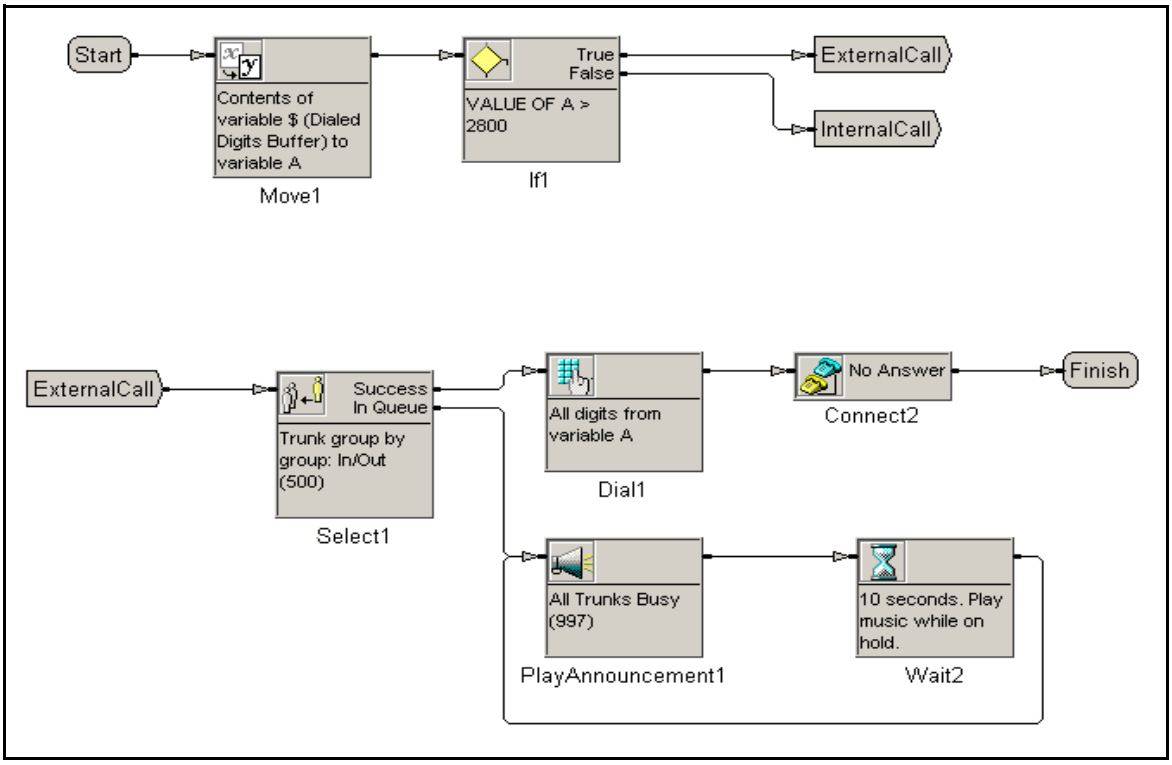
This section describes how to configure the following Call Control Tables (CCTs) that are needed to enable the Aspect TS and the Aspect CallCenter to work together.

- MakeCallCCT
- TransferInitCCT
- ExternalCCT
- RouteCCT
- BlindCCT
- AgentGroupCCT

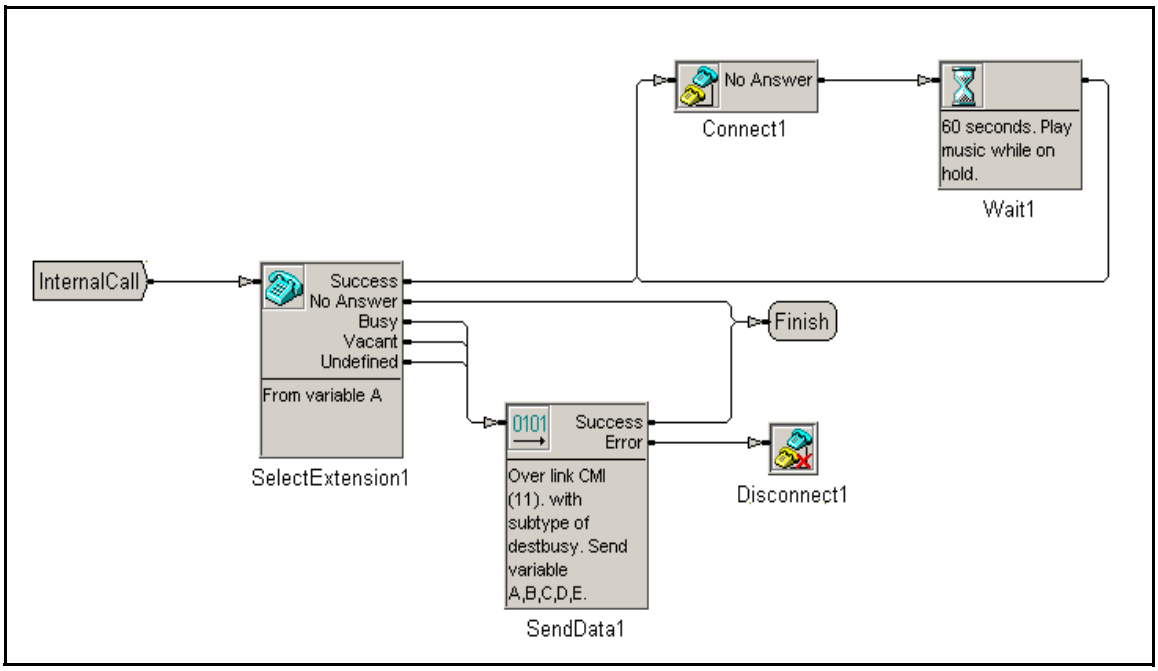
MakeCallCCT

The Aspect telephony event stream (Event Bridge) does not provide notification if the destination of make call is busy. However, the MakeCall CCT is aware of this case via the SELECTEXTENSION and Send Data steps.

The following diagram illustrates a MakeCallCCT for an external call:



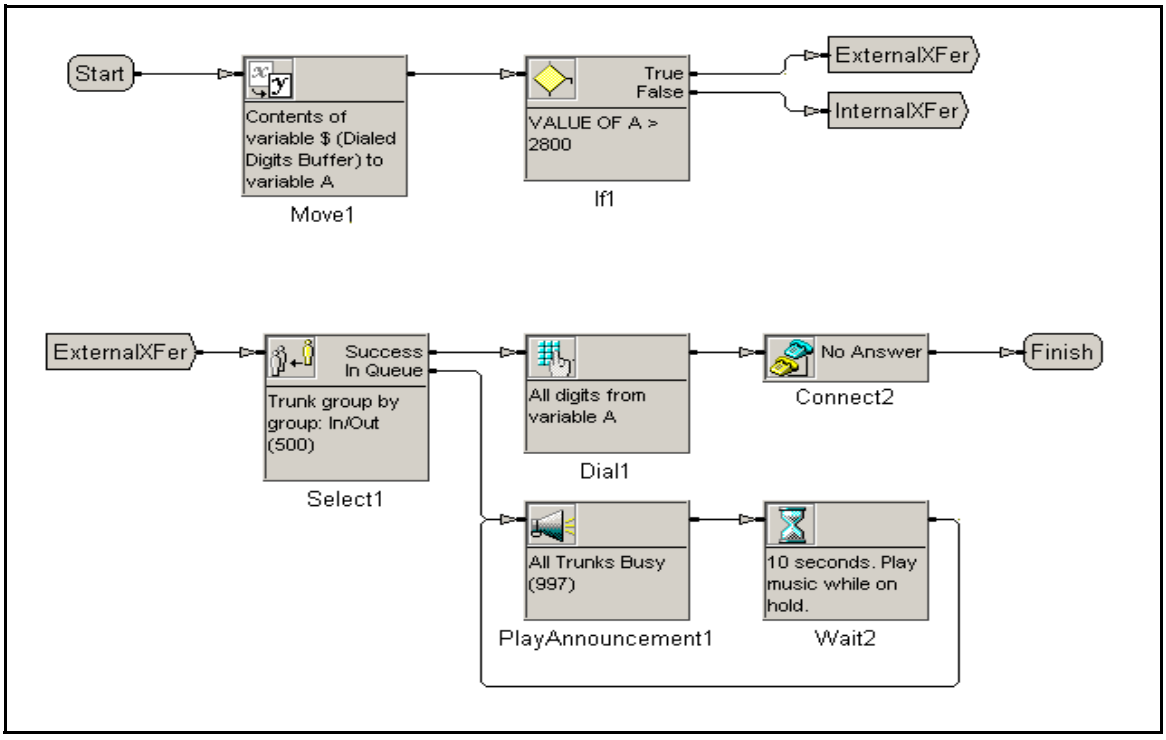
The following diagram illustrates a MakeCallCCT for an internal call:



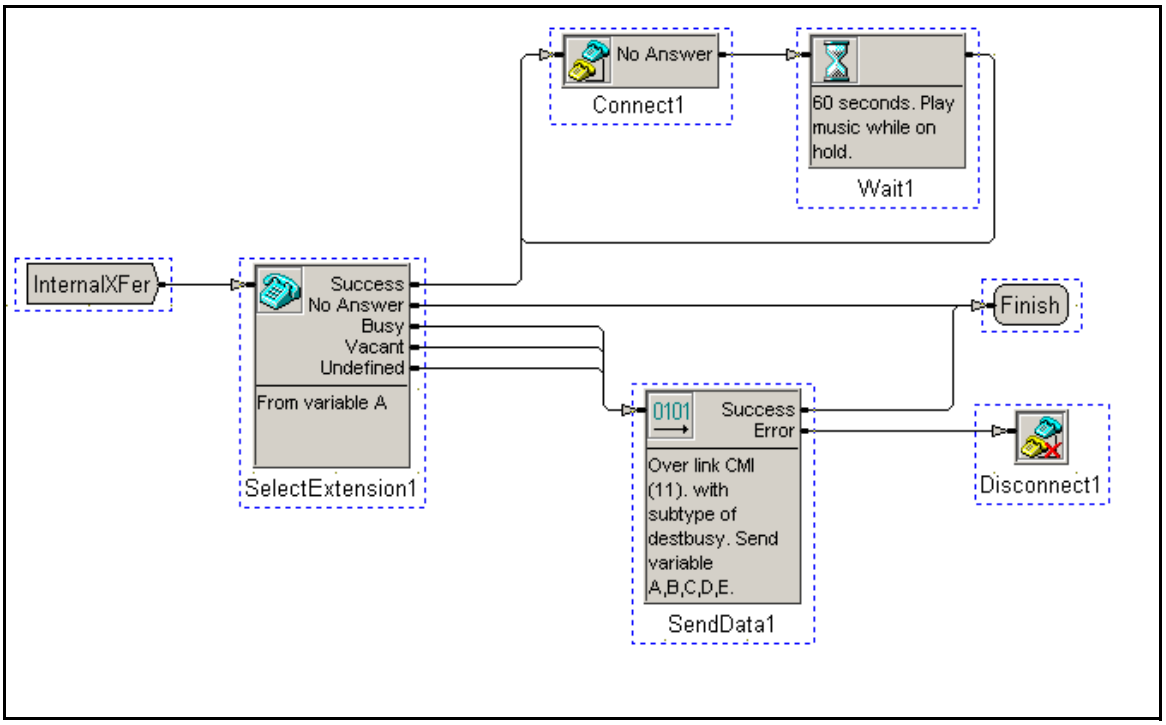
TransferInitCCT

The TransferInitCCT is provided for the same reason as specified in the previous MakeCallCCT description.

The following diagram illustrates a TransferInitCCT for an external transfer:

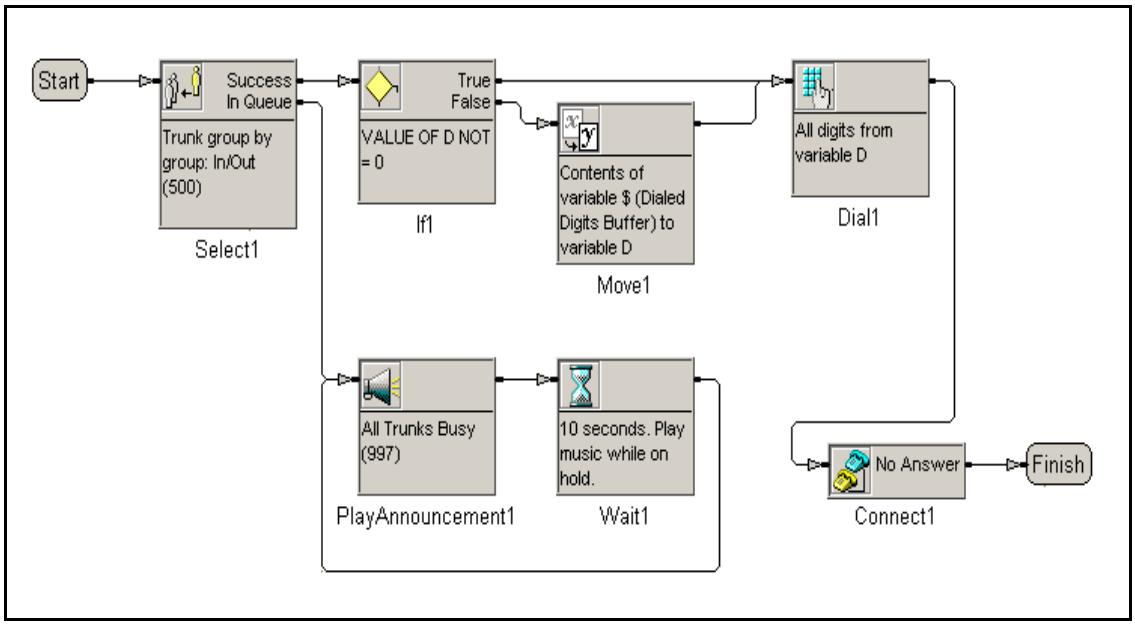


The following diagram illustrates a TransferInitCCT for an internal transfer:



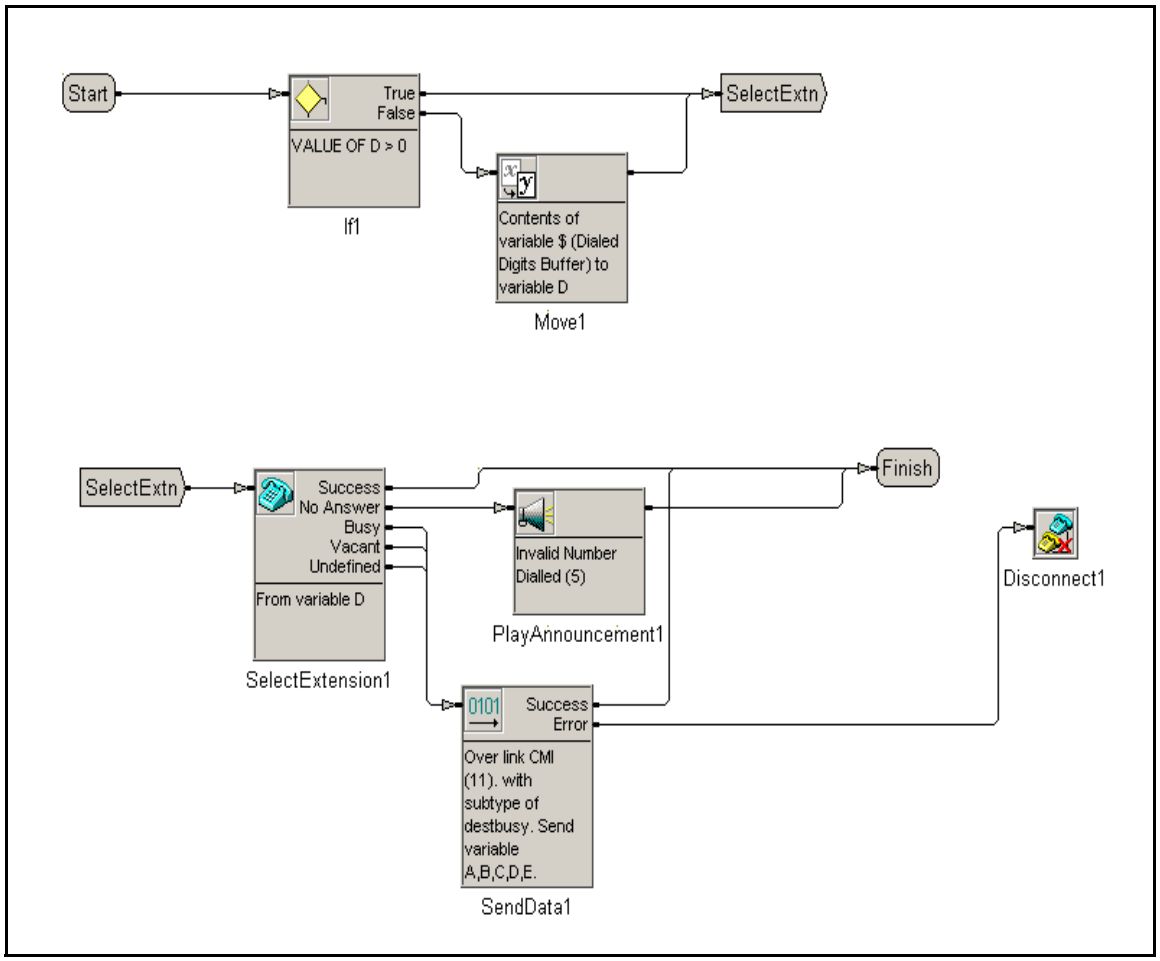
ExternalCCT

The External CCT gives the Aspect TS the ability to make calls which are external to the Aspect CallCenter System.



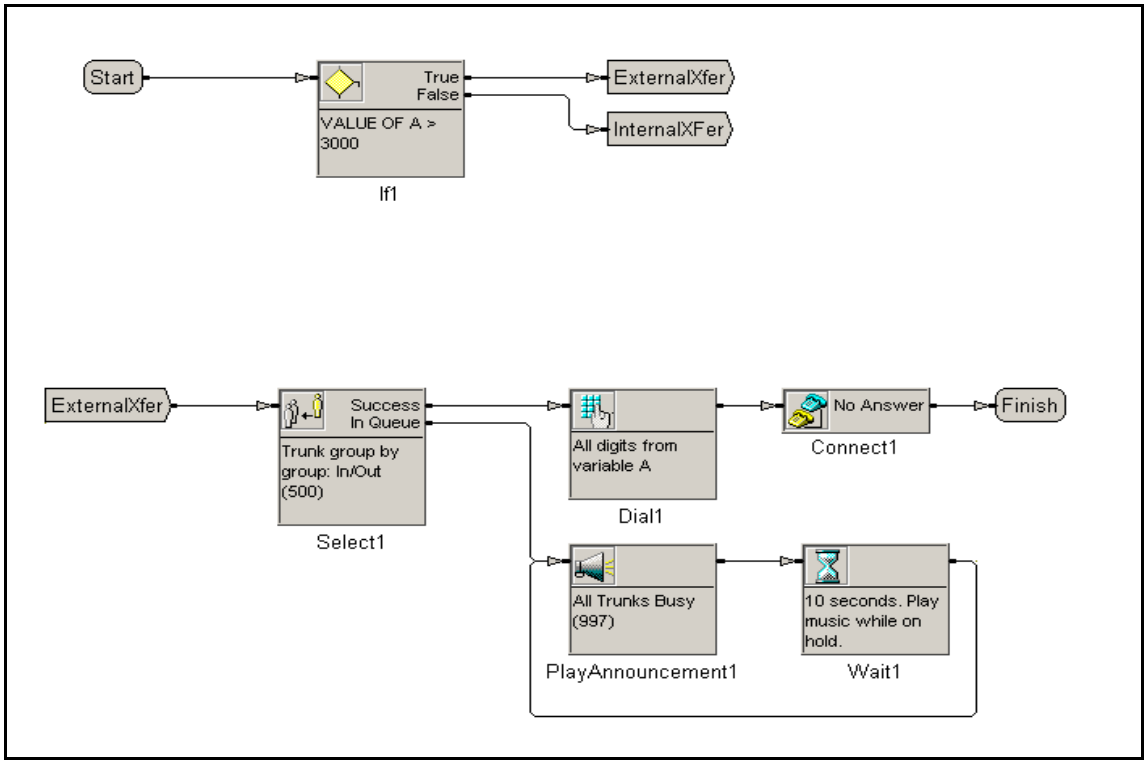
RouteCCT

The RouteCCT performs the necessary call routing in response to a RECEIVEDATA step. Refer to TS mechanisms on page 371 for more information on route points within the Aspect CallCenter.

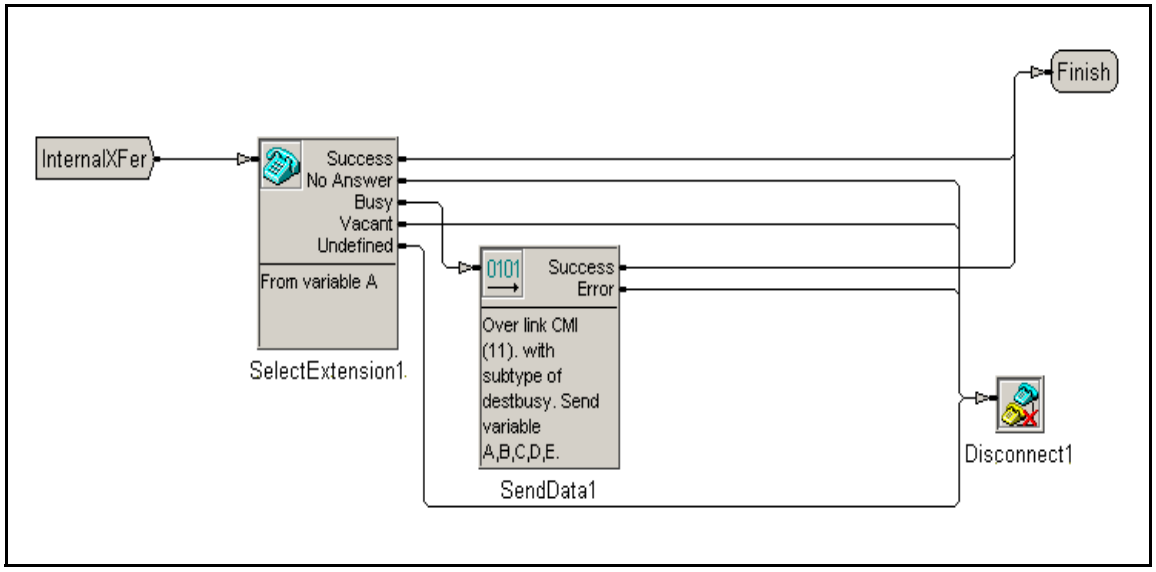


BlindCCT

The BlindCCT enables the Avaya TS to establish a connection to a specified resource. The following diagram illustrates a BlindCCT for an external transfer:

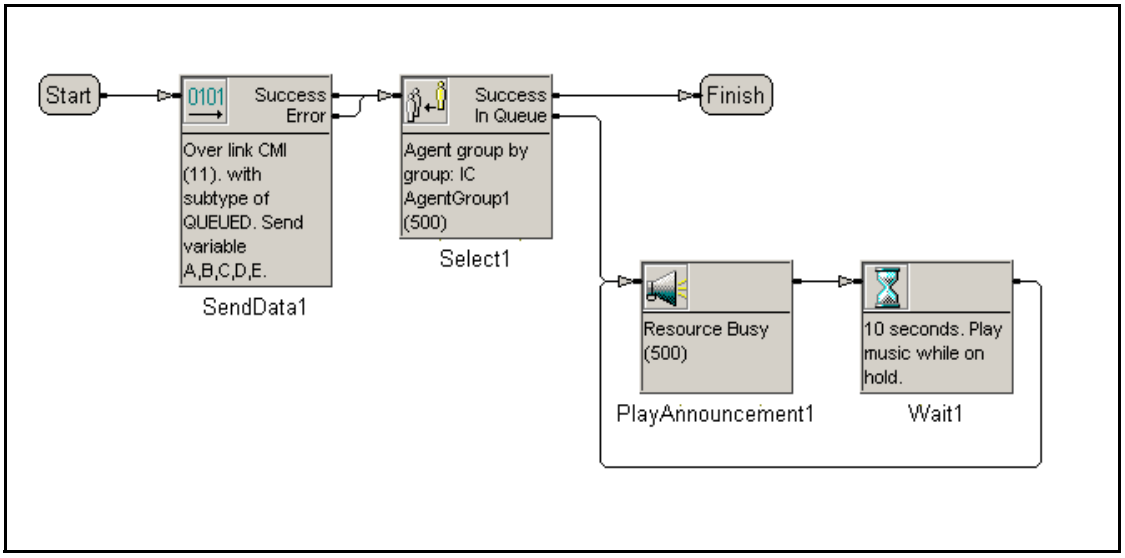


The following diagram illustrates a BlindCCT for an internal transfer:



AgentGroupCCT

The AgentGroupCCT routes calls to the queue used by a specified agent.



TS mechanisms

Route points

Route points on the Aspect CallCenter System are simulated by using a SENDDATA CCT step. The subtype of this step must identify, by name, the route point as specified within Avaya IC. For example, if the Avaya Workflow server is configured to perform a "*rSales" assignment to the Avaya TS, the SENDDATA CCT step must contain the subtype "Sales" to notify the Avaya TS, vla a Call Information Message (001), that a call has arrived at a logical point in the Aspect CallCenter switch.

The CCT must subsequently execute a RECEIVEDATA step to wait for a reply to the SENDDATA step. In this scenario, a positive reply indicates what needs to be redirected to the specified instrument or CCT. Refer to the Queue Statistics Server chapter of the *Telephony Connectors Programmer Guide* for more information about how route points are used on the TSQS.

Agent configuration

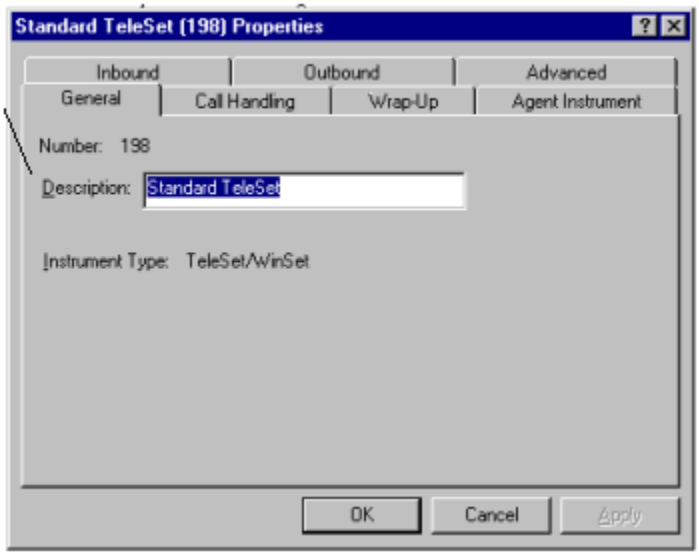
Agents do not sign into queues on the Aspect CallCenter System. Their queues are associated with their Agent ID on the switch. Therefore the “queue” IC agent configuration parameter is ignored by the Aspect version of the Avaya TS. When an agent logs into the Aspect CallCenter System and is made ready, the agent can receive calls from any agent group (such as a queue) in the Aspect CallCenter System with which the agent is associated.

Configure the Class of Service parameters for an Aspect agent using Avaya IC at the Aspect CallCenter System Hardware Administrator.

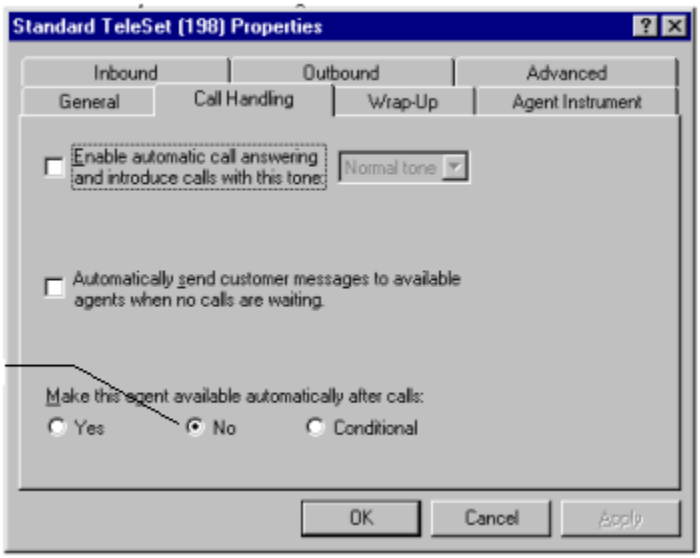
To configure the Class of Service parameters for an agent:

1. Start the **Aspect CallCenter Hardware Administrator**.
2. Navigate to the **Standard TeleSet Properties** dialog.
3. Select the **General** tab.

4. Fill in the **Description** field with the appropriate data.

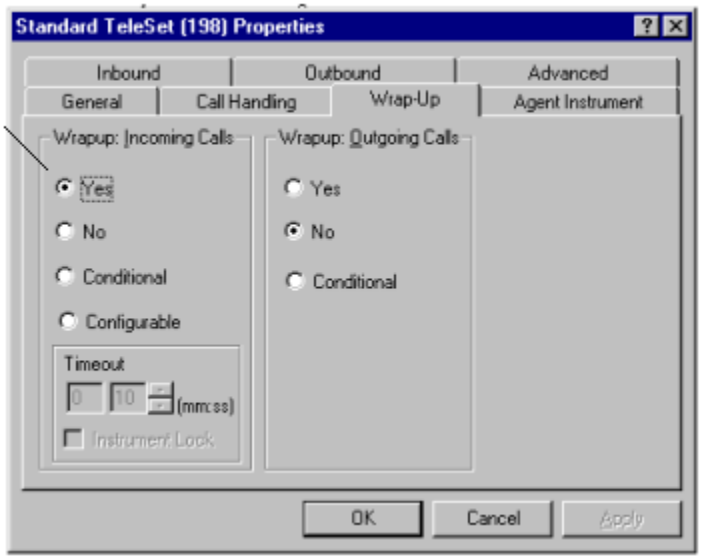


5. Select the **Call Handling** tab.
6. Click on the **No** radio button in the **Make this agent available automatically after calls** field.

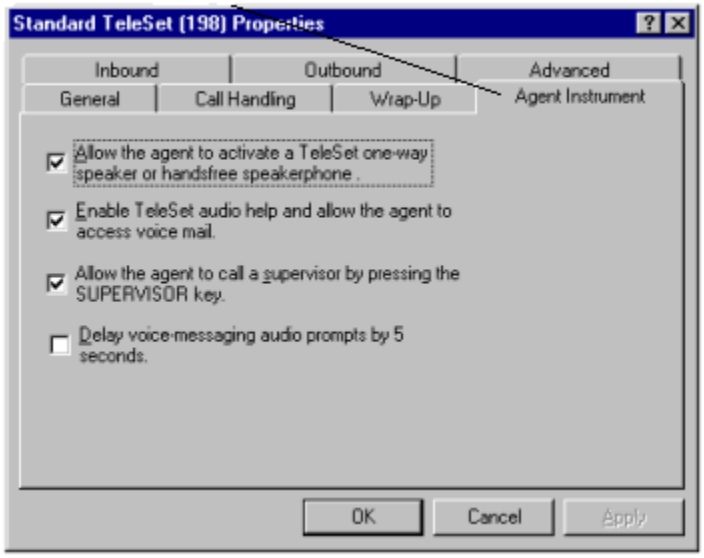


7. Select the **Wrap-Up** tab.

8. Click the **Yes** radio button in the **Wrapup: Incoming Calls** field if the agent is configured to perform wrapup duties in IC Manager.You must select the No radio button If the agent is not configured for wrapup in IC Manager.

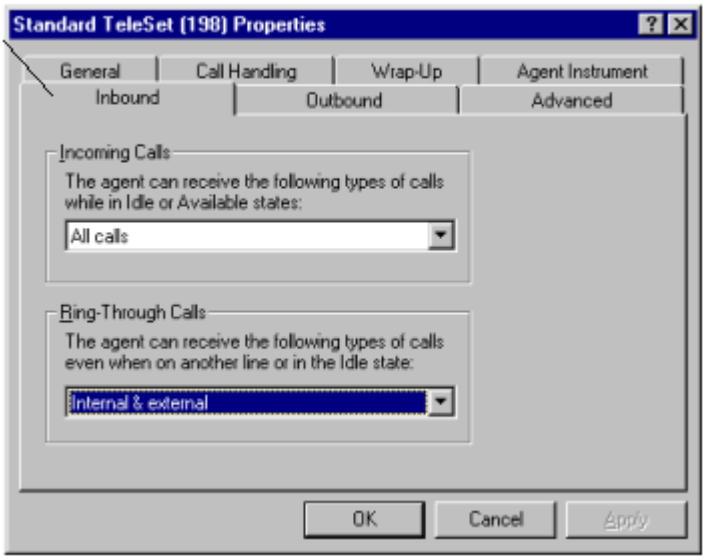


9. Select the **Agent Instrument** tab.
10. Check the check boxes for the first three parameters on this dialog.

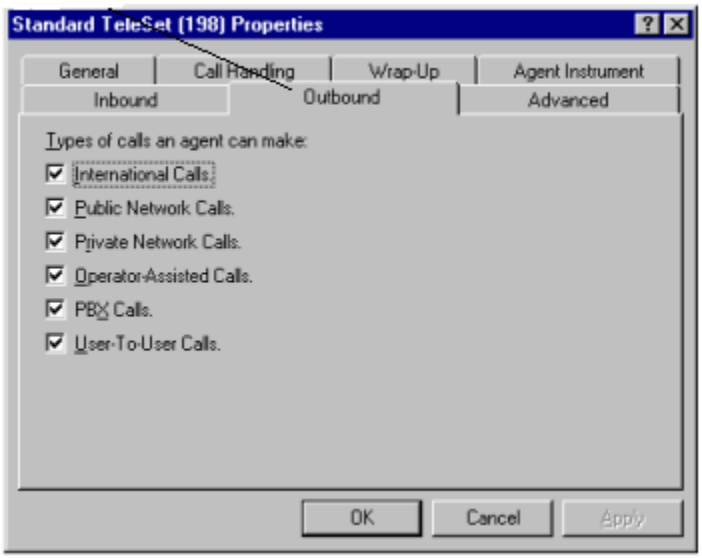


11. Select the **Inbound** tab.
12. Select **All Calls** from the drop down menu in the **Incoming Calls** field.

13. Select **Internal & external** from the drop down menu in the **Ring-Through Calls** field.

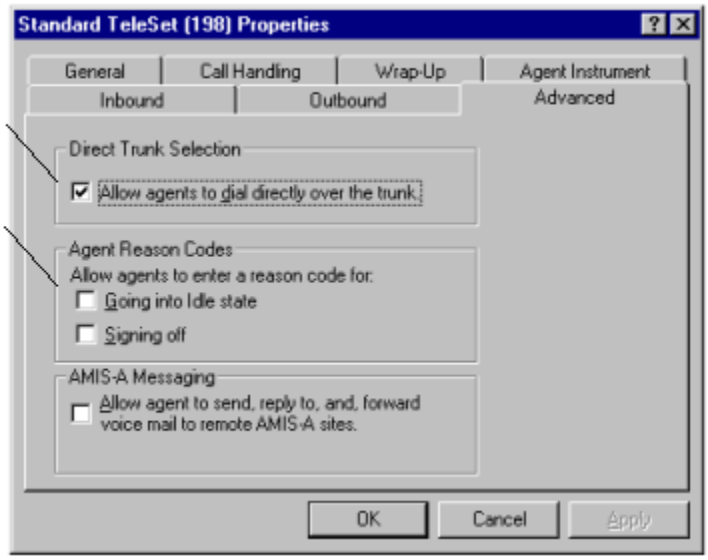


14. Select the **Outbound** tab.
15. Check the check boxes for the options you want for agent in the **Types of call an agent can make** field.



16. Select the **Advanced** tab.
17. Check the **Allow agents to dial directly over the trunk** option in the **Direct Trunk** field.

18. Uncheck any remaining check boxes that may be checked.



19. Click **OK** to save these agent configuration settings.

Predictive call properties

This section provides configuration and other information relating to the Aspect CMI TS and the PDK functionality available in IC 7.0. It contains the parameters that must be set on the Aspect CallCenter switch to enable outbound dialing functionality. For more information, refer to the instructions provided in the *Aspect CallCenter Administration Guide*:

Label	Description
predictive_country*	Specifies the country where the calls are destined. This controls how the Aspect call classification hardware identifies tones.
ams_delay*!	Represents a time, in seconds, that the answering machine detection should delay from being engaged on a predictive call. This prevents “quick” answers from engaging resource too “quickly”, when in all likelihood the call was answered by a human (waiting by the phone).
amr_mode*!	Determines “when” during answer detect the result is reported to the application issuing the predictive request.

Label	Description
ring_length!	Specifies the length in seconds of a ringing destination. This parameter is utilized in conjunction with the number of rings PDK configuration parameter. This parameter is necessary in that the PDK specifies a ring count while the Aspect expects a time (in secs) to ring prior to returning a ring no answer call classification.
adparam_mode_0*!	Only the first 4 bits are utilized for these parameters, however all 32 bits must be represented. These configuration parameters should be a 32-byte string representing the bits of a bit field. Where bit 0 represents the first char in the string. Bit 0 Bit31 "10010000000.....000" adparam_mode_X where X represents the “allocation” mode as provided by the PDK. The corresponding configuration parameter will (if specified) be utilized to override the default for that mode.
adparam_mode_1*!	see above
adparam_mode_2*!	see above
adparam_mode_3*!	see above
ansmap_mode_0*!	Only the first 17 bits are utilized for these parameters, however all 32 bits must be represented. These configuration parameters should be a 32-byte string representing the bits of a bit field. Where bit 0 represents the first char in the string. Bit 0 Bit31 "10010000000.....000" ansmap_mode_X where X represents the “allocation” mode as provided by the PDK. The corresponding configuration parameter will (if specified) be utilized to override the default for that mode.
ansmap_mode_1*!	see above
ansmap_mode_2*!	see above
ansmap_mode_3*!	see above
answer_mode_0*!	Specifies if answering machine detection is enabled for allocation mode 0.

Label	Description
answer_mode_1*!	Specifies if answering machine detection is enabled for allocation mode 1.
answer_mode_2*!	Specifies if answering machine detection is enabled for allocation mode 2.

* - Refer to the *Aspect Outbound Application Integration Guide* for further information regarding these configuration parameters

! - These should be custom configuration parameters, they are only available for override in the customer configuration tab.

Predictive dialing considerations

This section is to outlines the configuration and other information related to the Aspect CMI TS and the PDK functionality within IC 7.0.

Fax / modem detection

There is a known issue with the ability for calls to be classified by the Aspect CallCenter System's Answer Detect Card (ADC). If the ability to detect fax or modem is not functioning, predictively launched calls with these classifications will be delivered to an available agent for manual classification. Laboratory testing has concluded that these types of call destinations are considered as "answered" calls, that is, a live voice.

mcscon.ini

The mcscon.ini file has several notable configuration parameters relative to the Aspect CMI TS. The following table lists these parameters and specifies their usage:

Parameter	Description
PredictiveRoutePoint	The name of the "route point" as configured with the CCT used as a "route point".
PredictiveDropPoint	The CCT number used as a drop point on the Aspect. Append a "C" to this number to ensure it is considered a CCT. For example, if a CCT that performs "drop" processing is numbered 30, the PredictiveDropPoint parameter is 30c.
Allocation	Allocation mode 3 is NOT supported by the Avaya TS.

Multiple CMI server clients

This section outlines the configurations that are required if the Aspect CMI server has multiple client connections. This means the Aspect TS and any pre-existing CMI server clients that the customer may already use, such as Aspect Advanced Routing.

The Avaya TS must set `allow_unregistered_ subtype` to FALSE to prevent the Avaya TS from trying to process the Call Information Messages (CIM) that it received from the Aspect CallCenter that were intended for another client of the CMI server. This mechanism is necessary because the CMI server forwards all CIM messages it receives from the Aspect CallCenter System to every client of the CMI server.

Configure Aspect CallCenter for the TSQS

This section describes the Aspect CallCenter switch administration that is required to support the Avaya TSQS.

To configure the Aspect CallCenter switch to support the Avaya TSQS:

20. Set up the Aspect RealTime configuration file
21. Set up the Aspect RealTime Data Server

Set up the Aspect RealTime configuration file

The infogram that carries the statistics gathered from the Aspect CallCenter switch is configured on the Aspect ACD RealTime Contributor Administrator. This section describes how to set up the configuration file to support the TSQS.

In a typical Aspect system, this file is accessed through the Aspect web-based interface. The filename is `rts_aspect_admin.html`. For more detailed information on setting up the web based interface, refer to the Aspect CallCenter System switch documentation.

Complete the following fields in the **General Information** section of the Aspect RTB Contributor Administrator screen:

Field name	Description
RTS Server Host	IP address or machine name where the Aspect RealTime System is installed.
RTS Link Number	Link number that the contributor API concatenates with the literal "datahub" to produce the service name. For example, a contributor that specifies link 1 will use the port specified by the services entry "datahub1" in the service file to connect to the Aspect RealTime Server.

Field name	Description
Max Row	Maximum number of rows you want to retrieve from the data table in the ACD.
ACD Number	Number of the ACD to which the application will connect.
ACD Name	Name associated with this Aspect CallCenter System. For example, Aspect 1 or 8000.
Port	Port number associated with this Aspect CallCenter System. For example, 8000.
Interval (secs)	Number of seconds to wait until a reconnection is made. For example, 15.

Complete the following fields in the **Query Information** section of the Aspect RTB Contributor Administrator screen:

Field name	Description
ACD Name	Name of the Aspect switch that contains the statistics for the TSQS to gather.
Query String	SQL statement used by the TQSQ to gather statistics from the Aspect switch. This statement must look exactly like the example in the following SQL Statement section.
Duration	Number of seconds between Aspect database inquiries.
Infogram Number	Number of the infogram that contains the statistics information. This should match the Stats InfoGram Number parameter on the TSQS.

SQL Statement

This section describes the SQL statement that must be entered into Query String field of the Query information section of the Aspect RTB Contributor Administrator screen. If this statement is not entered exactly as shown below, the TSQS will not gather statistics correctly.

```
Select applic_num,long_wait_local,num_wait_local,num_hand_local,
num_aband_local,num_handws_local,avg_dly_que,num_talk_local,this_inc,
last_inc,this_aband_local,last_aband_local,avg_dly_que_aband,avg_spd_ans
  from applic WHERE applic.applic_num=64.
```

Important:

One exception is the `applic.applic_num` value on the last line of the statement. Change the "64" value in this example to the number of the application with the statistics you need.

Set up the Aspect RealTime Data Server

This section describes how to set up the Aspect RealTime Data Server for the Avaya TSQS. This server sends the statistics infogram from the switch to the Avaya TSQS.

For information on installing this server as well as additional configuration parameters, refer to the Aspect CallCenter System switch documentation.

The Aspect RealTime Data Server Configurator is used to configure the infograms that the Aspect RealTime Data Server will send to interested clients. This program can also be used to set up the infogram that will carry statistics information to the Avaya TSQS.

To create a statistics infogram on the Aspect RealTime Data Server Configurator:

1. Press the **New** button.
2. Complete the following fields on the Contributed InfoGram dialog box:

Field Name	Description
InfoGram ID	Number of the infogram to carry the statistics. This number should be the same number as the Stats InfoGram Number parameter on the TSQS and the Infogram Number parameter on the Query Information section of the Aspect RTB Contributor Administrator screen.
Description	Short description of the infogram.
Broadcast Frequency	Select the "When received from contributor" option.

3. Click **OK** to save these settings.

After the infogram is configured, check to see if the Aspect RealTime Data Server is receiving it for broadcast. From the Statistics menu option, open the InfoGram Statistics dialog box. If the statistics infogram you just created is not displayed in the list, refer to the Aspect RealTime Data Server documentation to find out if there are any special conditions that apply to your environment when creating a new infogram.

Aspect Reserved Subtypes

The Subtype field of the Send Data command is used to provide additional information about the nature of the data being sent to Avaya IC. As such, it is also used to correct or enhance the event stream and data between the TS and the PBX.

Some subtypes are used to manipulate the data passed directly between a CCT and the EDU. This data, that is manipulated to and from the EDU, is passed in the data_a field.

Subtypes can be processed by the Workflow server or by the TS. To receive notification about a specific subtype, the Workflow server needs to assign via the TS.Assign () method.

There are two assignment criteria:

Criteria	Description
*r	Related to call routing.
*s	Used to indicate to the TS that the assigned subtype is to be handled for data processing itself.

The following table describes the subtypes that are sent by the Aspect CallCenter switch. They are also described in more detail in the following sections.

Subtype	Description	Data	Returns
destbusy	Indicates the call destination is busy.	None	
gv*xxxxxxxxxx*	Retrieves one value from the EDU.	None	Retrieved value in data_a
newtrans	Changes the call reference ID of an existing call. Must be issued immediately after the preptrans command on any CCT.	data_e	New call reference ID
preptrans	Informs the TS that there will be a new call reference ID for an existing call via a newtrans control. Must be issued immediately before the newtrans command on any CCT.	data_e	
sv*xxxxxxxxxx*	Sets one value in the EDU.	data_a	Posts the value in the data_a field to the EDU. Note, the field name is the value in the subtype associated with prefix "sv".
timeout	Indicates a timeout during a route request.	None	

destbusy Destination Busy

During specific CCTs, such as MakeCall or Transfer, the destination might be busy. Aspect's event bridge does not post an event to indicate a busy state. To notify the TS of a busy state at the destination, you should use a CIM (SEND DATA command) or a CCM (SEND CONNECT command) to trigger a TS.Busy event.

Return Values None

Example

Step	Command	Attributes
1	SEND DATA	LINK#> 1 SUBTYPE destbusyVAR LIST A-E ON ERROR, EXECUTE CCT #999

gv*xxxxxxxxxx* Get One VDU Value

The value of data element *xxxxxxxxxx* is retrieved from the EDU server and sent to the requesting CCT via a combination of SEND DATA and RECEIVE DATA commands.

Subtypes starting with "gv" indicate the command VDU.GetOneValue() should be posted between the TS and the EDU server. The element in the EDUID is the data that follows the "gv".

For example, post a CIM (SEND DATA command) with subtype "gvlanguage" to the TS and wait for the response on a RECEIVE DATA command. The data is passed in the data_a field.

Note:

The RECEIVE DATA command is satisfied with the data, but the RESP field value is forced into a NAK, so processing continues in the local CCT.

Return Values

data_a contains the value returned.

Resp contains "N"

Example

Retrieve the value for "pubcode".

Step	Command	Attributes
1	SEND DATA	LINK#> 1 SUBTYPE gvpubcodeVAR LIST A-E ON ERROR, EXECUTE CCT #999
2	RECEIVE DATA	LINK#> 1 ON NAK, EXECUTE STEP 5 ON ERROR, EXECUTE CCT #999

newtrans New Transaction

When a NEW TRANSACTION command is executed in a CCT, the call reference ID of the call is changed, but the Aspect Application Bridge does not provide an event to notify the TS of the call id change.

A combination of two subtypes is required to provide the TS with enough data about the call id change.

1. The **preptrans** subtype tells the TS that a call id change is imminent, giving the TS an early warning that a given call id is about to change.
2. Once the NEW TRANSACTION command is completed, the **newtrans** subtype displays the new call id.

Return Values None

Example

Step	Command	Attributes
1	SEND DATA	LINK#> 1 SUBTYPE preptrans ON ERROR, EXECUTE CCT #999
2	NEW TRANSACTION	
3	SEND DATA	LINK#> 1 SUBTYPE newtrans ON ERROR, EXECUTE CCT #999

preptrans Prep Transaction

The preptrans subtype must be used to notify the PBX that the call reference ID of the call will be changed by a NEWSTRANS CCT command.

For more information, refer to newtrans New Transaction on page 385.

Return Values None

Example

Step	Command	Attributes
1	SEND DATA	LINK#> 1 SUBTYPE preptrans ON ERROR, EXECUTE CCT #999
2	NEW TRANSACTION	
3	SEND DATA	LINK#> 1 SUBTYPE newtrans ON ERROR, EXECUTE CCT #999

sv*xxxxxxxxxx* Set One VDU Value

This function stores a data element in the EDU with a name of *xxxxxxxx* and a value equal to the contents of data_a.

Subtypes starting with "sv" indicate the command VDU.SetOneValue() should be posted between the TS and the EDU server. The element in the EDUID is the data that follows the "sv". These subtypes allow you to send data to the EDU server.

Return Values None

Example Store the value for "pubcode".

Step	Command	Attributes
1	SEND DATA	LINK#> 1 SUBTYPE svpubcodeVAR LIST A-E ON ERROR, EXECUTE CCT #999

timeout Timeout

When a call on a RECEIVE DATA step times out, the Aspect switch does not notify the client application of the timeout. To notify the client application of the timeout, post a timeout subtype from the CCT to the TS. This prompts the TS to update the state of the call and, in turn, enhances TS call tracking capability.

Note:

Timeout is commonly used with the implementation of route points on Aspect, which is performed via a SEND DATA/RECEIVE DATA command pair.

Return Values None

Example

Step	Command	Attributes
1	SEND DATA	LINK#> 1 SUBTYPE aroutepoint ON ERROR, EXECUTE CCT #999
2	RECEIVE DATA	LINK#> 1 ON NAK, EXECUTE CCT #123, ON ERROR, EXECUTE STEP 10
...		
10	SEND DATA	LINK#> 1 SUBTYPE timeout ON ERROR, EXECUTE CCT #999

Meridian-1 administration: Symposium Server

This section describes how to configure the Nortel Meridian-1 switch to communicate with the Avaya TS using the Nortel Symposium Call Center Server. Refer to the Nortel Symposium Call Center Server documentation for more information about diagnosing faults and the various parameters that must be set for Symposium Call Center Server to communicate with the Avaya TS.

IC does not support Meridian's Auto-Hold feature. Hardphones must have a class of service (CLS) of Auto-Hold denied (AHD).

ELAN and VSID Configuration

The Embedded Local Area Network (ELAN) is a dedicated Ethernet TCP/IP LAN that enables Symposium Call Center Server to communicate with the Meridian-1 switch. The ELAN used by Symposium Call Center Server and the Meridian-1 switch is defined on the Meridian-1 switch as an Application Module Link (AML) over Ethernet.

The Value-added Server (VAS) provides communication between the Symposium Call Center Server and application software on the host to allow the application software to control phone set functions, such as answering a call or initiating a call. The ELAN must be associated with the VAS through a VAS ID (VSID) to allow message transmission between the Symposium Call Center Server and the application.

Use Overlay 17 (LD 17) to define and configure the ELAN and the VSID for Symposium Call Center Server.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To define and configure the ELAN:

1. Using the Meridian-1 PBX console, go to Overlay 17 (LD 17).
2. Complete the fields on the screen to match the following example:

```
REQ "CHG"
TYPE "CFN"
ADAN "NEW ELAN 16"
ELAN "16"
CTYP "ELAN"
VAS "NEW"
VSID "16"
```

Important:
For Avaya IC to take control of calls on a Symposium Call Center Server DN (agent phone set, IVR port, etc.), the ELAN's SECU prompt must be changed to YES, from the default setting of NO.

Value-added server (VAS) print out

Use Overlay 22 (LD 22) to print out the defined VAS IDs.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To print out defined VAS IDs:

1. Using the Meridian-1 PBX console, go to Overlay 22 (LD 22).
2. Complete the fields on the screen to match the following example:

```
>"LD 22"
...
REQ "PRT"
TYPE "VAS"
...
REQ "END"
```

These commands print out the defined Value-added Servers. Reference the ELAN that was configured for communication with the Symposium Call Center Server for more information.

Example

The following example illustrates a properly configured Overlay 22 (LD 22):

```
REQ prt
TYPE vas
...
VAS
   VSID 15
      DLOP
      AML 15
         SECU YES
         INTL 0001
         MCMT 9999
         CONF DIR
     APPL VMBA
             CUST 0
             DATA CORRECT OFF
             AUTO AUDIT ON
```

Symposium Call Center Server link start up

After you configure the ELAN and startup the Symposium Call Center Server, the ELAN link should come up.

To check the ELAN link:

1. Using the Meridian-1 switch console, go to Overlay 48 (LD 48).
2. Enter "STAT ELAN".
3. Ensure that, under your Symposium Call Center Server ELAN, IP-address, LYR7 and APPL are ACTIVE. Note the ELAN ID.

   Example: ELAN #: 16 DES: Avaya IC.
   APPL_IP_ID: 135.35.90.116 LYR7: ACTIVE EMPTY APPL ACTIVE
4. If the ELAN is not ACTIVE, check the ELAN connection by pinging the Meridian-1 switch's IP address from the Symposium Call Center Server.

Note:

If you enter "STAT ELAN" without an ADAN number, the Meridian-1 PBX console displays the status of all the ELAN links on the system.

Example:

```
ELAN #: 16 DES: Avaya IC
APPL_IP_ID: 135.35.90.116 LYR7: ACTIVE EMPTY APPL ACTIVE
```

Link 1 state changes to "Up" when the Avaya Telephony server, via CT-Connect, sends an ApplicationRegistration to the Symposium Call Center Server. This happens when the Avaya TS is started.

Link 1 state changes to "Enabled but down" when the Avaya Telephony server, via CT-Connect, sends an ApplicationRelease message to the Symposium Call Center Server. This happens when the Avaya TS is started.

Control DN (CDN) configuration

For a basic call on a Nortel switch, events for a contact are associated with a Nortel Control DN (CDN), which is monitored by the TS. There is a device queue for the CDN and OA reporting data is associated with the device queue. The events for the device queue are associated with a Nortel skill set which is monitored by the TSQS.

A Control DN (CDN) is like an ACD-DN, but it does not have any agents associated with it. When a call is received on the CDN, the switch sends a message to the TS requesting information on where to route the call. This assumes the TS has a CDN resource and has sent a DirectoryNumberRegistration message to the switch. Upon receiving the request for information from the switch, the TS must reply within a certain time period (4 seconds) or the call is given default routing treatment.

Important:
CDNs that are used by Avaya IC for routing calls (route points) must not be acquired by the Symposium Call Center Server.

If more than 10 consecutive route requests go unanswered, the Nortel switch considers the CDN inactive and default routes subsequent calls to the CDN.

Use Overlay 23 (LD 23) to configure a Control DN.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To configure a CDN:

1. Using the Meridian-1 PBX console, go to Overlay 23 (LD 23).
2. Complete the fields on the screen to match the following example:

```
>"LD 23"
...
REQ "NEW"
TYPE "CDN"
CUST "0"          <<---- Enter the customer number.
CDN "500"         <<---- Enter an available DN.
...
DFDN "400"        <<---- ACD-DN that untreated calls will be routed to by
                         default. This occurs if the application does not
                         respond to the 'RouteRequest' message in time.
CEIL "2047"       <<---- Maximum number of messages that can be queued.
RPRT "YES"        <<---- Report control.
CNTL "YES"        <<---- Controlled mode.
...
...
REQ "END"
```

Example

The following example illustrates a properly configured Overlay 23 (LD 23):

```
TYPE CDN
CUST 0
CDN 500
FRTT
SRTT
FROA NO
MURT
DFDN 400
CEIL 2047
OVFL NO
TDNS NO
RPRT YES
CNTL YES
VSID
HSID
CWTH 1
BYTH 0
OVTH 2047
ACNT
```

ACD-DN configuration

An Automatic Call Distribution Directory Number (ACD-DN) is a queue that agents are logged into and answers calls that enter in the queue. Use Overlay 23 (LD 23) to configure an ACD-DN.

After you set up the ACD-DN, use Overlay 11 (LD 11) to assign ACD position IDs to each agent's digital phone set. Note that you would use Overlay 10 (LD 10) to assign position IDs to each agent's analog phone sets. Overlay 11 is described in the Phone set and ACD agent configuration section of this chapter.

Use Overlay 23 (LD 23) to configure an ACD-DN.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To configure an ACD queue (ACD-DN):

1. Using the Meridian-1 PBX console, go to Overlay 23 (L23).
2. The following Overlay 23 prompts are required for the ACD to communicate with Avaya IC. Setting additional ACD prompts should not affect the communication with Avaya IC.

```
>"LD 23"
...
REQ "NEW"
TYPE "ACD"
CUST "0"          <<---- Enter the customer number assigned to the agents.
ACDN "400"        <<---- Select an available DN here.
...
MAXP "10"         <<---- Maximum number of agents assigned to the ACD.
...
ISAP "YES"        <<---- ACD to use Meridian Link messaging.
...

REQ "END"
```

Phone set and ACD agent configuration

For Avaya IC to control an ACD phone set, the AST and IAPG prompts must be properly configured on the set. This allows the Avaya TS to send messages to the switch that enable phone sets to answer, hang up, make calls, and so on.

For digital phone sets, use Overlay 11 (LD 11) and for analog phone sets, use Overlay 10 (LD 10).

The AST prompt, associates which keys on a digital set that can be made controllable by the Avaya TS. Since the phone set is an ACD phone set, KEY 00 is always used for the ACD key that allows agents to answer a queue call from the ACD-DN. Another KEY XX, for example KEY 01, can be defined, as a single-call ringing (SCR) or multi-call ringing (MCR) key, as the key from which the agent can use to make calls. In this example, the AST prompt would be set to "00 01".

The IAPG prompt controls the types of messages sent from the switch to Avaya IC when the ACD phone set changes state. By default, when IAPG is set to "1", all Meridian-1 messages, about the ACD phone set state, will be sent to Avaya IC.

Before you begin the following procedures, you must know the phone set’s type and TN. Refer to your Meridian-1 switch documentation for this information.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To configure digital phone sets:

1. Using the Meridian-1 PBX console, go to Overlay 11 (LD 11).
2. Complete the fields on the screen to match the following example:

```
>"LD 11"
...
REQ "NEW"
TYPE "2616"          <<---- Enter the phone set's type.
TN "028 0 03 04"     <<---- Enter the phone set's TN.
...
CUST "0"             <<---- Enter the customer number for the phone set.
...
AST "00 01"          <<---- Keys 00 and 01 will be controllable.
IAGP "1"             <<---- Allows phone state messages to be sent to IC.
...
KEY "0 ACD 400 401"  <<---- Key 0 must be the ACD agent. This example shows
                            Position ID 401 on ACD-DN 400.
KEY "1 MCR 123"      <<---- Multi-call ringing DN 123. This phone set can
                            also be dialed directly at DN 123.
...
REQ "END"
```

When using Symposium Call Center Server integration with Avaya IC and when Symposium Call Center Server has "acquired" the agent's phone set, the prompts on Overlay 11 are automatically set as follows:

```
AACS "YES"           <<---- Phone set was acquired by Symposium Server.
ACQ AS: TN           <<---- Based on what is acquired, ACQ AS can show any or
                            all of the following values:
                            TN for the TN
                            AST for the Position ID indicating that a
                            Meridian Link application registered for the ID
                            AST for the the DN indicating that a Meridian
                            Link application has registered for the
                            secondary DN key
ASID 16              <<---- VAS ID associated with the ELAN number that
                            Symposium Server is using
```

Use Overlay 20 (LD 20) to print the TN associated with the agent's phone set to view these prompts.

Example

The following example illustrates a properly configured Overlay 11 (LD11):

```
DES AGENT1
TN 036 9 01 12
TYPE 3905
CDEN 8D
CTYP XDLC
CUST 0
FDN 6999
TGAR 1
NCOS 3
RNPG 0
SSU
LNRS 16
SCPW
CLS CTD FBD WTA LPR MTD FNA HTA TDD CRPD STSD MWA RMMA SMWD IMD XHD IRA NID
    OLD VCE CRG1 POD DSX VMD CMSD SLKD CCSD SWD LNA CNDA CFTD SFA DDV CNID
    CDCA MSID DAPA BFED RDBD MCTD CLBD GPUD DPUD DNDD CFXD ARHD CNTD CLTD
    ASCD CFHD FICD NAID BUZZ AHD DDGA NAMA USRD ULAD RTDD RBDD RBHD PGND
    OCBD FLXD FTTC MCBN
CPND LANG ENG
RCO 1
HUNT 6999
LHK 1
LPK 1
SPID NONE
AST 00 01
IAPG 1
AACS YES
ACQ AS: TN,AST-DN,AST-POSID
ASID 16
SFNB 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
SFRB 1 2 15
USFB 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
CALB 0 1 2 3 4 5 6 7 8 9 10 11 12
FCTB
ITNA NO
DGRP
MLNG ENG
DNDR 0
RMTN
KEY 00 ACD 400 0 6001
AGN
    01 SCR 5001 0    MARP
    02
    03 ADL 16
    04 ADL 16
    05
    06 SCN 5999 0    MARP
    07
    08 MSB
    09 NRD
    10 DWC 400
    11
```

```
12
13
14
15
16 MWK 6999
17 TRN
18 AO6
19 CFW 4
20 RGA
21 PRK
22
23
24
25
26
27
28
29
30
31
```

TSQS Configuration

The Avaya TSQS (Queue Statistics server) only receives statistics for calls that are routed to an acquired CDN. As a result of this, the TSQS log does not contain the "contactcount" name value when a call is placed in a queue that is monitored by the TSQS.

To get updates for statistics on a TSQS configured for a Nortel Meridian switch using Symposium Call Center Server:

1. Create a CDN for incoming calls which is not acquired by SCCS. This is the CDN to which the workflow assigns.
2. Create a second CDN and acquire it to SCCS.
3. Create a workflow script that queues incoming calls to the ACD DN when agents are logged in.
4. Place a call to the CDN you created in step 1.
5. Have the workflow route the call to the acquired CDN you created in step 2. This queues the call to the proper ADC DN.

For more information on creating CDNs, refer to the Nortel Symposium Call Center Server Administration documentation that came with your switch.

Meridian-1 administration: Meridian Link

This section describes how to configure the Nortel Meridian-1 switch to communicate with the Avaya TS using the Meridian Link Module. Refer to the Meridian Link Module (MLM) documentation for more information about diagnosing faults and the various parameters that must be set for the MLM to communicate with the Avaya TS.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

IC does not support Meridian's Auto-Hold feature. Hardphones must have a class of service (CLS) of Auto-Hold denied (AHD).

AML configuration

Although Meridian Link effectively provides a single link between the host computer (the computer running the Avaya TS) and the Meridian-1 system, from an administrative and maintenance standpoint there are actually three links.

- Link 0 - The link between the IPE Module or Application Module and Meridian-1 is called link 0 or Application Module Link (AML).
- Link 1 - The link between the IPE Module or Application Module and the host computer is called link 1, the Host Link, or the Meridian Link.
- Link 2 - The link between the IPE Module or Application Module and Meridian Mail is called link 2 or the Meridian Mail Link (MML).

The AML (link 0) uses the LAPB protocol to transfer command and status messages, primarily to perform call-processing functions. The Host Link or Meridian Link (link 1) uses an X.25 switched virtual circuit or a TCP/IP protocol to transfer application messages.

To configure the AML on the Meridian-1 switch:

1. Define the ESDI/MSDL, STA, and SDI ports in the Configuration Record (LD 17). Make sure you refer to the prompts for your release of X11 software (Release 17 or later).
2. Identify the VASID and define the status message groups in LD 15.
3. Define ACD groups and agents in Automatic Call Distribution (LD 23) if they are required for the application.
4. Configure single-line telephones with the Associated Set (AST) and Unsolicited Status Messages (USM) features in Single-Line Telephone Administration (LD 10).
5. Configure multi-line telephones with the AST and USM features in Multi-Line Telephone Administration (LD 11).

6. Configure Control DNs (CDNs) in LD 23 if required for Host Enhanced Routing.
7. Enable the ESDI/MSDL port in Link Diagnostic (LD 48).
8. Enable the SDI port for console sharing in Input/Output Diagnostic (LD 37).

When configuring the Meridian-1 switch, you encounter the VSID, HSID, and AML prompts in LD17, LD15 and LD23. If you are adding Meridian Link or CCR to an IPE Module or an Application Module to create a co-resident system, you should understand what these prompts mean to avoid confusion.

If you have a system with a single IPE Module or Application Module and you should add either Meridian Link or CCR to create a co-resident system. You do not need to change the values entered at the VSID, HSID, or AML prompts.

If you have a system with two modules, one of which has Meridian Link (but not CCR) activated, the other of which has CCR (but not Meridian Link) activated, and you want to create a co-resident system by removing one module and activating both applications on the remaining module, you must make changes to the values entered at the VSID, HSID, and AML prompts. You should choose a configuration that requires the fewest changes.

Example:

```
ADAN  AML 6
   CARD 01
   PORT 3
   DES  MERLINK
   BPS  19200
   CLOK INT
   IADR 003
   RADR 001
   T1   04
   T2   010
   T3   010
   N1   128
   N2   08
   K    7
   RXMT 05
   CRC  10
   ORUR 005
   ABOR 005
   ENL  YES
...
VAS
  VSID   06
   DLOP
   AML   06
   SECU  YES
   INTL  0004
   MCNT  0400
   CONF  DIR
```

Meridian Link Module configuration

Systems shipped from the factory are configured as described in the following sections. The default configuration for link 0 applies to Meridian Link, CCR, and co-resident systems. Configurations for link 1 and link 2 are for Meridian Link and co-resident systems only.

Link 0: Application Module Link

Link 0 is defined as the Application Module Link (AML), with the following characteristics:

```
Protocol: HDLC                    Link type: 1
Machine ID: SL16
Delay: 0
Port type: H                      Physical DTE(0)/DCE(1): 0
PDN type: 0                       Maximum Frame length: 135
Baud rate: 19200                  Fail timer: 50
RFS timer: 150                    Internal address: 1
Remote address: 3                 T1: 20
Maximum out frames (K): 7         Maximum trans attempts: (N2): 8
```

Link 1: TCP/IP host link protocol (Meridian Link)

Link 1 is defined as the host link using the TCP/IP protocol if service 95 is equipped, with the following characteristics:

```
Protocol: LAN                     Link type: 2
Machine ID: Lanlink
Delay: 0
Port: 3000
```

In most cases, Avaya IC requirements are satisfied by the default Meridian Link configuration above.

Link 2: Meridian Mail Link (optional for Meridian Link).

Link 2 is defined as the Meridian Mail Link (MML) and is not needed for Avaya IC to function.

Meridian Link start up

After you configure the AML and start up the Meridian Link, the AML should come up. To start up the Meridian Link:

- Check the AML on the switch
- Enable the AML on the switch
- Check links 0 and 1 in the MLM
- Enable links 0 and 1 in the MLM

To check the AML on the switch:

1. Using the Meridian-1 switch console, go to Overlay 48 (LD 48).
2. Enter "STAT AML".
3. Ensure that, under your Meridian Link AML, LYR2 is CONNECTED.

Example:

```
AML: 06 ESDI: 06  DES: MERLINK
LYR2: CONNECTED   LYR7: ACTIVE  EMPTY   APPL ACTIVE
```

To enable the AML on the switch:

1. Using the Meridian-1 switch console, go to Overlay 48 (LD 48).
2. Enter "ENL AML # ACMS".
3. The link should come up in approximately 20 to 30 seconds.

To check Links 0 and 1 in the MLM:

1. Using the Meridian Link Module console, login as 'mlusr' user.
2. Enter "status link 0". The response "Link 0: Up" indicates that the link is functioning properly. If you receive a different response, refer to Nortel Networks' Application Module and Intelligent Peripheral Equipment Module Diagnostic and Maintenance Guide.
3. Enter "status link 1". The response "Link 1: Up" indicates that the host link is functioning properly. This message appears only if a host application, in this case Avaya TS is connected. If you receive a different response, refer to Nortel Networks' Application Module and Intelligent Peripheral Equipment Module Diagnostic and Maintenance Guide.

To enable Link 0 & 1 in the MLM:

1. Using the Meridian Link Module console, log in as 'mlusr' user.
2. Enter "enable link 0".
3. Enter "enable link 1".
4. Links 0 and 1 are enabled.

Control DN (CDN) configuration

For a basic call on a Nortel switch, events for a contact are associated with a Nortel Control DN (CDN), which is monitored by the TS. There is a device queue for the CDN and OA reporting data is associated with the device queue. The events for the device queue are associated with a Nortel skill set which is monitored by the TSQS.

A Control DN is like an ACD-DN, but it does not have any agents associated with it. When a call is received on the CDN, the switch sends a message to the application requesting information on where to route the call. This assumes the application has a CDN resource and has sent a DirectoryNumberRegistration message to the switch. Upon receiving the request for information from the switch, the application must reply within a certain time period or the call is given default routing treatment.

Important:
CDNs used by IC for routing calls (also known as route points) must not be acquired by the Symposium Call Center Server.

Use Overlay 23 (LD 23) to configure a Control DN.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To configure a controlled DN:

1. Using the Meridian-1 PBX console, go to Overlay 23 (LD 23).
2. Complete the fields on the screen to match the following example:

```
>"LD 23"
...
REQ "NEW"
TYPE "CDN"
CUST "0"          <<---- Enter the customer number.
CDN "500"         <<---- Enter an available DN.
...
DFDN "400"        <<---- ACD-DN that untreated calls will be routed to by
                         default. This occurs if the application does not
                         respond to the 'RouteRequest' message in 4 seconds.
RPRT "YES"        <<---- Report control.
CNTL "YES"        <<---- Controlled mode.
VSID "1"          <<---- VAS ID used for Meridian Link messaging.
HSID "1"          <<---- VAS ID for application module link (AML) to host.
...
REQ "END"
```

ACD-DN configuration

This section describes overlay 23, which is used to set up the ACD-DNs. The use Overlay 11 to assign ACD position numbers to each phone set. Overlay 11 is described in the Phone set and ACD agent configuration section of this chapter.

Use Overlay 23 (LD 23) to configure an ACD-DN.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To configure an ACD queue (ACD-DN):

1. Using the Meridian-1 PBX console, go to Overlay 23 (LD 23).
2. The following Overlay 23 prompts are required for the ACD to communicate with Avaya IC. Setting additional prompts should not affect communication with Avaya IC.

```
>"LD 23"
...
REQ "NEW"
TYPE "ACD"
CUST "0"          <<---- Enter the customer number assigned to the agents.
ACDN "400"        <<---- Select an available DN here.
...
MAXP "10"         <<---- Maximum number of agent positions.
...
ISAP "YES"        <<---- ACD-DN that uses Meridian Link messages.
VSID "1"          <<---- VAS ID defined in Overlay 17.
```

```
...

REQ "END"
```

Phone set and ACD agent configuration

Before the protocol stack can control a phone set connected to the switch, the phone set must be made "controllable" by the switch administrator. This allows Avaya Agent to send messages to the switch that enable phone sets to answer, hang up, make calls, and so on. The phone set is made "controllable" by assigning the "AST" prompt to two keys on the phone set.

Use overlay 11 to configure multi-line phone sets. The "IAPG" prompt controls the messages sent from the switch to the Avaya Agent when the phone set changes state. This parameter can also be set in the phone set configuration. The "Key" prompt is used to define an ACD phone's position ID.

Before you begin the following procedures, you must know your telephone's type and TN. Refer to your Meridian Link Module documentation for this information.

User input is displayed in double quotes. Do not type the double quotes when entering the commands. Where an ellipsis (...) is displayed, press ENTER to select the default value for the prompt.

To configure digital phone sets:

1. Using the Meridian-1 PBX console, go to Overlay 11 (LD 11).
2. Complete the fields on the screen to match the following example:

```
>"LD 11"
...
REQ "NEW"
TYPE "2616"
TN "028 0 03 04"     <<---- Every phone set will have a different TN.
...
...
CUST "0"
...
...
AST "0 1"            <<---- Keys 0 and 1 will be controllable.
ISAP "1"             <<---- Allows phone state messages to be sent to the
                            application.
...
KEY "0 ACD 400 401"  <<---- Key 0 must be the ACD agent. This example shows
                            position 401 on ACD queue DN 400
KEY "1 MCR 123"      <<---- Multi-call ringing on DN 123. This phone set can
                            also be dialed directly at DN 123.
...
REQ "END"
```

Ericsson MD110 Administration

This section describes how to configure the Ericsson MD110 switch, using Ericsson Application Link Server 4.0, to connect to the Avaya Telephony server (TS) on Avaya IC. Refer to the Ericsson MD110 administration and configuration documentation that was provided with your switch for more details on administering the switch to accommodate the goals of this section.

Avaya IC supports the RONA (Redirect on No Answer) switch feature that redirects calls that are sent to agents, but are not answered by the agents. Agents must be configured for RONA on the Ericsson MD110 switch to use RONA. For RONA configuration instructions, refer to the Ericsson MD110 administration and configuration documentation that was provided with your switch.

Note:

Ericsson MD110 does not support reason codes for placing an agent in AUX mode.

Software requirements

Ericsson MD110 uses Intel NetMerge Call Processing 6.0 software to connect the TS to the Ericsson Application Link 4.0 Server.

The following table lists the software required by Avaya IC and the machine on which it should be installed:

Required Software	Installed On..
Ericsson MD110 release BC10 or above	PBX (phone switch)
Ericsson Application Link Server 4.0 (with the latest service pack and hot fixes)	ApplicationLink server
Intel NetMerge Call Processing 6.0	Telephony server

Configuring the Application Link

This section describes how to configure the Ericsson Application Link Server to connect to the TS in Avaya IC.

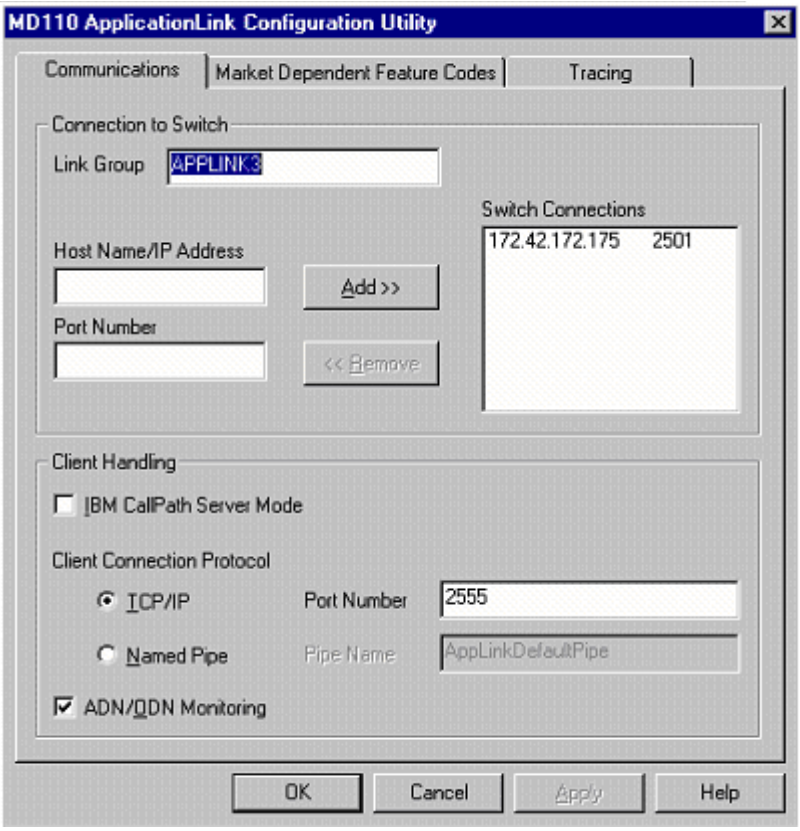
To configure the Ericsson Application Link Server to connect to the TS:

1. Open the **MD110 ApplicationLink Configuration Utility** dialog.
2. Select the **Communications** tab.
3. In the **Link Group** field, enter a name for the new **Link Group** to identify the link to the PBX.
4. In the **HostName/IP Address** text box, enter the IP address of the PBX.
5. In the **Port Number** text box, enter the port number of the PBX.
6. In the **Client Connection Protocol** section:
   a. Click the **TCP/IP** radio button and
   b. Enter **2555** (Default) in the **Port Number** field.
7. Select the **ADN/ODN Monitoring** check box.

   Note:

   The Application Link Server can monitor ODNs and ADNs on the same DTS. When the **ADN/ODN Monitoring** feature is selected on the **MD110 ApplicationLink Configuration Utility** configuration dialog, the feature is enabled the next time the Application Link Server is started.
8. Press **OK** to save these settings.

The following example illustrates a **Communications** tab on the **MD110 ApplicationLink Configuration Utility** dialog:

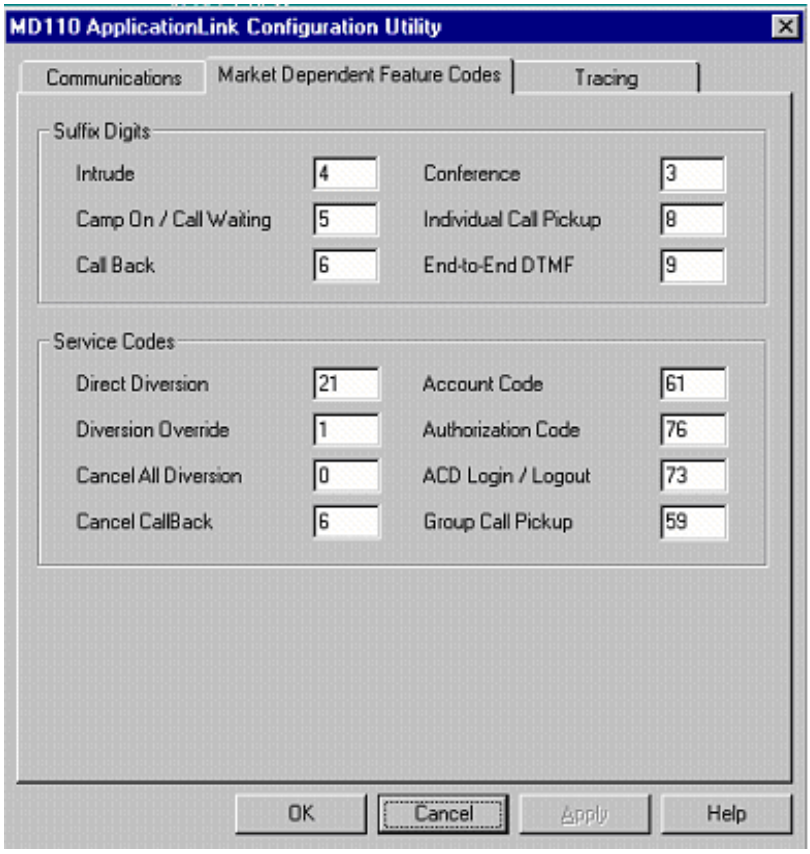


The **Market Dependent Feature Codes** tab must have an appropriate value in the **ACD Login / Logout** parameter. These values vary by region, so contact your Ericsson MD110 PBX administrator to get the value(s) that apply to your region.

To enter the ACD Login / Logout setting:

1. At the **MD110 ApplicationLink Configuration Utility** dialog, select the **Market Dependent Feature Codes** tab.
2. In the **Service Codes** section, enter the values for your region in the **Direct Diversion** and **ACD Login / Logout** fields.
3. Press **OK** to save the value.

The following example illustrates a **Market Dependent Feature Codes** tab on the **MD110 ApplicationLink Configuration Utility** dialog:



Timed ACW

Ericsson MD110 supports Timed ACW through the Clerical Time (CLT) feature. CLT is associated with an ADN in an ACD group. You need to configure the number of seconds that an ADN can be in CLT for every ADN on the system.

The Agent Mode Preset function is not available on the Ericsson MD110. For example, an agent who is on a call cannot request an ADN to go to the Not Ready state (AUX) after the call is disconnected. If Clerical Time (CLT) is not configured for an ADN, the agent goes directly into the Ready state when the call is disconnected. In this case, an ACD call could reach him before the TS asks the switch to move him to the Not Ready state.

To resolve this issue, the Clerical time (CLT) for the ADNs of all the IC agents must be set to a minimum of 1 second.

Example: The following command sets the CLT of ADN 5000 to 1 second

```
ACGMC :DIR=5000,CLT=1;
```

- If WrapUp is not configured on IC, set the CLT value to **1** second.
- If WrapUp is configured on IC, set the CLT value to **999** seconds.

Note:

Setting the CLT value to 999 seconds keeps the ADN in clerical mode long enough for the agent to complete wrap up activities on the contact before clicking Ready on the Softphone. If this value is set too low, the ADN will go into the Ready state while IC remains in the WrapUp state. In this case, an agent could receive a new call while still working on wrap up activities from the previous call. You can set this value based on the expected wrap up duration at your contact center.

ACD and CTI groups

The ACD (Automatic Call Distribution) and CTI (Computer Telephony Integration) groups are associated with a directory number, a queue of a certain size, and a number of ACD agents, which for the Ericsson MD110 are monitorable ADNs programmed on a DTS.

A CTI group is a special type of ACD group, which has a queue associated with it but may not have any agents associated with it.

To monitor an ACD or CTI group, the directory number of the group is stated in the monitor start request. A queued event is generated when no ACD agents are available and the call is queued.

When a call is received on a CTI group that is monitored by the TS, the switch sends an inbound call message to it. Upon receiving the event from the switch, the TS can divert the call from the CTI group to a destination.

The maximum number of seconds that the call remains queued in an ACD/CTI group is 32768. There can be a maximum of 255 calls queued in an ACD/CTI group.

Important:

When a call is deflected from a CTI group to another group, the Call ID reported in the destination is different from the original Call ID. To resolve this issue monitor all of the devices that are part of the call and apply ApplicationLink 4.0 Hot Fix 1004 on the Application Link Server.

The following examples illustrate ACD and CTI group commands:

1. The following command initiates ACD group 7050 as an ACD group:

```
<ACGRI:GRP=7050,LIM=1,SERV=1010,TRAF=15,SEL=11015,QUE=00010010101;
```

2. The following command initiates ACD group 7051 as a CTI group:

```
<ACGRI:GRP=7051,LIM=1,SERV=1011,TRAF=15,SEL=11015,QUE=00010010101;
```

3. The following command prints the configuration for ACD group 7050:

```
ACGCP:GRP=7050;
ACD GROUP CALL DATA
GRP       LIM    SERV   TRAF   SEL    QUE          QIC   CUST  SAT   ACTC
7050      1      1010   15     11015  00010010101              NO    10
```

4. The following command prints the configuration for CTI group 7051:

```
ACGCP:GRP=7051;
ACD GROUP CALL DATA
GRP       LIM    SERV   TRAF   SEL    QUE          QIC   CUST  SAT   ACTC

7051      1      1011   15     11215  10150752525              NO    180
```

Appendix B: IIS Lockdown Tool

You can use the IIS Lockdown Tool to increase the security of an IIS deployment that hosts Websites and Web applications for Avaya IC and Avaya OA. Microsoft recommends the Lockdown Tool to close some security risks that can occur with IIS. IIS is not supported with Avaya Agent Web Client.

This section describes the steps tested and recommended by Avaya for how to configure and implement security with the IIS Lockdown Tool. Deviations from this recommended configuration could interfere with the performance of Avaya IC.

Perform this configuration after you install and configure the Avaya IC system.

This section includes the following topics:

- Prerequisites for the IIS Lockdown Tool on page 411.
- Downloading the IIS Lockdown Tool on page 412.
- Configuring security with the IIS Lockdown Tool on page 412.
- Testing the security settings on page 415.
- Troubleshooting the security settings on page 415.

Note:

Microsoft developed and maintains the IIS Lockdown Tool. Avaya recommends that you review and follow the security guidelines for IIS outlined by Microsoft. Avaya does not make security recommendations for IIS or Windows.

Prerequisites for the IIS Lockdown Tool

Before you install and use the IIS Lockdown Tool, do the following:

1. Apply the most recent security patches and hot fixes for the Windows Server operating system. For more information, see Microsoft Windows on page 215.
2. Apply the most recent security patches and hot fixes for Microsoft IIS 5.0. For more information, see Security patches and hot fixes for Microsoft IIS on page 283.
3. Back up all files on the machine that hosts the IIS Web server.

4. Install and configure the Avaya IC system, including all channels and prerequisites, as described in *IC Installation and Configuration*.

Downloading the IIS Lockdown Tool

To download the IIS Lockdown Tool version 2.1:

- Go to the following Website in your Web browser:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC

- If that link is no longer valid:
  1. Go to the Microsoft Web site at http://www.microsoft.com
  2. Navigate to the Download Center.
  3. In the **Search for a Download** section:
     - Select IIS from the **Product/Technology** drop-down list.
     - Enter `Lockdown Tool 2.1` in the **Keywords** field.

Follow the instructions on the Website to install the IIS Lockdown Tool.

Configuring security with the IIS Lockdown Tool

This section provides the security settings for the IIS Lockdown Tool that are compatible with IIS and Avaya IC.

The instructions and information in this section assume that the machine that hosts Microsoft IIS 5.0 uses Windows 2000 Server SP4. This information was current at the time of publication. Check the documentation and other information provided on the Microsoft Web site for the most recent changes.

To configure security with the Lockdown Tool.

1. Navigate to the folder where you downloaded and installed the IIS Lockdown Tool.
2. Double-click `iislockd.exe`.

3. Complete the windows in the IIS Lockdown Tool with the properties described in the following table.

Window	Property	Recommended value
Lockdown Security Templates	Server templates	Select Static Web Server. Avaya IC does not use ASP. You can select Dynamic Web Server if you host an ASP application on the same machine as Avaya IC.
	View Template Settings	Check this box. You need to view template settings to be able to customize the template.
Internet Services **Note:** If a service has not been installed, the options are not available.	Web services (HTTP)	Check this box.
	File transfer service (FTP)	If you want to allow the ability to FTP files from the machine that hosts the Avaya IC Website, check this box.
	E-mail service (SMTP)	If the Avaya IC system uses an SMTP server on the target machine to make SMTP connections for the email channel, check this box.
	News service (NNTP)	If you host NNTP on the same machine as the Avaya IC Website, check this box.
	Remove unselected services	Do not check this box. If you do not check this box, the IIS Lockdown Tool disables the service but does not remove it. You can enable the service later, if required.
Script maps	Disable support for the selected script maps.	Check all boxes.

Window	Property	Recommended value
Additional security	Remove the selected virtual directories from this server	If desired, check the boxes for virtual directories.
	Set file permissions to prevent anonymous IIS users from performing these actions	Check all boxes.
	Disable Web Distributed Authoring and Versioning	Check this box.
URLScan	Install URLScan filter on the server.	If desired, check this box. **Note:** The URLScan filtering tool runs as an ISAPI filter at the root of the IIS installation. Rules to block URL requests are in the urlscan.ini file. Avaya has not evaluated the impact of this tool and IIS on Web server performance.

After the IIS Lockdown Tool completes the configuration, it generates a report of the changes.

4. If you installed the URLScan ISAPI filter:

   a. Open the `urlscan.ini` file in a text editor and add the verb `POST` to the list of verbs in the `[AllowVerbs]` section.

      By default, `urlscan.ini` is installed in the following location: `...\winnt\system32\inetsrv\urlscan\urlscan.ini`

   b. In the Services control panel, stop and restart the World Wide Web Publishing Service.

   If you do not add `POST`, a user might receive `404 - Page Not Found` errors from an Avaya IC Website.

   The URLScan tool writes a log file to `...\winnt\system32\inetsrv\urlscan`. Check this log file to determine if URLScan has rejected a particular request.

5. If you plan to install Avaya IC agent desktop applications from a Web server, delete the `EXE` from the list in the `[Deny Extensions]` section.

   You do not need to perform this step if you plan to install Avaya IC agent desktop applications from a network share.

Testing the security settings

After you configure security settings with the IIS Lockdown Tool, test Microsoft IIS 5.0 to validate that the Web server performs as expected.

To test the security settings:

1. In IC Manager, select **Services** > **WebACD** to access the Avaya IC Administration Website.
2. Access the Avaya IC Customer Website at the following URL:

   `http://<`*machine_name*`>.<`*domain_name*`>/website/public`
3. Start a chat contact and make sure that:
   a. The chat applet launches correctly.
   b. An agent can receive and respond to the chat contact.
4. Send an email contact from the Website and make sure that an agent receives the email contact.
5. If the Avaya IC system includes Self Help or other Web Management features, test those features to make sure that they perform correctly.
6. Open the Email Template Administration Web pages at the following URL:

   `http://<`*machine_name*`>.<`*domain_name*`>/rlmanager/index.jsp`

Troubleshooting the security settings

If you encounter any issues with the tests:

- To undo one or more of the changes that you made to the security settings, re-run the IIS Lockdown Tool.
- To disable the URLScan tool, remove the URLScan ISAPI filter from the IIS server. After you make this change, stop and restart the World Wide Web Publishing Service for the change to take effect.

Index

A

Acrobat Reader 302
Active Directory 307, 310
adapting
  adding servers 113
  co-locating servers 113
  deployment scenarios 111
  multi-processor machines 112
  servers and domains 112
Adjunct Route Capacity 49, 269, 270
adjunct routing requirements, summarized 332
ADU persistence 94
ADU server 93, 102
Advanced Reporting Tools
  see Operational Analyst
Advocate
  see Business Advocate
agent desktop 29
agent desktop applications
  Avaya Agent 30
  browsers 65
  operating systems 65
  prerequisites 65
agent states 268
AgentGroupCCT 370
agents, remote 79
AIX
  configuration requirements 223, 229
  configuration settings 229
  disk space requirements 227
  IBM HTTP Server 282, 290
  Java SDK 293
  locales 228
  maintenance level 226
  patches 226
  physical address 213
  SDK compiler 302
  setting up 226
  time synchronization 92
  verifying DNS resolution 241
  web server 290
  windowing environment 229
AIX VisualAge compiler 302
Alarm server 94
APP_CTL_HEAP_SZ 263
APPLHEAPSZ 263
applications
  Citrix 68, 233
applications, time zones 86
Aspect
  administration 357
  requirements 271
  support 271
Aspect Server Topology 357
Attribute server 99
Avaya Agent
  about 30
  Citrix 68, 232, 233
  Citrix interfaces 235
  desktop 29
  hardware requirements 204
Avaya Agent Web Client 30
  deployment guidelines 188
  deployment summary 189
  hardware requirements 205
  IBM Websphere 293
  required software 66
Avaya Computer Telephony 30
Avaya Definity 267
  configuring redundant CTI links 334
  configuring the switch in an ACD environment . 336
  switch configuration 322, 342
  switch setup 334
Avaya FTSE 34
Avaya Full Text Search Engine 34
Avaya IC for Siebel 7
  about 34
  required software 63
Avaya Interactive Response 279
Avaya OA
  see Operational Analyst

B

bandwidth, remote agents 80
binary sort order 252
BlindCCT 368
browsers
  agent desktop applications 65
  customers 69
  Design & Administration Tools 64
  exceptions 71
  Internet Explorer 217
bufferpool, DB2 263
Business Advocate

about . . . 32
configuring SQL Server . . . 312
configuring SQL Server for Thai . . . 315
configuring Windows for Thai . . . 311
data center . . . 181
databases . . . 84, 102, 249
deployment
high volume voice . . . 121
multi-channel . . . 135
multi-site . . . 160, 164, 181
voice only . . . 118
Event Collector server . . . 106
installing MSMQ . . . 310
Logical Resource Manager . . . 102
multi-instance . . . 164
nethome . . . 313
Oracle
client . . . 319
components . . . 316
configuring . . . 315
Net8 . . . 319
NTS authentication . . . 318
tablespaces . . . 316
user . . . 317
prerequisites . . . 62
requirements . . . 62
Resource Manager server . . . 102
resource store . . . 84
servers . . . 60, 101
setting up Active Directory . . . 307, 310
setting up MSMQ . . . 306
single instance . . . 160
supported exceptions . . . 305
system store . . . 84
TSA server . . . 103
user . . . 314
WAA server . . . 104
Workflow server . . . 97

C

C for AIX compiler . . . 302
call control tables . . . 377
CallCenter, Aspect . . . 271
CallCenterQ
Citrix . . . 232
cataloguing DB2 client . . . 264
CCQ
see CallCenterQ
CCQ database . . . 84
changing
adding servers . . . 113
co-locating servers . . . 113
deployment scenarios . . . 111
multi-processor machines . . . 112
servers and domains . . . 112
channels
email . . . 31
outbound telephony . . . 31
telephony . . . 30
web . . . 31
chat
co-locating servers . . . 113
DUStore server . . . 99
multi-site . . . 170
server guidelines . . . 99
single site . . . 138
Checkpoint . . . 95
CIRS server . . . 100
Citrix
Avaya Agent . . . 232
Avaya IC servers . . . 232
clients . . . 232
connectors . . . 232
deployment . . . 231
Design & Administration Tools . . . 232
exceptions . . . 234
integration limitations . . . 237
interfaces
about . . . 235
Web . . . 235
licensing . . . 234
multiple applications . . . 232
software . . . 68, 233
support . . . 231
Website . . . 232
client applications . . . 91
Client to connection ratio . . . 86
co-locating servers . . . 113
Communication Manager
CVLAN client . . . 270
requirements . . . 268
support . . . 267
communication protocol . . . 78
compiler
AIX . . . 302
SDK . . . 302
compilers for SDK . . . 302
components
about . . . 27
agent desktop applications . . . 29
Avaya Agent . . . 30
Avaya FTSE . . . 34
Avaya IC for Siebel 7 . . . 34
Business Advocate . . . 32
Computer Telephony for IC . . . 30
Content Analyzer . . . 33
core servers . . . 28
Database Designer . . . 29
deployment on Citrix . . . 231

Design & Administration Tools . . . 28
Email Management . . . 31
IC Manager . . . 28
optional databases . . . 45
Oracle, Business Advocate . . . 316
Outbound Contact Management . . . 31
performance . . . 76
required databases . . . 45
Telephony . . . 30
time zones . . . 86
Web Management . . . 31
Workflow Designer . . . 29
Computer Telephony . . . 30
configuration parameters
IBM HTTP server . . . 291
Sun Java System Web server 6.0 . . . 287
Sun Java System Web server 6.1 . . . 288
configuration parameters, DB2 . . . 263
configuration, network . . . 239
configuring
binary sort order . . . 252
database machine . . . 84
DB2 . . . 262
IBM WAS . . . 294
IIS 6.0 . . . 284
IIS 6.0 for Voice Chat . . . 286
Intel NetMerge Call Processing Software . . . 277
network . . . 78
POP3 servers . . . 297
SMTP servers . . . 297
configuring SQL Server for Thai . . . 315
configuring Windows for Thai . . . 311
connections
VPN . . . 79
connections, network . . . 79
connectors
Citrix . . . 232
contacts, volume . . . 77
Content Analyzer
about . . . 33
prerequisites . . . 55
required software . . . 54
servers . . . 54
supported languages . . . 33
CONVERSANT System for IVR . . . 279
core servers
about . . . 28, 43
CT Connect, see Intel NetMerge Call Processing Software
Customer HTML Chat Client . . . 70
Customer Interaction Repository . . . 84, 246
customer requirements, browsers . . . 69
customization, workflows . . . 96
CVLAN client . . . 270

D

data center . . . 174, 181
Data server . . . 94
database tables . . . 86
guidelines . . . 94
location . . . 85
database clients
requirements . . . 251
supported . . . 250
Database Designer
about . . . 29
prerequisites . . . 64
database machine . . . 85
databases
about . . . 84, 246
Business Advocate . . . 84, 102, 249
CCQ . . . 84
client location . . . 251
clients . . . 250
connection pool . . . 86
Customer Interaction Repository . . . 84
DB2 . . . 261
DB2 client . . . 264
DB2 server . . . 262
Dialer . . . 84
IC Repository . . . 84
login requirements . . . 249
machine . . . 84
Operational Analyst historical . . . 85
Operational Analyst real-time . . . 85
optional . . . 45
Oracle . . . 255
Oracle client . . . 261
Oracle server . . . 256
prerequisites . . . 46
required . . . 45
servers . . . 84, 249
setting up . . . 245
Siebel 7 . . . 85
SQL Server . . . 252
supported . . . 45, 246
date/time . . . 86
DB2
bufferpool . . . 263
cataloguing client . . . 264
client . . . 264
configuration parameters . . . 263
configuring . . . 262
fix pack level . . . 262
patches . . . 262
registry variables . . . 263
server . . . 262
setting up . . . 261

tablespace . . . 264
DB2_INDEX_2BYTEVARLEN . . . 263
DB2_RR_TO_RS . . . 263
DB2_STRIPED_CONTAINERS . . . 263
DB2COMM . . . 263
DBMS . . . 245, 246
default gateway . . . 240
Definity
CVLAN client . . . 270
requirements . . . 268
Service Observing . . . 337
support . . . 267
deployment
adapting scenarios . . . 111
adding servers . . . 113
additional servers and domains . . . 112
Business Advocate
high volume voice . . . 121
multi-channel . . . 135
multi-site . . . 160, 164, 181
voice only . . . 118
Citrix . . . 231
co-locating servers . . . 113
components . . . 27, 76
concurrent users . . . 77
Data server . . . 94
database servers . . . 85
Email Management . . . 100
Event Collector server . . . 108
examples . . . 111, 143
multi-processor machines . . . 112
multi-site
chat and email . . . 170
multi-channel . . . 152
multi-channel data center . . . 174
voice only . . . 144
network
communication protocol . . . 78
connections . . . 79
firewall . . . 82
multiple cards . . . 81
remote agents . . . 79
security . . . 78
network configuration . . . 78
performance factors . . . 76
planning . . . 75
server performance . . . 200
servers . . . 88
single site
chat and email . . . 138
multi-channel . . . 125, 130
voice only . . . 114
Telephony . . . 98
volume of contacts . . . 77
Web Management . . . 100
deployment scenarios
Avaya Agent Web Client . . . 187
basic . . . 191
clustered . . . 192
load balancing . . . 194
multiple cell . . . 196
Design & Administration Tools
about . . . 28
browsers . . . 64
Citrix . . . 232
Database Designer . . . 29
hardware requirements . . . 203
IC Manager . . . 28
operating systems . . . 64
other software . . . 64
Workflow Designer . . . 29
Dialer database . . . 84
Dialing Kernel server . . . 101
Directory server . . . 94
disk space . . . 202
AIX . . . 227
Solaris . . . 221
distribution, servers . . . 201
DMZ . . . 82
DNS
unresolved . . . 242
verifying on AIX . . . 241
verifying on Solaris . . . 241
verifying on Windows . . . 240
verifying resolution . . . 240
documentation
online . . . 26
prerequisites . . . 302
Readme file . . . 25
domain name system . . . 240
domains
agent . . . 93, 108
DNS . . . 82
Event Collector server . . . 105
logical partitioning . . . 90
naming convention . . . 90
Outbound Contact . . . 101
DUStore server
chat . . . 99
email . . . 100
voice . . . 99

E

EAS . . . 268
Edify Interactive Voice Response . . . 279
EDU persistence . . . 95
EDU server . . . 95
educational services . . . 21
email

co-locating servers . . . 113
Content Analyzer . . . 33
DUStore server . . . 100
EDU server . . . 95
multi-site . . . 170
single site . . . 138
email channel
Workflow server . . . 97
Email Management
about . . . 31
configuring firewall . . . 298
deployment . . . 100
email servers . . . 297
POP3 servers . . . 297
prerequisites . . . 55
required software . . . 54
server guidelines . . . 100
servers . . . 54
SMTP servers . . . 297
Email server . . . 100
enabling TCP/IP networking . . . 239
Ericsson
requirements . . . 276
support . . . 276
Event Collector Bridge . . . 107
Event Collector server . . . 105
examples
Business Advocate
high volume voice . . . 121
multi-channel . . . 135
multi-site . . . 160, 164, 181
voice only . . . 118
deployment scenarios . . . 111, 143
multi-site
chat and email . . . 170
multi-channel . . . 152
multi-channel data center . . . 174
voice . . . 144
single site
chat and email . . . 138
multi-channel . . . 125, 130
voice . . . 114
exceptions
Business Advocate . . . 305
Citrix . . . 234
Sun JVM for customers . . . 72
supported operating systems . . . 42
exceptions, customer browsers . . . 71
experience . . . 36
Expert Agent Selection . . . 268
ExternalCCT . . . 366

F

factors, performance . . . 76
failover
ADU server . . . 93
capacity . . . 113
Event Collector server . . . 108
Operational Analyst . . . 107
Resource Manager server . . . 102
servers . . . 201
TSA server . . . 103
failover, CTI . . . 334
failure
server guidelines . . . 93
finding IP address . . . 240
firewall . . . 82
communication through . . . 83
deployment outside . . . 83
DNS domains . . . 82
Email Management . . . 298
For . . . 234
Forte Developer . . . 302
FQDN . . . 240
FTSE
see Avaya FTSE
fully qualified domain name . . . 240

G

guidelines
ADU server . . . 93
AIX configuration . . . 223, 229
AIX disk space . . . 227
Alarm server . . . 94
Attribute server . . . 99
Avaya Agent Web Client . . . 188
Business Advocate databases . . . 102
Business Advocate servers . . . 101
Business Advocate workflows . . . 104
chat channel servers . . . 99
CIRS server . . . 100
client applications . . . 91
components . . . 76
concurrent users . . . 77
core servers . . . 93
Data server . . . 94
database files . . . 85
database server . . . 85
database tables . . . 86
Directory server . . . 94
DUStore server . . . 99, 100
EDU server . . . 95
email channel servers . . . 100
Email server . . . 100
Event Collector Bridge . . . 107
Event Collector server . . . 105
firewall . . . 82
ICM server . . . 100

licensing . . . 91
logical partitioning . . . 90
Logical Resource Manager . . . 102
machine speed . . . 201
network
communication protocol . . . 78
connections . . . 79
multiple cards . . . 81
remote agents . . . 79
security . . . 78
Notification server . . . 96
Operational Analyst failover . . . 107
Operational Analyst servers . . . 104
ORB server . . . 95
Outbound Contact servers . . . 101
physical partitioning . . . 90
Report server . . . 96
Resource Manager server . . . 102
server failure . . . 93
server naming . . . 89
server partitioning . . . 89
servers . . . 88
Solaris configuration . . . 223
Solaris disk space . . . 221
Telephony server . . . 98
time synchronization . . . 91
TSA server . . . 103
TSQS server . . . 98
voice channel servers . . . 98
volume of contacts . . . 77
WAA server . . . 104
Web License Manager . . . 91
Web Management servers . . . 100
Workflow server . . . 96
gvxxxxxxxxxx Get One eDU Value . . . 384

H

hardware . . . 204
Avaya Agent . . . 204
Avaya Agent Web Client . . . 205
Design & Administration Tools . . . 203
machine speed . . . 201
requirements . . . 199
servers . . . 201
Host ID
See physical address
Hosts file . . . 242
HRQ
Citrix . . . 232
HTML Chat Client . . . 70
hunt groups, defining . . . 331

I

IBM AIX . . . 226
IBM DCE . . . 275
IBM HTTP Server
about . . . 290
configuration parameters . . . 291
IBM Logical Partition technology . . . 202
IBM WAS . . . 303
configuring . . . 294
IBM WebSphere . . . 303
IBM Websphere
about . . . 293
IBM WebSphere Voice Response . . . 279
IC Manager
about . . . 28
Citrix . . . 232
multi-processor machines . . . 112
prerequisites . . . 64
time zones . . . 86
IC Repository . . . 84, 246
ICM server . . . 100
IIS 5.0
Lockdown Tool . . . 284
security . . . 284
security patches . . . 283
setting up . . . 283
IIS 6.0
configuring . . . 284
configuring ISAPI extensions . . . 285
mime types . . . 286
security . . . 284
Voice Chat . . . 286
IIS Lockdown Tool
about . . . 284, 411
downloading . . . 412
IIS Lockdown Wizard
see IIS Lockdown Tool
IMAP . . . 299
implementation roles . . . 36
installing
AIX maintenance level . . . 226
AIX patches . . . 226
database clients . . . 250
database servers . . . 249
DB2 client . . . 264
DB2 server . . . 262
DB2 version . . . 262
IIS 5.0 security patches . . . 283
IIS Lockdown Tool . . . 412
Internet Explorer . . . 217
license file . . . 207
MSMQ . . . 310
Oracle client . . . 261

Oracle server . . . 256
Solaris patches . . . 222
SQL Server . . . 253
SQL Server Client . . . 254
SQL Server service pack . . . 254
Windows 2000 service packs . . . 216
Windows XP Professional service packs . . . 217
Intel NetMerge Call Processing Software
configuring . . . 277
interaction
ADU server . . . 93
CIRS server . . . 100
DUStore server . . . 99, 100
EDU server . . . 95
ICM server . . . 100
Outbound Contact servers . . . 101
time synchronization . . . 91
TSQS server . . . 98
interfaces
Citrix . . . 235
Internet Explorer
about . . . 217
configuring Microsoft JVM . . . 219
downloading . . . 218
encoding . . . 220
JVM plugin . . . 218
Internet Information Server . . . 283
Intervoice TRM . . . 279
IP address . . . 240
iPlanet . . . 287
ISAPI extensions, IIS 6.0 . . . 285
IVR
Avaya Interactive Response . . . 279
CONVERSANT System for IVR . . . 279
Edify Interactive Voice Response . . . 279
IBM WebSphere Voice Response . . . 279
Intervoice TRM . . . 279
Periphonics . . . 279
IVRs, supported . . . 279

J

Java SDK
AIX . . . 293
Solaris . . . 292
versions . . . 292
Windows . . . 292
Java Virtual Machine
configuring Microsoft JVM . . . 219
Java Virtual Machine plugin . . . 218

L

LAN . . . 79
languages
Traditional Chinese . . . 25
languages, Content Analyzer . . . 33
languages, supported . . . 24
latency, remote agents . . . 81
license file
obtaining . . . 207
prerequisites . . . 207
replacing . . . 211
requesting . . . 209
updating . . . 210
licensing
Citrix . . . 234
guidelines . . . 91
limitations
ADU data collection . . . 106
ADU server . . . 93
Business Advocate databases . . . 102
Citrix . . . 234
Citrix integration . . . 237
EDU . . . 95
Resource Manager server . . . 102
Sun Java System Web Server . . . 287
Traditional Chinese . . . 25
Link 5c . . . 274
Locale
AIX . . . 229
Solaris . . . 224
locales, AIX . . . 228
localhost . . . 242
location
Alarm server . . . 94
Attribute server . . . 99
client applications . . . 91
core servers . . . 93
Data server . . . 85, 94
database client . . . 251
database files . . . 85
Directory server . . . 94
Email server . . . 100
Event Collector server . . . 105
Notification server . . . 96
ORB server . . . 95
Report server . . . 96
Resource Manager server . . . 102
servers . . . 98, 99, 100
Telephony server . . . 98
TSA server . . . 103
WAA server . . . 104
Web License Manager . . . 91
Web Management servers . . . 100
Workflow server . . . 96
log file allocations . . . 202
logical partitioning . . . 90
Logical Resource Manager
ADU server . . . 102

guidelines . . . 102
Lotus Sametime . . . 303
LPAR . . . 202

M

machine speed . . . 201
maintenance level, AIX . . . 226
MakeCallCCT . . . 362
MAXAPPLS . . . 263
MAXLOCKS . . . 263
MD110, Ericsson . . . 276
media
email . . . 31
outbound telephony . . . 31
telephony . . . 30
web . . . 31
Meridian
requirements . . . 274
support . . . 273
Meridian MAX . . . 274
Message Queuing services
see MSMQ
Microsoft
Internet Explorer . . . 217
Internet Information Server 5.0 . . . 283
SQL Server . . . 252
Windows . . . 216
Windows XP Professional . . . 217
Microsoft JVM plugin
about . . . 218
configuring Internet Explorer . . . 219
mime types, IIS 6.0 . . . 286
minimum hardware requirements . . . 204
MSMQ
Active Directory . . . 307, 310
installing . . . 310
setting up . . . 306
multi-channel
multi-site . . . 152
multi-site data center . . . 174
single site . . . 125, 130
multi-instance, Business Advocate . . . 164
multiple network cards . . . 81
multi-processor machines . . . 112
multi-site
Business Advocate
data center . . . 181
multi-instance . . . 164
single instance . . . 160
chat and email . . . 170
deployment scenarios . . . 143
multi-channel . . . 152
multi-channel data center . . . 174
voice . . . 144

N

naming, domains . . . 90
naming, servers . . . 89
Net8 . . . 319
nethome directory . . . 313
Netscape . . . 72
NetWare . . . 239
network . . . 100
bandwidth for remote agents . . . 80
communication protocol . . . 78
configuration . . . 78, 239
connections . . . 79
data server location . . . 94
firewall . . . 82
multiple cards . . . 81
multiple network cards . . . 81
Novell Netware . . . 239
security . . . 78
VPN . . . 79
network cards, multiple . . . 81
network configuration
database machine . . . 84
servers . . . 200
Network Interface Cards . . . 81
networks
TCP/IP . . . 239
topology . . . 78
newtrans New Transaction . . . 385, 386, 388
NICs . . . 81
Nortel
Meridian . . . 272
support . . . 272
Symposium . . . 272
Nortel Meridian
Intel NetMerge Call Processing Software . . . 277
requirements . . . 274
Notification server . . . 96
Novell NetWare . . . 239
nslookup . . . 241, 242
number, concurrent users . . . 77

O

obtaining, license file . . . 207
ODBC, database tables . . . 86
online documentation . . . 26
operating systems
AIX . . . 226
Citrix . . . 68, 231, 233
exceptions . . . 42
setting up . . . 215, 305
Solaris . . . 220
supported . . . 215, 305

Windows . . . 216
Windows 2000 . . . 216
Windows Server 2003 . . . 217
Windows XP Professional . . . 217
Operational Analyst . . . 35
Event Collector . . . 105
Event Collector Bridge . . . 107
failover . . . 107
historical database . . . 85
real-time database . . . 85
server guidelines . . . 104
optional databases . . . 45
Oracle
Business Advocate
client . . . 319
components . . . 316
configuring . . . 315
Net8 . . . 319
NTS authentication . . . 318
tablespaces . . . 316
user . . . 317
client . . . 261
patches . . . 256
server . . . 256
setting up . . . 255
Technet . . . 261
ORB server . . . 95
Outbound Contact
about . . . 31
prerequisites . . . 58
required software . . . 56
servers . . . 57, 101
Telephony exceptions . . . 266
time zones . . . 86
overview . . . 23

P

partitioning, servers . . . 89
patches
AIX . . . 226
DB2 . . . 262
Oracle . . . 256
performance
components . . . 76
factors . . . 76
volume of contacts . . . 77
performance dependencies . . . 200
Periphonics . . . 279
physical address, identifying . . . 208
physical partitioning . . . 90
physical redundancy . . . 113
planning
components . . . 76
concurrent users . . . 77
deployment . . . 75
experience . . . 36
network
communication protocol . . . 78
connections . . . 79
firewall . . . 82
multiple cards . . . 81
remote agents . . . 79
security . . . 78
network configuration . . . 78
performance factors . . . 76
servers . . . 88
volume of contacts . . . 77
POP3 . . . 100, 297
POP3 servers . . . 297
Post Office Protocol . . . 297
prerequisites
about . . . 41
agent desktop applications . . . 65
Aspect . . . 271
Avaya IC for Siebel 7 . . . 63
Business Advocate . . . 62
Citrix . . . 68, 233
Communication Manager . . . 268
Content Analyzer . . . 55
core servers . . . 43
databases . . . 46
Definity . . . 268
Design & Administration Tools . . . 64
Email Management . . . 55
Ericsson . . . 276
experience . . . 36
license file . . . 207
Nortel Meridian . . . 274
Outbound Contact . . . 58
Telephony servers . . . 48
Web Management . . . 53

R

RAM, database clients . . . 251
RDBMS . . . 245
Readme file . . . 25
registry variables, DB2 . . . 263
remote agents
bandwidth . . . 80
latency . . . 81
VPN . . . 79
replacing, license file . . . 211
Report server . . . 96
requesting
license file . . . 209
replacement license file . . . 211
required databases . . . 45
required experience . . . 36

required hardware 204
required software
agent desktop applications 65
Avaya Agent Web Client 66
Avaya IC for Siebel 7 63
Business Advocate 60
requirements
about 41
Aspect 271
Avaya IC for Siebel 7 63
browsers 69
Citrix 68, 233
Content Analyzer 55
core servers 43
database clients 251
database login 249
databases 46
Definity 268
Design & Administration Tools 64
Email Management 55
Ericsson 276
hardware 199
Meridian 274
Nortel Meridian 274
Outbound Contact 58
Symposium 275
Telephony 48
Web Management 53
Resource Manager server 102
resource store 84
roles, implementation 36
RouteCCT 367

S

Sametime 303
Scheduled Call, servers 52
SDK compiler
AIX 302
Solaris 302
SDK compilers 302
security
accounts 36
databases 249
firewall 82
IIS 5.0 284
IIS 6.0 284
IIS Lockdown Tool 411
license file 207
network 78
passwords 36
patches, IIS 5.0 283
patches, Solaris 222
server location 93
server partitioning 89
validation 202
Send Data command
subtypes 381-388
servers
about 28
ADU 93
Alarm 94
Attribute 99
Business Advocate 60
guidelines 101
Logical Resource Manager 102
Resource Manager 102
TSA 103
WAA 104
chat channel 99
CIRS 100
Citrix 232
Content Analyzer 54
core 43
core server guidelines 93
Data 94
database guidelines 85
Dialing Kernel 101
Directory 94
distribution 201
DUStore 99, 100
EDU 95
Email 100, 297
email channel 100
Email Management 54
failover 201
failure 93
guidelines 88
hardware requirements 201
ICM 100
interaction
ADU server 93
CIRS server 100
DUStore server 99, 100
EDU server 95
ICM server 100
Outbound Contact 101
TSQS server 98
location 85, 98, 99, 100
Alarm server 94
Attribute server 99
client applications 91
Data server 94
Directory server 94
Email server 100
Notification server 96
ORB server 95
Report server 96
Telephony server 98
Web License Manager 91

Web Management . . . 100
Workflow server . . . 96
machine speed . . . 201
machines . . . 200
Microsoft Internet Information . . . 283
naming . . . 89
Notification . . . 96
Operational Analyst . . . 104
Event Collector . . . 105
Event Collector Bridge . . . 107
ORB . . . 95
Outbound Contact . . . 57, 101
partitioning
guidelines . . . 89
logical . . . 90
physical . . . 90
performance . . . 200
platform considerations . . . 200
POP3 . . . 297
prerequisites . . . 43, 48, 58
Report . . . 96
Scheduled Call . . . 52
SDK compilers . . . 302
SMTP . . . 297
Telephony . . . 47, 57, 98
time synchronization . . . 91
time zones . . . 86
TSQS . . . 98
voice channel . . . 98
Voice Chat . . . 52
web . . . 281
Web License Manager . . . 91
Web Management . . . 52, 54, 100
Workflow . . . 96
Service Observing . . . 337
service packs
SQL Server . . . 254
Windows 2000 . . . 216
Windows XP Professional . . . 217
setting up
AIX . . . 226
databases . . . 245
DB2 . . . 261
email servers . . . 297
Intel NetMerge Call Processing Software . . . 277
Oracle . . . 255
Solaris . . . 220
third party applications . . . 301
Tomcat . . . 303
web servers . . . 281
Windows . . . 216
Siebel 7 database . . . 85
Siebel, Avaya IC for . . . 34, 63
Simple Mail Transport Protocol . . . 297
single instance, Business Advocate . . . 160
single site
Business Advocate
high volume voice . . . 121
multi-channel . . . 135
voice only . . . 118
chat and email . . . 138
deployment scenarios . . . 111
multi-channel . . . 125, 130
voice . . . 114
Sizing Tool . . . 112
skill groups, defining . . . 331
SMTP . . . 100
SMTP servers . . . 297
software
AIX . . . 226
Citrix . . . 68, 231, 233
databases . . . 245, 246
DB2 . . . 261
Design & Administration Tools . . . 64
email servers . . . 297
exceptions . . . 266
Internet Explorer . . . 217
Oracle . . . 255
Sametime . . . 303
SDK compilers . . . 302
Solaris . . . 220
SQL Server . . . 252
SQL Server Client . . . 254
telephony . . . 265
web servers . . . 281
Windows . . . 216
Windows 2000 . . . 216
Windows Server 2003 . . . 217
Windows XP Professional . . . 217
Solaris
configuration requirements . . . 223
disk space requirements . . . 221
Java SDK . . . 292
patches . . . 222
physical address . . . 213
SDK compiler . . . 302
setting up . . . 220
Sun Java Web Server 6.0 . . . 282
Sun Java Web Server 6.1 . . . 282
Sun ONE Web Server . . . 282
time synchronization . . . 92
ulimit parameters . . . 224
user accounts . . . 225, 230
verifying DNS resolution . . . 241
web server . . . 287
windowing environment . . . 224
SQL Server
Business Advocate . . . 312
Client . . . 254
database tables . . . 86

installing . . . 253
service pack . . . 254
setting up . . . 252
stations, defining . . . 327
subnet mask . . . 240
Sun Forte Developer . . . 302
Sun Java System Web Server
6.0
download . . . 287
6.1
download . . . 287
limitations . . . 287
Sun Java System Web server
6.0
configuration parameters . . . 287
6.1
configuration parameters . . . 288
setting up . . . 287
Sun JVM . . . 72
Sun JVM plugin . . . 218
Sun ONE Web Server . . . 287
Sun ONE Web server . . . 287
Sun Solaris . . . 220
support
Traditional Chinese . . . 25
supported
databases . . . 45
languages . . . 24
operating systems . . . 215, 305
third party applications . . . 301
svxxxxxxxxxx Set One eDU Value . . . 387
switches
Aspect . . . 271
Communication Manager . . . 267
Definity . . . 267
Ericsson . . . 276
exceptions . . . 266
Nortel . . . 272
TSA server . . . 103
Symposium
requirements . . . 275
support . . . 273
system store . . . 84

T

tablespace, DB2 . . . 264
Tardis 2000 . . . 92
TCP/IP . . . 78
TCP/IP networking . . . 239
Telephony
about . . . 30
agent states . . . 268
Aspect . . . 271
Communication Manager . . . 267
Definity . . . 267
deployment . . . 98
Ericsson . . . 276
Event Collector server . . . 106
exceptions . . . 266
IVRs . . . 279
multi-site . . . 144
Nortel . . . 272
Outbound Contact Management . . . 31
prerequisites . . . 48
required software . . . 47, 56
servers . . . 47, 57
single site . . . 114
switches . . . 265
TSA server . . . 103
Telephony Queue Statistics server . . . 98
Telephony server . . . 98
Telephony Services Adaptor server . . . 103
Thai
configuring SQL Server . . . 315
configuring Windows . . . 311
third party applications . . . 301
time synchronization . . . 91
time zones . . . 86
Tomcat . . . 303
Traditional Chinese, limitations . . . 25
TransferInitCCT . . . 364
troubleshooting
Event Collector server . . . 108
license files . . . 213
unresolved DNS . . . 242
TSA server . . . 103
TSQS server . . . 98

U

ulimit parameters
Solaris . . . 224
uname . . . 213
Universal Call ID (UCID) . . . 356
UNIX . . . 220, 226
updating, license file . . . 210
user accounts, Solaris . . . 225, 230
users, concurrent . . . 77

V

validation . . . 202
Vector Directory Numbers (VDNs), defining . . . 325
vectors, defining . . . 326
verifying DNS resolution
AIX . . . 241
Solaris . . . 241
Windows . . . 240
voice

adding server machines . . . 113
DUStore server . . . 99
multi-site . . . 144
single site . . . 114
Voice Chat
IIS 6.0 . . . 286
servers . . . 52
volume of contacts . . . 77
VPN . . . 79

W

WAA server . . . 104
WAN . . . 79
Web Advocate Adaptor server . . . 104
Web interface, Citrix . . . 235
Web License Manager . . . 91, 210, 211, 212
Web Management
about . . . 31
binary sort order . . . 252
Citrix . . . 232
deployment . . . 100
prerequisites . . . 53
required software . . . 51
Scheduled Call . . . 52
server guidelines . . . 99
servers . . . 52, 54, 100
web servers . . . 281
Web Self-Service
about . . . 34
web servers
AIX . . . 290
Avaya Agent Web Client . . . 293
IBM HTTP Server . . . 290
IBM Websphere . . . 293
Solaris . . . 287
Sun Java System Web server . . . 287
Windows 2000 . . . 283
WebLM . . . 91
WebQ
web servers . . . 281
Website
Citrix . . . 232
WebSphere . . . 66
Websphere . . . 303
Windowing environment . . . 224, 229
Windows
Citrix . . . 68, 233
IIS 5.0 . . . 282
Java SDK . . . 292
physical address . . . 213
setting up . . . 216
time synchronization . . . 92
verifying DNS resolution . . . 240
Windows 2000
Active Directory . . . 310
MSMQ . . . 306
service packs . . . 216
support . . . 216
web server . . . 283
Windows Server 2003
Active Directory . . . 307
JVM . . . 218
support . . . 217
Windows XP Professional . . . 217
JVM . . . 218
service packs . . . 217
Workflow Designer
about . . . 29
prerequisites . . . 64
Workflow server . . . 77, 96
Business Advocate . . . 97
email qualification . . . 97
workflows
Business Advocate . . . 104
customization . . . 96

X

X-Windows . . . 224, 229