Avaya Aura® Communication Manager Overview and Specification

Release 6.3
03-604233
Issue 4
June 2014

© 2014 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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 to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.
- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can 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 Toll 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 Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 7
- Purpose 7
- Intended audience 7
- Document changes since last issue 7
- Related resources 7
  - Documentation 7
  - Training 10
  - Avaya Mentor videos 11
- Support 12
- Warranty 12

Chapter 2: Communication Manager overview 13
- Feature Description 13
  - Port network and gateway connectivity 14
  - Trunk connectivity 14
  - Communication Manager public networking and connectivity 15
  - Communication Manager intelligent networking 15
  - Communication Manager data interfaces 16
  - Call Center 16
  - Computer Telephony Integration 17
  - Communication Manager mobility 17
  - Collaboration 18
  - Communication Manager call routing 19
  - Telecommuting and Remote Office 19
  - Communication Manager localization 20
  - Communication Manager customization features 20
- New in this release 20

Chapter 3: Interoperability 23
- Product compatibility 23
- Server compatibility 23
- Operating system compatibility 24
- Supported endpoints 25

Chapter 4: Performance specification 27
- Capacity and scalability specification 27
- Traffic specification 29
- Survivability specification 30
- Dial plan specification 30
- Call Admission Control specification 31

Chapter 5: Security specification 33
- Communication Manager security, privacy, and safety 33
  - RTP encryption 34
  - Timers and key exchange details 34
- Port utilization 35

Chapter 6: Licensing requirements 37
- Virtual appliance licensing on VMware 37

Centralized Licensing..... 38
Chapter 7: Virtualization specification..... 39
Glossary..... 41
Index..... 43

Chapter 1: Introduction

Purpose

This document describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Intended audience

This document is intended for anyone who wants to gain a high-level understanding of the product features, functionality, capacities, and limitations within the context of solutions and verified reference configurations.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Updated the *New in this release* section.
- Updated the *Virtualization specification* section.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Security Design	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Solution Design Considerations and Guidelines	Describes the Avaya Aura® solution, IP and SIP telephony product deployment, and network requirements for integrating IP and SIP telephony products with an IP network.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Implementation		
Deploying Avaya Aura® Communication Manager on System Platform, 18-604394	Describes the implementation instructions for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Upgrading to Avaya Aura® Communication Manager 6.3	Provides the instructions to upgrade Communication Manager to a specific release.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Alarms for Avaya Aura® Communication Manager	Provides procedures to monitor, test, and maintain an Avaya server or Media Gateway.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Title	Description	Audience
Maintenance Commands for Avaya Aura® Communication Manager	Provides information to monitor, test, and maintain hardware components of an Avaya servers or Gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Server Alarms	Provides procedures to monitor, test, and maintain an Avaya servers.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Denial Events	Describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Toll Fraud and Security Handbook	Describes the security risks and measures that can help prevent external telecommunications fraud involving Avaya products.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel

Title	Description	Audience
Avaya Aura® Communication Manager Screen Reference	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Call Center Elite Overview and Specification	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales Engineers, Solution Architects, Support Personnel
What's New in Avaya Aura® Release 6.2 Feature Pack 4	Describes the new features for the current release of Avaya Aura®.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that are requested by specific customers for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
Docu00158	Whats New in Avaya Aura® Release 6.2 Feature Pack 2
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	

Course code	Course title
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
4U00115I, 4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Communication Manager overview

Avaya Aura® Communication Manager is the open, highly-reliable and extensible IP Telephony foundation on which Avaya delivers intelligent communications to large and small enterprises. Communication Manager effectively scales from less than 100 users up to 36,000 users on a single system.

Communication Manager is an important component of the Avaya Aura architecture, which consolidates several components into a holistic package that enterprises need for Unified Communications. Communication Manager software is part of all the Avaya Aura® editions. This software is available with a single-user licensing fee.

Communication Manager provides centralized call control for a distributed network of gateways and a wide range of analog, digital, and IP-based communication devices. Communication Manager comes with several built-in mobility applications, call center features, advanced conference calling, and E911 capabilities.

With support for SIP, H.323, and other industry-standard communications protocols, Communication Manager provides centralized voice mail and attendant operations to organizations and call centers, across multiple locations.

Communication Manager can be configured as an evolution server or a feature server. Communication Manager configured as an evolution server uses the full-call model to provide Communication Manager features to SIP and non-SIP endpoints. As a feature server, Communication Manager only supports SIP endpoints registered to Avaya Aura® Session Manager. Communication Manager configured as a feature server uses the IP Multimedia Subsystem (IMS) half-call model for full application sequencing.

Feature Description

Communication Manager offers a wide variety of basic and advanced telephony features that include the following:

- Port network and gateway connectivity
- Trunk connectivity
- Public networking and connectivity
- Intelligent networking
- Data interfaces
- Call center feature support

- Computer telephony integration
- Automatic call distribution
- Call routing
- Telecommuting and remote office
- Localization support
- Interfaces for feature customizing

Port network and gateway connectivity

Communication Manager supports the following connectivity features:

- Circuit-switched network
- Branch gateway control for Avaya Branch gateways
- Separation of bearer and signaling

For more information about port network and gateway connectivity, see *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

Trunk connectivity

Communication Manager supports the following types of trunks:

- DS1 trunks
- H.323 trunks
- IP trunks
- SIP trunks
- Auxiliary trunks
- Central Office (CO) trunks
- Direct Inward Dialing (DID) trunks
- Direct Inward/Outward Dialing trunks
- E911 CAMA trunks
- Foreign Exchange (FX) trunks
- ISDN trunks
- Release Link trunks (RLT)
- Tie trunks
- Wide Area Telecommunications Service (WATS) trunks

For more information about trunks, see *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

Communication Manager public networking and connectivity

Communication Manager supports the following public networking features:

- Caller ID on analog trunks
- Caller ID on digital trunks
- Flexible billing
- Local exchange trunks
- QSIG Supplementary Service for advice of call charges

For more information about public networking trunks, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Related topics:

Trunk connectivity on page 14

Communication Manager intelligent networking

Communication Manager Intelligent networking features include:

- VoIP network quality monitoring
- Multiple switch configuration
- Call routing over tandem network
- Extension number portability
- IP support for audio and video calls
- Standards-based control for branch gateways, Avaya 8XXX server, HP ProLiant DL360 G7 server, and Dell™ PowerEdge™ R610 server
- QSIG Unicode support
- Uniform dial plan for extension-to-extension dialing between private-switching systems

For more information about intelligent networking features, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Communication Manager data interfaces

Communication Manager data interface features include:

- Administered connections
- Data call setup
- Data hot line
- Data privacy
- Data restriction
- Default dialing
- IP asynchronous links
- Multimedia Application server interface
- Multimedia calling
- Advice of charge information for BRI endpoints

For more information about data interface features, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Call Center

Avaya Aura® Call Center applications provide a fully integrated telecommunications platform to meet call center needs of customers.

Using Call Center applications, such as Avaya Aura® Call Center Elite, customers can:

- Reach out through outbound dialing
- Combine historic and real-time contextual customer information
- Optimize agent utilization and productivity
- Enhance supervisor performance to deliver superior customer experience

For description of Call Center features, see *Avaya Aura® Call Center Feature Reference*.

Communication Manager Automatic Call Distribution

Automatic Call Distribution (ACD) is the basic building block for call center applications. With ACD, you can:

- Distribute incoming calls efficiently and equitably among available agents
- Direct incoming calls to the first idle or most idle agent within a group of agents
- Integrate call center applications with Avaya Aura® Call Center Elite for effective handling of calls

For more information, see *Avaya Aura® Call Center Elite Overview and Specification* and *Avaya Aura® Call Center Elite Feature Reference*.

Computer Telephony Integration

With Computer Telephony Integration (CTI), you can control Communication Manager features by using external applications and integrate a customer database with call control features.

Avaya Computer Telephony is a server software that integrates the premium call control features of Communication Manager with customer information. Avaya Computer Telephony delivers the architecture and platform that supports call center applications, along with application programming interfaces (APIs).

Communication Manager mobility

Communication Manager supports the following mobility features:

- Personal Station Access (PSA)
- Automatic Customer Telephone Rearrangement (ACTR)
- Administration Without Hardware
- Avaya Extension to Cellular (EC500)
- E911 ELIN for IP wired extensions
- Avaya Wireless Telephone Solutions (AWTS)
- Terminal Translation Initialization (TTI)
- TransTalk 9000
- X-station mobility

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Collaboration

To collaborate with groups of peers, customers, and partners, Communication Manager provides collaboration features that include the following:

Conferencing:

- Abort conference
- Three-party conference
- Six-party conference
- Conference and transfer display prompts
- Toggle and swap capabilities for conference and transfer
- Group listen

Note:

Group listen is not available for IP telephones.

- Hold and unhold conference

Note:

Hold and unhold conference is not available for BRI stations or attendant consoles.

- Meet-me Conference
- Expanded Meet-me conference
- No-dial tone conference
- No-hold conference
- Select line appearance conference
- Selective conference party display
- Selective party drop
- Selective conference mute
- Enhanced SIP signaling

Multimedia calling:

- Multimedia Application Server Interface
- Multimedia call early answer on vectors and stations
- Multimedia Call Handling (MMCH)
- Multimedia call redirection to multimedia endpoint
- Multimedia data conferencing (T.120) through an ESM

- Multimedia hold, conference, transfer, and drop
- Multimedia queuing with voice announcement

Paging and intercom:

- Code calling access
- Group paging
- Automatic intercom
- Dial intercom
- Loudspeaker paging access
- Manual signaling
- Whisper page

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Communication Manager call routing

Communication Manager provides the following call routing features:

- Automatic routing
- En bloc dialing and Call Type Digit Analysis
- Generalized route selection
- Multiple location support
- Alternate facility restriction levels
- Traveling Class Marks
- Answer detection

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Telecommuting and Remote Office

Communication Manager supports the following telecommuting features:

- Redirected off-net call coverage
- Extended user administration of redirected calls (telecommuting access)
- Off-premises station
- Remote access permits authorized callers from remote locations

Communication Manager localization

Communication Manager supports a range of language features, such as administrable language displays and country-specific localization. Communication Manager localization features are:

- Administrable language displays
- Administrable loss plan
- Bellcore calling name ID
- Busy tone disconnect.
- Country-specific localization
- Multinational Locations
- QSIG support for Unicode
- World class tone detection
- XOIP Tone Detection Bypass

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Communication Manager customization features

Communication Manager provides the following interfaces for customization:

- Device and media control API
- Co-resident branch gateway
- Java telephony application programming interface (JTAPI)
- Telephony Services Application Programming Interface (TSAPI)
- Automatic Number Identification (ANI)

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

New in this release

Communication Manager Release 6.3.6 provides the following features:

- Avaya one-X® Communicator Display and Log to show E164+
- Inter-Gateway Alternate Routing for SIP endpoints
- DSP resource reduction for Avaya one-X® Communicator SIP endpoints
- Video SRTP and TLS support with Scopia 8.3
- Limit Number of Concurrent Calls
- EC500 Call Suppression enhancement
- T.38 fax during audio
- Team button enhancements
- Scopia 8.3 interoperability
- SIP undelivered call notification
- Support for increase in number of digits in call logs
- Administrable Timers for One–X Mobile VM Detection
- Delayed drop on receiving DISC
- RAS limit increased to 65%
- Full CM release string in MST trace
- Online/Offline Call Journal (Call History)
- Password complexity enhancement

For detailed information about the new features for this release, see *What's New in Avaya Aura® Release 6.2 Feature Pack 4*, 03-601818.

Chapter 3: Interoperability

Product compatibility

For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Server compatibility

Communication Manager as a template is a virtualized version that runs on System Platform. The Communication Manager template image has all the features that Communication Manager supports, whether the image is on a duplicated server or a branch server.

The following table provides the information about servers compatible with each template type.

Template type	Applications supported	Server
Survivable Core template	• Avaya Aura® Communication Manager • Avaya Aura® Communication Manager Messaging • Utility Services	• S8510 • S8800 • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R620
Survivable Remote template	• Avaya Aura® Communication Manager • Branch Session Manager • Utility Services	• S8510 • S8800 • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7

Template type	Applications supported	Server
		• HP ProLiant DL360p G8 • Dell™ PowerEdge™ R620
Main or Survivable Remote template	• Avaya Aura® Communication Manager • Avaya Aura® Communication Manager Messaging • Utility Services	• S8300D • S8510 • S8800 • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R620

Note:

Avaya no longer sells the S8800 and S8510 servers. You can only reuse the S8800 and S8510 servers with an upgrade.

For information on template capacities, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.

For information about hardware specifications, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Operating system compatibility

The following table provides information about the operating system versions compatible with the various releases of Communication Manager.

Communication Manager release	Linux version	Kernel version
6.3	Red Hat Enterprise Linux 5.8	2.6.18-348.AV04
6.2	Red Hat Enterprise Linux 5.3	2.6.18-238.AV02 XEN
6.0.1	Red Hat Enterprise Linux 5.3	2.6.18-128.AV14 XEN

Communication Manager release	Linux version	Kernel version
6.0	Red Hat Enterprise Linux 5.3	2.6.18-128.AV11 XEN
5.2.1	Red Hat Enterprise Linux 4.0	2.6.18-128.AV07 PAE

Note:

Communication Manager uses a modified version of Red Hat Enterprise Linux.

Supported endpoints

Avaya Aura® Communication Manager supports the following analog, digital and IP-based communication devices:

- Avaya IP deskphones
- Avaya one-X® IP Telephones
- Avaya 4600-Series IP Telephones
- Avaya digital deskphones and telephones
- Avaya Callmaster telephone
- Avaya DECT Handsets
- Avaya IP wireless telephones
- Avaya Attendant Console
- Avaya analog telephones
- Avaya IP conference phones
- 96x1 H.323 and 96x1 SIP Deskphones

For a complete list of supported devices, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Chapter 4: Performance specification

Capacity and scalability specification

Resource	Release 5.2.x	Release 6.0	Release 6.2	Release 6.3
SIP endpoints for general business configurations	18,000	18,000	36,000	36,000
Crisis Alert buttons for special application SA8608	250	250	750	750
Maximum number of bridges for the principal party call appearance	25	25	63	63
Maximum number of bridges for the principal party call appearance for special application SA9018	127	127	255	255
Maximum number of table entries for the IP-network-map table	500	500	4000	4000
Video-capable H.323 stations	12,000	12,000	18,000	18,000
Communication Manager servers supported by one AES Server	16	16	16	16
Overall administered trunks	12,000	24,000	24,000	24,000
Remote MWI per Extension	80	80	80	80

Resource	Release 5.2.x	Release 6.0	Release 6.2	Release 6.3
DS1 circuit packs including MM710s	522	522	522	522
Offer Limit: Administered trunks for Communication Manager as an evolution server	12,000	12,000	12,000	12,000
Offer Limit: Administered trunks for Communication Manager as a feature server	—	For Release 6.0: 12,000 **Note:** For Release 6.0.1, 24,000 trunks can be administered for Communication Manager as a feature server.	24,000	24,000
Administered trunks for Analog, ISDN, IP, and SIP trunk pool	—	24,000	24,000	24,000
Offer Limit: Simultaneous in use trunks for Communication Manager as an evolution server	7,000	7,000	12,000	12,000
Offer Limit: Simultaneous in use trunks for Communication Manager as a feature server	7,000	7,000	24,000	24,000
Port Network media processing channels	16,383	16,383	16,383	32,767
Maximum Simultaneous Calls Being Classified	600	600	600	1200
Coverage Answer Group (CAG)	1000	1000	1000	1500
Network Region and Location	250	250	250	2000

For the entire list of updated capacities, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.

Traffic specification

In Communication Manager, the processor occupancy or the server occupancy consists of:

- Static occupancy
- Call processing occupancy
- System management occupancy

Due to the fluctuating nature of system management functions, a fixed portion of the total processing capacity is assigned to system management. For all Communication Manager servers, 27% of the total processing capacity of the system is allocated to system management. If the total processor occupancy exceeds approximately 92%, all system management operations are delayed, and subsequent call attempts are rejected.

Considerations:

To ensure that the proposed solution design manages the anticipated traffic load, the Avaya Sales Factory team determines the Communication Manager CPU occupancy. Some of the considerations for calculating the traffic usage are:

- Busy Hour Call Completion (BHCC) for inbound calls.
- Call vectoring, especially for announcements that Communication Manager plays for calls in queue.
- The number of simultaneous active SIP trunks. The active SIP trunks that support calls that are in a queue have a greater impact on the Communication Manager CPU occupancy than the number of active SIP trunks that support calls being handled by agents.
- The Communication Manager release, CPU clock speed, and server duplication mode.
- Computer Telephony Integration (CTI) operations, such as monitoring, adjunct routing, and third-party call control.
- Intelligent Customer Routing (ICR) and Best Service Routing (BSR) operations.

For more information about traffic engineering and specifications, see *Avaya Aura® Communication Manager Solution Design Considerations and Guidelines*, 03-603978.

Survivability specification

Communication Manager supports two survivability options: survivable core and survivable remote.

Survivable core server

With survivable core servers, the system continues to operate in the events of network outage. A survivable core server provides survivability support to IP port networks and to Processor Ethernet for registering gateways and IP endpoints. This survivability option is available only for Communication Manager.

Survivable remote server

Survivable remote servers provide enhanced redundancy for branch gateways operating within networks. Survivable remote servers take over segments that loose connection from their primary call server and provide those segments with Communication Manager operation until the outage is resolved. A survivable remote server provides survivability support to IP and SIP telephones and to branch gateways when the connection to the core server fails. This survivability option is available for both, Communication Manager and Session Manager.

For more information about survivability options, see *Avaya Aura® Communication Manager Survivability Options*, 03-603633.

Dial plan specification

The Dial Plan feature supports intra-server dialing for extensions at the main server as well as for extensions at remote locations. To support inter-server dialing, Communication Manager uses the uniform dial plan (UDP) to route a call from the local server. With the Dial Plan feature, you can set extensions of maximum 13 digits. You can further extend the extension length to 18 digits by using uniform dial plans.

To preserve the dial plan for extensions and attendants in a multiple independent node network that is being migrated to a single distributed server, Communication Manager provides the Multi-location Dial Plan feature.

To assign short extensions to different branches and administer the same numbering format across all the branches, you can use the Per-Location Dial Plan feature.

Define the dial plan information for each type of call, including:

- Attendant
- Automatic Alternate Routing (AAR)
- Automatic Route Selection (ARS)

- Dial access codes, including feature access codes (FACs) and trunk access codes (TACs)
- En bloc extensions (enb-ext)
- Extensions
- FACs only
- Prefixed extensions

For more information about the dial plan feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Call Admission Control specification

To protect voice traffic from being negatively affected by other voice traffic and to prevent WAN links from being overloaded, you can set a limit on the bandwidth consumption by using Call Admission Control (CAC) mechanisms. The CAC concept is applicable to voice traffic only, and not data traffic.

In case of data traffic congestion on a particular link in the network, queueing, buffering, or dropping of data packets resolve the congestion. However, for real-time traffic, which is sensitive to both, latency and packet loss, it is better to deny network access under network congestions than to allow data packets to be dropped or delayed. CAC is, therefore, made before a voice call is established. Application of CAC is based on the network resources available to provide suitable QoS for a new call.

The bandwidth limit is applicable to all calls, regardless of the codec of the calls. Therefore, while administering the field for bandwidth consumption limit, ensure that either all calls use the same codec or that you have set a manual limit after considering the highest possible bandwidth consumed by the specified inter-region codec set.

Note:

If SRTP media encryption is used for SIP and H.323 calls, adjust CAC for the additional bandwidth consumption imposed by the authentication process. SRTP authentication adds up to 4 (HMAC32) or 10 (HMAC80) bytes to each packet.

Chapter 5: Security specification

Communication Manager security, privacy, and safety

Communication Manager provides security features for detecting probable breaches, taking measures to protect the system, and tracking and notifying activities. Communication Manager also provides real-time media encryption for environments where enhanced voice privacy over a LAN/WAN is required.

Communication Manager supports:

- Industry Standard STRP for authentication and media encryption
- Real Time Media and Signaling Encryption
- Access Security Gateway
- Malicious Call Tracking
- Toll Fraud protection
- Emergency Calling Services (E911)

The first security layer is the isolation of Communication Manager telephony servers from the rest of the enterprise network to safeguard the servers from viruses, worms, DoS and other attacks. To reduce susceptibility to malicious attacks, Communication Manager uses the minimum number of services and access ports. To secure the voice stream and signaling channels, Communication Manager employs encryption between servers, gateways, and endpoints.

The second security layer incorporates a hardened Linux operating system with inherent security features for Avaya servers with Communication Manager. This operating system provides the functions necessary to protect the core applications from malicious attacks.

Communication Manager and the gateways use encryption as the third layer of Avaya security. This security strategy ensures privacy for the voice stream. Alongside encrypting data, integrated signaling security protects and authenticates messages to all connected gateways and IP telephones, and eliminates tampering with confidential call information.

The Avaya Product Security Support Team (PSST) is responsible for:

- Managing Avaya product vulnerabilities and threats
- Maintaining information posted at http://support.avaya.com/security.
- Performing security testing and auditing of Avaya core products.

- Resolving security-related field problems in support of Avaya Global Services.
- Managing the securityalerts@avaya.com mailbox.

For more information about security design, see *Avaya Aura® Communication Manager Security Design*.

Related topics:

RTP encryption on page 34
Timers and key exchange details on page 34

RTP encryption

Communication Manager supports the following high-strength encryption algorithms:

- Avaya Encryption Algorithm (AEA), a 104-bit RC4-like encryption algorithm
- Advanced Encryption Standard (AES), which is a 128-bit encryption algorithm
- SRTP

In all these encryption algorithms, the system dynamically creates encryption keys for each connection. The system creates the encryption keys within the gatekeeper and transmits the keys to the endpoints and the processing boards over secure links. Additionally, the system produces separate keys for the incoming and outgoing streams of each call. For conference calls, the system assigns a unique pair of keys for encrypting the payload of each endpoint, one for the incoming stream and one for the outgoing stream. With the introduction of SRTP, the system derives additional keys to authenticate the RTP and RTCP message.

Because all the authentication keys are dynamically created and assigned, the system stores these keys only in RAM. These keys are not accessible by administrators or users. RTP keys are not escrowed.

Timers and key exchange details

Key negotiations for IPSI streams, which is based on AES-128-Cipher Block Chaining, and for H.248 streams, which is based on AES-128-Output FeedBack, are authenticated with 128-bit Diffie-Hellman and fixed symmetric keys. When Communication Manager starts or re-configures a data stream, Communication Manager inserts the encryption keys again to decrypt the data streams. The average cycle length for AES and SRTP with AES-128-CBC is reported to be 2^{127}, which is too long to permit a practical attack. Avaya uses a block size of 128 bits to maximize the average cycle length of transmission. A cycle of any length is invisible unless the transmitted information is identical.

SRTP inherently provides anti-replay and integrity protection because SRTP accepts a packet only once. In addition, packets contain the session key along with the SSRC or the synchronization source that are different for each packet.

Port utilization

The main server, survivable remote servers, and survivable core servers use specific ports for registration and translation distribution.

Note:

Use ports 80 and 443 to gain access to System Management Interface (SMI). Use port 5022 for the secured System Access Terminal (SAT).

Use the following table to determine which ports are available in the customer network.

Port	Used by	Description
20	ftp data	—
21	ftp	—
22	ssh and sftp	—
23	telnet server	—
68	DHCP	—
514	Communication Manager 1.3	To download translations
1719 (UDP port)	The survivable core server	To register to the main server
1024 and above	Processor Ethernet	To connect to TCP outgoing
1956	Command server - IPSI	—
2312	Telnet firmware monitor	—
5000 to 9999	Processor Ethernet	To connect to TCP incoming
5010	IPSI or Server control channel	—

For more information about port utilization, see the Communication Manager port matrix on the Avaya Support website at http://www.avaya.com/support.

Chapter 6: Licensing requirements

To use the Communication Manager software, you require a valid Communication Manager license file. Without a valid license file, Communication Manager enters the License Error mode, with a 30-day grace period. If the grace period expires before a valid license file is installed, Communication Manager enters the License Restricted mode. In this mode, you cannot save any administrative changes to Communication Manager.

Communication Manager Release 6.x uses the Avaya Product Licensing and Delivery System (PLDS) to manage license entitlements and generate license files. The license file contains information regarding the product, major release, license features, and capacities. PLDS provides the ability to move licenses between Communication Manager servers if the support offer and the move policy are followed. Communication Manager releases earlier than 6.0, except for Midsize Business Template (MBT) Communication Manager Release 5.2.1, continue to use the Remote Feature Activation (RFA) online tool to generate license files. MBT Communication Manager Release 5.2.1 and Communication Manager Release 6.0 and later use PLDS to manage licenses.

Starting from Release 6.2, Communication Manager uses the Service Pack and Dot Release Guardian technology to protect and control the authorized use of service packs and dot releases. Using this technology, Communication Manager inserts the Support End Date (SED) in the license file and compares it with the publication date of the service pack or the dot release, thus, preventing the use of a service pack or a dot release that has a publication date after the SED.

Virtual appliance licensing on VMware

Each Communication Manager software that is deployed on the VMware platform uses a single instance of WebLM license server to host the license file. The WebLM instance located within System Manager is the first and the preferred WebLM instance.

In a network of multiple Communication Manager systems, each Communication Manager server or Communication Manager software-duplication pair requires a separate license file. Using the Centralized Licensing feature, install the Communication Manager or Communication Manager software-duplication pair license files on System Manager WebLM. You can also install the Communication Manager license files on the standalone WebLM virtual appliance (per Communication Manager/Communication Manager software-duplication pair).

Related topics:

Centralized Licensing on page 38

Centralized Licensing

System Manager WebLM Release 6.3.4 supports the Centralized Licensing feature in System Platform and VMware Enablement environments. The Centralized Licensing feature is available only for Avaya Aura® Communication Manager. Using the Centralized Licensing feature, you can install up to 600 license files for Communication Manager on a single System Manager WebLM server. After installing a license file for a Communication Manager main server (simplex or duplex pair), you must link the Communication Manager main server to the license file in WebLM.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Communication Manager main server.
- Eliminates the need to log in to each WebLM server to manage licenses for each Communication Manager main server.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Communication Manager.

Note:

- The standalone (non-System Manager) WebLM server does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Communication Manager server.

For System Manager and Communication Manager centralized licensing backward compatibility, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Chapter 7: Virtualization specification

Communication Manager Release 6.2 and later is available as an open virtual application (OVA) that can be installed on VMware vSphere Release 5.0, 5.1, and 5.5. The Communication Manager VMware virtualization environment is available in a vAppliance package, which is ready for deployment on VMware certified hardware.

Note:

Communication Manager Release 6.2 and later does not support VMware vSphere Release 4.1.

Communication Manager on the VMware platform is deployed either as a simplex or as a duplicated Communication Manager software-duplication pair. The Communication Manager Simplex OVA deployment supports VMware high availability.

The Communication Manager virtual machine requires the following set of resources to be available on the ESXi host before deployment. These resources are specified in the Communication Manager OVA.

VMware component	Description
ESXi host	The physical machine that runs the ESXi Hypervisor software.
ESXi hypervisor	A platform to simultaneously run multiple operating systems on the host computer.
vSphere client	The client application installed on a personal computer or accessible through a web interface. It connects to a vCenter server or directly to an ESXi server where vCenter is not used. Supports installation and management of virtual machines.
vCenter	A software to centrally control and monitor each level of the virtual infrastructure. Provides alarms and monitors performance of ESXi hosts and virtual machines.

For more information on virtualization, see *Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment*.

Glossary

Automatic Call Distribution	A programmable device at the contact center. Automatic Call Distribution (ACD) handles and routes voice communications to queues and available agents. ACD also provides management information that can be used to determine the operational efficiency of the contact center.
Busy Hour Call Completions	A measure of dynamic traffic calls that can be completed in an average busy hour.
Call Admission Control	A method of limiting voice traffic over a particular link in a network.
Call Management System	An application that enables customers to monitor and manage telemarketing centers by generating reports on the status of agents, splits, trunks, trunk groups, vectors, and VDNs. Call Management System (CMS) enables customers to partially administer the Automatic Call Distribution (ACD) feature.
Codec	A coder and decoder (Codec) is a device that encodes or decodes a signal.
Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
Multi-Location Dial Plan	An Avaya feature that provides a mechanism for merging systems with overlapping dial plans. With this feature, users can retain their original n-digit dialing.
S8300	A Communication Manager server supporting medium-sized customers.
Session Manager	A SIP routing and integration tool that is the core component within the Avaya Aura® solution.
System Manager	A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity.

Index

A

Automatic Call Distribution 17
Avaya courses 10

C

CAC 31
Call admission control 31
Call Center 16
Call Distribution 17
    Automatic 17
Call Routing 19
Capacity and scalability 27
    specification 27
Collaboration 18
Communication Manager 16, 20
Communication Manager features 13
Communication Manager Localization 20
Communication Manager overview 13
Communication Manager virtual appliance licensing . 37
Computer Telephony Integration 17
connectivity 14
    gateway 14
    port network 14
Connectivity 14
    Trunk 14
CTI 17
Customization 20

D

Data Interfaces 16
dial plan specification 30
document changes 7
document purpose 7

F

feature description 13

I

Intelligent Networking 15
intended audience 7
Interfaces 16
    Data 16

L

legal notice 2
licensing requirements 37
Localization 20

M

Mobility 17

N

Networking 15
    Intelligent 15
    Public 15
new features 20
new in this release 20

O

operating system 24
operating system compatibility 24

P

port utilization 35
Privacy 33
product compatibility 23
Public Networking and Connectivity 15
purpose of document 7

R

related documentation 8
Remote Office 19
RTP encryption 34

S

Safety 33
Security 33
server compatibility 23
support 12

contact 12
Supported endpoints 25
survivability 30
survivability specifications 30

T

Telecommuting 19
Timers and key exchange details 34
traffic specifications 29
training 10
Trunk Connectivity 14

V

videos 11
virtual appliance licensing 37
virtualization 39
VMware 39
VMware licensing 37

W

Warranty 12
WebLM 38
centralized licensing 38