Avaya Aura® Communication Manager Overview and Specification

Release 10.2.x
Issue 6
April 2025

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 in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. 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 or on the express behalf of 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. Please refer to your agreement with Avaya 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

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, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, 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

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document describes tested Avaya Aura® Communication Manager characteristics and capabilities, including the product overview, feature descriptions, and security and licensing requirements.

This document is intended for anyone who wants to gain a high-level understanding of the product features and functions.

Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the End of sale G650 document published on the Avaya Support website.

Change history

Issue	Date	Summary of changes
6	April 2025	Added the following sections for Release 10.2.1.1: • New in Communication Manager Release 10.2.1.1 on page 12 • Licensing requirements on page 46

Table continues…

Issue	Date	Summary of changes
5	April 2025	Updated the following section: • Collaboration on page 29
4	February 2025	Updated the following section: • Communication Manager security, privacy, and safety on page 44
3	December 2024	Added the following section for Release 10.2.1: • New in Communication Manager Release 10.2.1 on page 12 Updated the following section for Release 10.2.1: • Communication Manager feature matrix on page 9
2	July 2024	Added the section: Communication Manager feature matrix on page 9
1	December 2023	Release 10.2

Chapter 2: Overview

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 can scale from less than 100 users to 41,000 users on a single system.

Communication Manager is a core component of the Avaya Aura® platform and the foundation for delivering real-time voice, video, messaging, mobility, and other services. 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 has several built-in mobility applications, call center features, advanced conference calling, and E911 capabilities.

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

Note:

From Avaya Aura® Communication Manager Release 10.1 SMI page will have the following options but are for future use:

- Administration > Licensing > Feature Administration > Current Settings > Display > Optional Features > Clustering
- Administration > Server (Maintenance) > Server Configuration > Configure Memory (for LSP) > This Server's Memory Setting > X- Large/Array

Note:

- From Avaya Aura® Release 10.1, HP ProLiant DL360p G8 (CSR2), HP ProLiant DL360 G9 (CSR3), Dell™ PowerEdge™ R620 (CSR2), Dell™ PowerEdge™ R630 (CSR3), and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.1, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x, and S8300E can be upgraded to Avaya Solutions Platform S8300 R5.1.x.
- From Avaya Aura® Release 10.1, Appliance Virtualization Platform is not available for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura®

applications, migrate the Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.

Avaya Aura® overview

Avaya Aura® is a flagship communications solution that uses an IP and SIP-based architecture to unify media, modes, networks, devices, applications, and real-time, actionable presence across a common infrastructure. This architecture provides on-demand access to advanced collaboration services and applications that improve employee efficiency. Avaya Aura® is available under Core or Power Suite Licenses. Each suite provides a customized set of capabilities designed to meet the needs of different kinds of users. Customers might mix Core and Power licenses on a single system based on their needs.

The following are some of the capabilities that the Avaya Aura® solution provides:

- Support for up to 28 instances of Session Manager and 300,000 users and 1 million devices
- Support for up to 18,000 simultaneously registered H.323 endpoints out of 41,000 endpoints per single Communication Manager server and SIP endpoints in an enterprise
- Advanced Session Management Capabilities
- Converged voice and video call admission control
- SIP features, including E911, which reports the desk location of the caller

Communication Manager feature matrix

The following table lists the feature matrix of Communication Manager from Release 7.1.x to Release 10.2.x. The features listed in the table covers the key features only.

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
OVA signing	Y	Y	Y	Y	Y	Y
IPv6 support	Y	Y	Y	Y	Y	Y
Enhanced Access Security Gateway (EASG)	Y	Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
Compliance with DISA security STIGs	Y	Y	Y	Y	Y (R 10.1.0.2 onwards)	Y
Extended Security Hardening	Y	Y	Y	Y	Y	Y
Support for TLS 1.2	Y	Y	Y	Y	Y	Y
Customer Root Access		Y	Y	Y	Y	Y
Preserve security hardening modes on upgrade		Y	Y	Y	Y	Y
SIP trunk optimization		Y	Y	Y	Y	Y
Automatic Call Distribution	Y	Y	Y	Y	Y	Y
Emergency Calling Services	Y	Y	Y	Y	Y	Y
Alphanumeric URI dialing	Y (R 7.1.2 onwards)	Y	Y	Y	Y	Y
Extended security hardening	Y (R 7.1.2 onwards)	Y	Y	Y	Y	Y
Support for Avaya Solutions Platform 120 Appliance		Y	Y	Y		Y
Support for Avaya Solutions Platform 130 Appliance		Y	Y	Y	Y	Y

Table continues…

Feature name	Release 7.1.x	Release 8.0.x	Release 8.1, Release 8.1.1, and Release 8.1.2	Release 8.1.3	Release 10.1.x	Release 10.2.x
Support for J-Series phone migration				Y	Y	Y
Support for VMware ESXi 7.0				Y	Y	Y
Emergency Location Management Solution				Y	Y	Y
Support for TLS 1.3					Y	Y
Support for Red Hat Enterprise Linux (RHEL) 8.4					Y	Y
Support for Red Hat Enterprise Linux (RHEL) 8.10						Y (R 10.2.1 onwards)
Avaya Solutions Platform S8300					Y	Y
Optional Upgrade Sequence					Y	Y
License expiration (Blocking of call processing and system administration)						Y (R 10.2.1.1 onwards)

New in this release

New in Communication Manager Release 10.2.1.1

With Release 10.2.1.1, Avaya Aura® Communication Manager supports the following new enhancements:

Enhancement to Communication Manager License Expiration

With Release 10.2.1.1, Communication Manager is changing its licensing behavior to keep customers informed about license expiration dates so they can renew licenses on time and avoid service disruption. Communication Manager is introducing two new alarms that warns customers about license expiration date and its impact:

- LIC-EXP90: This alarm is raised 90 days before the expiration of Communication Manager license.
- LIC-EXP60: This alarm is raised 60 days before the expiration of Communication Manager License.

The Communication Manager enters into a 30-day Grace Period on expiration of License. After 30-day grace period expiry, if license is not renewed:

- Call Processing, including Emergency calling, will be blocked. That is, Communication Manager will not process any type of calls.
- System Administration will be blocked.

Customer must renew their licenses on time to avoid this disruption.

This feature enhancement is applicable only for main Communication Manager and not for Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS).

Enhancement to Survivable License Grace Period

With Release 10.2.1.1, Communication Manager supports configurable Survivable License Grace Period for the Enterprise Survivable Server (ESS). This field is applicable only for ESS, and not for LSP.

New in Communication Manager Release 10.2.1

With Release 10.2.1, Avaya Aura® Communication Manager supports the following new features and enhancements:

Red Hat Enterprise Linux (RHEL) 8.10 support

With Release 10.2.1, Communication Manager supports Red Hat Enterprise Linux Release 8.10.

Support for Software-Only Deployment on Nutanix Environment

With Release 10.2, Communication Manager Software-Only application can be deployed on Nutanix 6.5 later.

Kernel-based Virtual Machine (KVM) on RHEL 8.10 hypervisor support

With Release 10.2, Communication Manager can be deployed on Avaya-supplied KVM on RHEL Release 8.10 hypervisor (Avaya Solutions Platform 130 R6.0).

Optional upgrade sequence

An alternate upgrade sequence that allows you to upgrade your core Communication Manager before you upgrade your Survivable Remote Servers, formerly known as Local Survivable Processors (LSP). While you use the latest features from the core Communication Manager, you can continue to upgrade your Survivable Remote Servers (LSP) to the same or a higher software version than your core Communication Manager. This sequence of upgrading has a limitation of configurations not synchronizing between the upgraded core Communication Manager and yet-to-be-upgraded Survivable Remote servers (LSP).

Ensure to read the complete details of the Optional Upgrade Sequence feature before you implement this upgrade sequence. For more information, see *Upgrading Avaya Aura® Communication Manager*

New in Communication Manager Release 10.2

With Release 10.2, Avaya Aura® Communication Manager supports the following new features and enhancements:

Support for VMware 8.0

With Release 10.2, Avaya Aura® applications support the VMware® vSphere ESXi 8.0 and VMware® vCenter Server 8.0 in a VMware virtualized environment.

Support for Trellix AV (formerly known as McAfee) in Virtualized Deployments

Avaya Aura® Release 10.2 supports the deployment of Trellix AV software in a virtualized (OVA-based) environment. This new feature effectively detects, prevents, and eliminates malware threats, resulting in enhancing the security of your Avaya Aura® environment. The IT industry widely recognizes Trellix AV as a trusted cybersecurity solution. With the integration capabilities in Avaya Aura® Release 10.2, you can seamlessly integrate Avaya Aura® applications as managed devices as part of your existing Trellix deployment. For more information on support of Trellix for AV on Avaya Aura®, see *Application Note for Support of Trellix AV on Avaya Aura®* on the Avaya Support website at https://support.avaya.com.

Support for J139, J159, J189, and J189CC endpoints

With Release 10.2, Communication Manager supports the following J-Series endpoints: J139, J159, J189, and J189CC.

To administer these endpoints, use System Manager.

When you add these endpoints from System Manager, Communication Manager displays these endpoints in the **Type** field of the **Station** form as **AvyaSIP** or **AvyaSIPCC**, and the actual endpoint type, such as J139 and J159, appears in the **Actual** field.

Edge Friendly Branch Survivability

In the previous Avaya Aura® Release 10.1, support for Edge Friendly Branch Survivability feature was introduced, which made it easier to have seamless connections between your on-premise G4xx Gateways and the Core Communication Manager hosted on the Cloud. Avaya designed this innovation to protect your investments, especially when you are considering a shift to a Cloud-based infrastructure.

With Avaya Aura® Release 10.2, migrating to the Cloud is even more streamlined. You can now configure edge topology for Cloud deployment. Survivable components like Local Survivability Processor (LSP) and Branch Session Manager (BSM) within G4xx Gateways can connect to Core

Communication Manager and Session Manager on the Cloud. This connection between Gateways and Cloud can be established over the Internet or through SD-WAN, providing significant advantages in terms of Total Cost of Ownership (TCO).

To configure LSP topology to edge, do the following:

- Download TLS certificates to the new **Edge Topology (E)** repository. The certificates are required to set up a new WebSocket connection between the main Communication Manager and the Communication Manager LSP.
- On the Communication Manager SMI, go to **Administration** > **Server (Maintenance)** > **Server Configuration** > **Server Role** page and configure the **LSP Topology Configuration** section.
- On the main Communication Manager SAT, go to the change survivable-processor screen and do the following:
  - Configure the LSP topology as “Edge”.
  - In the **Serial Number** field, enter the serial number of Communication Manager LSP.

Line Load Control (LLC) feature enhancement

In previous releases, you must configure LLC using System Manager or Communication Manager SAT only, but now you can easily configure LLC using Feature Access Codes.

Avaya Aura® Release 10.2 enhances the LLC feature for enhanced security. It provides an option to implement two-factor authentication for LLC setup, requiring the entry of a security code, which strengthens the security process.

In Avaya Aura® Release 10.2, you can limit the scope of LLC at the site level of your organization. It means that LLC can be applied selectively, exclusively to users of your organization associated with the site from which you initiated the LLC. It offers a more precise and site-specific approach to LLC deployment, enhancing the flexibility and control over LLC configurations.

Support to record the call originated from bridged line appearances

Communication Manager's Bridged Appearance feature is a widely used feature in both Unified Communications (UC) and Contact Center (CC) environments. In previous releases, a call originated using bridged appearance in a SIP environment was never recorded. This gap is addressed in this current release.

With Release 10.2, Avaya Aura® sends the required events for recording over Adjunct Switch Applications Interface (ASAI) when the call is initiated using Bridged Appearance.

Mask CLI and Station Name support on SIP

In Release 10.2, Avaya Aura® further enhances its functionality by extending the capability to mask the calling party number and name on outgoing calls. You can achieve this functionality using the **send-nn** button on SIP Phones. This feature enables your organization to keep the caller's identity confidential, thus enabling the implementation of a standardized approach for callback interactions.

Alerting internal users with a tone during external communications

In Release 10.2, Avaya Aura® introduces a security enhancement that notifies internal users with an audible tone when they are communicating with external parties. This unique tone is heard only by internal users. You can adjust the time interval between these tones through the System-Parameter Features form. Additionally, you can apply this feature to selective trunk groups, ensuring it operates only on the configured trunk groups.

STIR/Shaken support for verification level display on phones

STIR/Shaken is a set of protocols designed to counter caller ID spoofing on public telephone networks. Avaya Aura® Release 10.2 supports STIR/Shaken and enables the display of the attestation or verification level set by service providers on user or agent phones. This feature works exclusively over SIP trunks. You can enable or disable this feature at the Avaya Aura® solution level based on your preferences.

New field added to the Coverage path page

With Release 10.2, the **Description** field is added to Coverage path page. You can use the **Description** field to specify a name for a coverage path to distinguish the coverage paths.

Discontinued support of legacy technologies

Avaya Aura® Release 10.2 discontinued the following legacy technologies to reduce the risk to Business Continuity for customers:

- G650 or any cabinet/Gateway that connects to Communication Manager using IP Server Interface (IPSI) is no longer supported. For more information, see the End of sale G650 document published on the Avaya Support website.
- VMware ESXi version 6.7 or lower versions are not supported.
- Avaya Device Adapter Snap-in is no longer supported.

Features

Administration features

Avaya Aura® Communication Manager supports several administration interfaces for ease of use.

- System Access Terminal: A screen-oriented interface for telephony administration. System Access Control is available using the System Manager package. The system-level limit on the number of concurrent System Access Control sessions is 22. This limit is only for login profiles 18 to 69 and not for system logins. A user can have up to five concurrent System Access Control sessions.
- System Management Interface: Uses graphical user interface screens for telephony administration. Using System Management Interface, you can perform system management tasks.
- System Manager: Provides central administration for Communication Manager and other Avaya Aura IP Telephony products.
- Solution Deployment Manager: This is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. Install the client on the computer of the technician. The Solution Deployment Manager client provides the functionality to deploy the OVAs or ISOs on an Avaya™-provided server, customer-provided virtual environment, or software-only environment.

To label each point-to-point session with a globally unique identifier, Communication Manager generates a 128-bit identifier and inserts the identifier in the Global Session ID (GSID) header of the request. To troubleshoot call flows, you can use a tracing tool and filter GSIDs from the relevant logged messages.

For more information about administering the Communication Manager features, see *Administering Avaya Aura® Communication Manager*.

Attendant features

Communication Manager supports the following two types of attendant consoles:

- Traditional console: It consists of a hard or a soft console. A hard console uses digital or DCP signaling, and a soft console uses H.323 signaling. The call queues for calls to these attendant positions are hosted on Communication Manager.

  Note:

  Avaya no longer sells attendant products that support H.323 signaling.

- Avaya Workplace Attendant: It comprises a Windows-based soft client that uses SIP signaling and the Avaya Workplace Attendant Snap-in where call queues (Topics) are hosted. This Snap-in resides on a Breeze Server or Breeze Cluster. Presence Services can be co-deployed with Avaya Workplace Attendant Snap-in.

Traditional console

Communication Manager contains many features that provide easy ways to communicate through your telephone system attendant (operator). Additionally, attendants can connect to their console (switchboard) from other telephones in your system, thereby expanding the attendant capabilities.

- Attendant backup: With the attendant backup feature, you can access most attendant console features from one or more specially-administered backup telephones. Consequently, you can answer calls more promptly, thus providing better service to your guests and prospective clients.
- Attendant room status: With the attendant room status feature, you can see whether a room is vacant or occupied and the housekeeping status of each room.

  Note:

  This feature is available when enhanced hospitality is enabled for your system.
- Attendant functions using the Distributed Communications System protocol:
  - With control of trunk group access, an attendant at any node in the Distributed Communications System can control any outgoing trunk group at an adjacent node.
  - With direct trunk group selection, the attendant can press a button assigned to a trunk group to directly access an idle outgoing trunk in that local or remote trunk group.
  - With Inter-PBX attendant calls, attendants for multiple branches can be concentrated at the main location.
- Call handling:
  - Attendant intrusion: Using this feature, An attendant can intrude to an existing call. This feature is also called as Call Offer.

- Attendant lockout - privacy: This feature prevents an attendant from re-entering a multiple-party connection held on the console unless a telephone user recalls them.
- Attendant split swap: With this feature, the attendant can alternate between active and split calls. This operation can be useful if the attendant needs to transfer a call but must talk independently with each party before completing the transfer.
- Attendant vectoring: Attendant vectoring provides a highly flexible approach for managing incoming calls to an attendant. For example, with the current night service operation, calls redirected from the attendant console to a night station can ring at that station and do not follow any coverage path.
- Automated attendant: With an automated attendant, the calling party can enter any extension number on the system. The call is then routed to the extension. Therefore, to reduce cost, you can reduce the requirement for live attendants.
- Backup alerting: The backup alerting feature notifies backup attendants that the primary attendant cannot pick up a call.
- Call waiting: With call waiting, an attendant can let a single-line telephone user who is on the telephone know that a call is waiting. The attendant is then free to answer other calls. The attendant hears a call waiting ringback tone, and the busy telephone user hears a call waiting tone. The called telephone user hears this tone.
- Calling of inward restricted stations: A telephone with a class of restriction (COR) that is inward restricted cannot receive public network, attendant-originated, or attendant-extended calls. You can use this feature to override this restriction.
- Conference: With the conference feature, an attendant can set up a conference call for as many as six conferees, including the attendant. Conferences from inside and outside the system can be added to the conference call.
- Enhanced Return Call to (same) Attendant. Communication Manager provides individual queuing functions for each attendant supporting a multiplicity of waiting calls at a time.
- Listed directory number: Outside callers can access your attendant group in two ways, depending on the type of trunk used for the incoming call.
- Override of diversion features: With this feature, to bypass diversion features such as send all calls and call coverage, an attendant can put a call through to an extension even when these diversion features are on. This feature, together with attendant intrusion, can be used to get an emergency or urgent call through to a telephone user.
- Priority queue: Priority queue places incoming calls to the attendant in an orderly queue when these calls cannot go immediately to the attendant.
- Release loop operation: With this operation, the attendant can hold a call at the console if the call cannot immediately go through to the called person. A timed reminder begins after the call is on hold.
- Selective conference mute: With this operation, user can mute a conference call participant, who has a display station, to mute a noisy trunk line. Selective conference mute is also known as far-end mute.
- Serial calling: The serial calling feature enables an attendant to transfer trunk calls that return to the same attendant after the called party hangs up. The returned call can then transfer to another station within the switch. This feature is useful if trunks are scarce and direct inward dialing services are unavailable.

  - Timed reminder and attendant timers: Attendant timers automatically alert the attendant after an administered time interval for certain types of calls.

- Centralized attendant service: Centralized attendant service enables attendant services in a private network to be concentrated at a central location. Each branch in a centralized attendant service has its listed directory number or another type of access from the public network. Incoming calls to the branch and calls made by users directly to the attendants are routed to the centralized attendants over release link trunks.
- Display: The display feature shows call-related information that helps the attendant to operate the console. This feature also shows personal service and message information.
- Making calls
  - Auto Start and Do Not Split: With this feature, the attendant can make a telephone call without pushing the start button first. If the attendant is on an active call and presses digits on the keypad, the system automatically splits the call and dials the second call.
  - Auto Manual Splitting: With this feature, attendant can announce a call or consult privately with the called party without being heard by the calling party on the call. It splits the calling party away so the attendant can confidentially determine if the called party can accept the call.
- Monitoring calls:
  - Attendant control of trunk group access: With this feature, the attendant can control outgoing and two-way trunk groups.
  - Attendant direct extension selection: With this feature, the attendant can keep track of extension status - whether the extension is idle or busy. The attendant can place or extend calls to extension numbers without dialing the extension number.
  - Attendant direct trunk group selection: With this feature, for direct access to an idle outgoing trunk, the attendant presses the button assigned to the trunk group. This feature eliminates the need for the attendant to memorize, look up, and dial the trunk access codes associated with frequently used trunk groups.
  - Crisis alerts to an attendant console: Crisis alert uses audible and visual alerting to notify attendant consoles when an emergency call is made. Audible alerting sounds like an ambulance siren. Visual alerting flashes the CRSS-ALRT button lamp and displays the caller's name and extension (or room).
  - Trunk group busy/warning indicators to attendant: This feature provides the attendant with a visual indication that the number of busy trunks in a group has reached an administered level. A visual indication is also provided when all trunks in a group are busy. This feature is particularly helpful to show the attendant that the attendant control of the trunk group access feature needs to be invoked.
  - Trunk identification by attendant: With this feature, the attendant or display-equipped telephone user can identify a specific trunk being used on a call. This capability is provided by assigning a trunk ID button to the attendant console or telephone. This feature is helpful for identifying a faulty trunk. That trunk can then be removed from service and the problem quickly corrected.
  - Visually Impaired Attendant Service: Visually Impaired Attendant Service provides voice feedback to a visually impaired attendant. Each voice phrase is a sequence of one or more single-voiced messages. This feature defines six attendant buttons to aid visually impaired attendants.

Avaya Workplace Attendant

Key features of Avaya Workplace Attendant are as follows:

- Customizable welcome and attendant greetings.
- Supports multiple topics: A topic is a call queues for a location or department.
- Incoming calls are queued and presented in a Call Preview panel.
- Attendants can cherry-pick the most important incoming calls in the queue from the Call Preview window.
- Topics can be prioritized up to five levels to show important incoming calls first.
- The operator can provide a more personal touch using the Contextual information. This includes call history for the incoming caller and taking notes against each caller, which are visible to other attendants or marked private to an individual attendant.
- Dynamically created suggested users display a list of recommended transfers based on previous calls of callers.
- Dynamically created favorites display a list of users to whom the attendant frequently transfers calls.
- The attendant can “Look Ahead” and see the status of the destination user, including calendar status using the integration with Presence Services.
- Busy display based on destination user’s presence: This can be organized by multiple tab views consisting of a range of numbers, a list of individual numbers, or a combination of both. You can create location or department views using this.
- Customizable screen layout supporting multiple monitors: Busy display window, call preview, call detailed, and target user panels can be undocked, repositioned within the Avaya Workplace Attendant window, or placed on other monitors.
- Integration into multiple databases can be synced by time into the Avaya Workplace Attendant phone book. Avaya Workplace Attendant supports the most common databases, including Active Directory, Open LDAP, IBM Domino, Progres, Oracle DB, My SQL, Sybase, CSV files, Communication Manager, and System Manager.
- Attendant can update a database and instantly sync the result into the Attendant phone book.
- Unified search shows comprehensive information of user search results. Additionally, you can search using the multiple fields in the phone book.

Avaya Workplace Attendant also supports the following features:

- Status: Set the status to **Available** to receive distributed calls. When you set the status to **Busy**, calls are not automatically presented to the attendant. The attendant can cherry-pick a call from the Call Preview window when their status is Busy.
- Supports computer mode: Calls are managed on Windows PC, and media is presented to PC.
- Desk phone modes: Attendant manages calls on PC, but media is presented to users on 96x1 or J Series desk phone.
- Make outgoing calls.
- Answer calls: Calls are distributed based on the longest idle or cyclic (in the order the Attendant logged in) rules.

- Attendants can cherry-pick from the queued calls.
- Transfer calls to users, after consulting users or directly doing a blind transfer.
- Transfer to the voice mail of destination users.
- End calls without transferring the calls to the user.
- Hold calls.
- Retrieve calls put on hold.
- Park calls on a topic or attendant.
- Park calls on a busy destination user.
- Un-park a call.
- Recall to attendant due to time out on transferred or parked calls.
- Recall to the attendant where the internal caller hangs up before the external caller. A timer can be programmed, which defines the period between an internal caller hanging up and a time for the external caller ending the call. If this period exceeds, the call is recalled to the attendant. Setting this timer to Zero disables this feature.
- Start conferences by adding users to existing calls.
- Use DTMF digits to navigate IVR systems.
- Add callers to a Speed dial list.
- Create personal contacts for an attendant.
- Transfer out-of-hour calls to a Night service number or a Night Service IVR.
- Overflow from one topic to a second topic based on call duration or the number of calls in the queue.
- Comprehensive list of attendant statics by attendant and topic.
- Support for a web-based dashboard.

Customization features

Using Communication Manager, you can customize interfaces with Avaya and third-party adjuncts and solutions.

- Application Programming Interface (API): With APIs, numerous software applications can work with Communication Manager. Client programmer can create their applications using APIs that work with Communication Manager.
- Application Enablement Services (AE Services): Provides connectivity between applications and Communication Manager. With connector, you can develop new applications and new features without modifying Communication Manager or exposing its proprietary interfaces.

Note:

AE Services has its set of customer documentation, including an overview. This overview of Communication Manager does not outline the changes to AE Services.

- Device and media control API: Provides a connector to Communication Manager that clients can use to develop applications that provide first-party call control. Applications can register as IP extensions on Communication Manager and then monitor and control those extensions.

  Device and media control API consists of a connector server software and a connector client API library. The connector server software runs on a hardware server independent of Communication Manager. That is, the device and media control API does not run co-resident with Communication Manager.

  Tip:

  Contact your Avaya representative for a complete set of device and media control API documentation.
- Co-resident Branch Gateway: Enables communication between TCP/IP clients and Communication Manager call processing. The Branch Gateway is an application that routes internetwork messages from one protocol to another (ISDN to TCP/IP) and bridges all ASAI message traffic through a TCP/IP tunnel protocol.
- Java telephony application programming interface (JTAPI): Enables integration with Communication Manager ASAI.
- Telephony Services Application Programming Interface (TSAPI): An open API supported by Avaya computer telephony using which you can integrate to Communication Manager ASAI. TSAPI is based on international standards for CTI telephony services. Specifically, the European Computer Manufacturers Association (ECMA) CTI standard definition of Computer-Supported Telecommunications Applications (CSTA) is the foundation for TSAPI.

Scalability

For the entire list of system capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

Communication Manager reliability

Communication Manager supports a wide range of servers, gateways, and survivability features, enabling maximum availability for customers. The software can mirror processor functions, provide alternate gatekeepers, support multiple network interfaces, and ensure survivability at remote and central locations.

Note:

If you have an S8300 server configured in embedded CM main, survivable remote, or embedded survivable remote configurations, migrate to Avaya Solutions Platform S8300.

The reliability feature includes:

- Alternate gatekeeper: Provides survivability between Communication Manager and IP communications devices such as IP telephones and IP softphones.
- Auto fallback to primary for Branch Gateway: Automatically returns a fragmented network, where several Branch Gateways are serviced by one or more Communication Manager Survivable Remote sites to the primary server. This feature is targeted for Branch Gateways.

- Connection preserving failover/failback for Branch Gateway: Preserves existing bearer or voice connections while Branch Gateways migrate from one Communication Manager server to another. A network or server failure can cause the existing bearer or voice connections on the Branch Gateway to move to another Communication Manager server.
- Connection preserving upgrades for duplex servers: Provides connection preservation on upgrades of duplex servers for:
  - Connections involving IP telephones
  - Connections on Branch Gateway
- Communication Manager Survivable Core: Provides survivability for backup servers to be placed in various locations in the customer network.
  - When the Survivable Core is in control due to a network fragmentation or catastrophic main server failure, the return to the main server is automatic. It is provided by the scheduled, manual, and automatic options.
  - Dial Plan Transparency for Survivable Remote and Survivable Core preserves dialing patterns of users if a Branch Gateway registers with Survivable Remote.
- IP endpoint Time-to-Service: Improves a customer's IP endpoint time to service, especially where the Communication Manager has many IP endpoints trying to register or re-register. With this feature, the system considers that IP endpoints are in-service immediately after registering. The feature of TTS-TLS supports TTS over a secure TLS connection. This is the Avaya recommended configuration choice.
- Survivable processor: A survivable processor is an Internal Call Controller (ICC) with an integral Branch Gateway. The ICC is administered to function as a spare processor rather than the main processor. The standby Avaya Solutions Platform S8300 Server runs in standby mode, with the main server ready to take control in an outage with no loss of communication.
- Handling of split registrations: Occurs when resources on one network region are registered to different servers. For example, after an outage activates the Survivable Remote server (Local Survivable Processors) or Survivable Core server (Enterprise Survivable Server), telephones in a network region register to the main server, while the Branch Gateways in that network region are registered with the Survivable Remote server. The telephones registered with the main server are isolated from their trunk resources. Communication Manager detects a split registration and moves telephones to a server with trunk resources.
- Power failure transfer: Provides service to and from the local telephone company central office (CO), including a wide-area telecommunications system, during a power failure. With this feature, you can make or answer important or emergency calls during a power failure. This feature is also called emergency transfer.
- SRTP for video call flows: This support is available only when the call-originating and the receiving endpoints are SIP-registered, and the IP-codec-set administration on Communication Manager is SRTP. SRTP for video does not work for H.323 signaling. H.323-registered endpoints always send video RTP. SIP-H.323 interworking with video encryption is not supported, and video is blocked in this case. However, if the SIP signaling follows the Best effort SRTP mode, video RTP can pass through in SIP to H.323 interworking in Communication Manager.

Localization

Communication Manager supports various language features, such as administrable language displays and country-specific localization.

Communication Manager localization features include:

- Administrable language displays: With this feature, you can see the messages that appear on SIP stations, DCP and H.323 telephone display units in the language the user speaks. These messages are available in English (the default), French, Italian, Spanish, user-defined, or Unicode; where user-defined can be almost any language using the Latin, Russian or Katakana writing scripts, and Unicode can be almost any language in the world. An administrator configures the language to be displayed for messages for each user. The feature requires 40-character display telephones.
- Administrable loss plan: It is necessary to administer signal loss and gain for telephone calls because the amount of loss permitted on voice calls can vary by country.
- Bellcore calling name ID: With this feature, the Communication Manager can accept calling name information from a Local Exchange Carrier network that supports the Bellcore calling name specification. The system can send calling name information if Bellcore calling name ID is administered. The following caller ID protocols are supported:
  - Bellcore (default) - US protocol (Bellcore transmission protocol with 212 modem protocol).
  - V23-Bell - Bahrain protocol (Bellcore transmission protocol with V.23 modem protocol).
- Busy tone disconnect: In some regions of the world, the central office sends a busy tone for the disconnect message. With a busy tone disconnect, the switch disconnects analog loop-start central office trunks when a busy tone is sent from the central office.
- Country-specific localization
  - Brazil-Block collect call: Blocks collect calls on a class-of-restriction basis. This feature is available for any switch that uses the Brazil country code.
  - Japan
    - National private networking provides support for Japanese private ISDN networks.
    - Katakana character set Communication Manager supports the Katakana character set.
  - Russia
    - Central Office support on Branch Gateways: Communication Manager supports central office trunks in Russia using Avaya Branch Gateways.
    - ISDN/DATS network support: Supports ISDN/DATS trunk networks when the tone generated field is set to 15 (Russia) on the system-parameters tone-generation screen. It modifies the overlap sending delay and ISDN T302 and T304 timers to support the Russian trunk network.
    - Multi-Frequency Packet signaling: Multi-Frequency Packet (MFP) address signaling is provided in Russia on outgoing central office trunks. Calling party number and dialed number information is sent on outgoing links between local and toll switches.

- E&M signaling: E&M trunks are used to provide analog communication links. Continuous, pulsed Continuous, and pulsed E&M signaling are modifications to the E&M signaling used in the United States. Continuous E&M signaling is intended for Brazil but can also be used in Hungary. Pulsed E&M signaling is intended for use in Brazil.
- Multinational Locations: For customers who operate in multiple countries, the Multinational Locations feature enables the use of a single Enterprise Communication Server (ECS) across multiple countries.
- Public network call priority: Provides call retention, forced disconnect, intrusion, mode-of-release control, and re-ring to switches on public networks. Different countries frequently refer to these capabilities by different names.
- QSIG support for Unicode: Extends the Unicode support on a single server to multi-node Communication Manager networks. This feature supports Unicode across large campus configurations.
- World class tone detection: Enables Communication Manager to identify and handle different types of call progress tones, depending on the system administration.
- XOIP Tone Detection Bypass: The X over IP Tone Detection Bypass feature (where X = modem, fax, TTY-TDD) serves customers using older or non-standard external equipment such as modems, fax, TTY devices which are not easily recognized by VoIP resources within Communication Manager.

Optional Upgrade Sequence

With the Optional Upgrade Sequence feature, you can upgrade your core Communication Manager before you upgrade your Survivable Remote Servers, formerly known as Local Survivable Processors (LSP). This sequence of upgrading has a limitation of configurations not synchronizing between the upgraded core Communication Manager and yet-to-be-upgraded Survivable Remote servers (LSP).

Ensure to read the complete details of the Optional Upgrade Sequence feature before you implement this upgrade sequence. For more information, see *Upgrading Avaya Aura® Communication Manager*

Call Center

The Avaya Aura® Call Center provides a fully integrated telecommunications platform that supports a powerful assortment of features, capabilities, and applications designed to meet all Call Center needs of your customer.

Call Center applications, such as Avaya Call Management System for real-time reporting and performance statistics, and Avaya Business Advocate for expert predictive routing based on incoming calls rather than historical data, are easily integrated.

Communication Manager supports the Agent ID feature using telephones to retrieve specific agent greetings and play the greetings when calls are received.

Communication Manager also supports the Restrict Call Joining feature on Avaya Aura® Contact Center. If enabled, Communication Manager restricts the agents from initiating a transfer or a

conference operation. The restriction applies to outbound calls. With the Restrict Second Agent Consult feature, agents can use only one consult operation, transfer or conference at a time.

For a complete description of Call Center features for Communication Manager, see the following documents:

- *Avaya Aura® Call Center Elite Overview and Specification*
- *Planning for an Avaya Aura® Call Center Elite Implementation*
- *Administering Avaya Aura® Call Center Elite*
- *Avaya Aura® Call Center Elite Feature Reference*
- *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*

Related links

Avaya Call Center on Branch Gateway on page 25

Avaya Call Center on Branch Gateway

Avaya Call Center survivability functionality is supported on the same servers that Communication Manager supports.

For more information about the supported servers and gateways, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Avaya Call Center Basic software is included with Communication Manager capability and optional Computer Telephony Integration (CTI). This package provides a low-cost call center solution for small or branch offices.

The optional Avaya Call Center Elite provides more robust call center capabilities, which features Avaya Expert Agent Selection and services as the foundational software for the optional Avaya Business Advocate and Avaya Dynamic Advocate software.

Communication Manager Call Center customers can enhance their customer service, help desk, travel, and other operations by providing powerful, integrated call routing through call vectoring and resource selection using the call center capabilities found in the Elite Call Center software package.

Related links

Call Center on page 24

Computer Telephony Integration

Computer Telephony Integration (CTI) enables Communication Manager features to be controlled by external applications and integrate customer information databases, with call control features.

Avaya Computer Telephony is server software that integrates the premium call control features of Communication Manager with customer information in databases of customer. It is a local area network (LAN)-based CTI solution consisting of server software that runs in a client/server configuration. Avaya Computer Telephony delivers the CTI architecture and platform that supports contact center application requirements, and emerging applications programming interfaces (APIs). For more information about Computer Telephony Integration, see *Avaya Aura® Application Enablement Services Overview*.

Automatic Call Distribution

Automatic Call Distribution (ACD) is the basic building block for call center applications. ACD offers you a method for distributing incoming calls efficiently and equitably among available agents. With ACD, incoming calls can be directed to the first idle or most idle agent within a group of agents. ACD and Call Center Elite provide a very feature rich complement of routing and call handling capabilities. For more information about Automatic Call Distribution, see the *Avaya Aura® Call Center Overview* and *Avaya Aura®Call Center Feature Reference* guides.

Avaya Basic Call Management System

The Avaya Basic Call Management System (BCMS) helps you fine-tune your call center operation by providing reports with the data necessary to measure your call center agents performance integrated with Communication Manager software.

The BCMS feature offers call management control and reporting at a low cost for call centers of up to 3000 agents. BCMS collects and processes ACD call data (up to seven days) within Communication Manager. An adjunct processor is not required to produce call management reports.

Communication Manager can generate real-time and historical reports.

Related links

Avaya Business Advocate on page 26

Avaya Business Advocate

Avaya Business Advocate is the collection of features that provide flexibility in how a call is selected for an agent in a call surplus situation and an agent is selected for a call in agent surplus situations. Instead of the traditional “first in, first out” approach, the needs of the caller, potential business value, and the desire to wait are calculated. The system then decides what agents should be matched to the callers.

The Avaya Business Advocate features include:

- Auto reserve agents: With this feature, the Communication Manager can use the percent allocation distribution feature for agent skills.
- Call selection override per skill: Call selection override is determined by skill. Call center supervisors can override the normal call handling activity on particular skills, or for the entire call center.
- Dynamic percentage adjustment: With this feature, the Communication Manager can compare actual levels of service with service targets. The system can then adjust the service target so that the overall use of the skill is more efficient.
- Dynamic queue position: With this feature, the Communication Manager can put calls from multiple vector directory numbers (VDNs) into a skill queue. This feature ensures balanced call handling across VDNs.
- Dynamic threshold adjustment: With this feature, the Communication Manager can compare actual service levels with service targets and to adjust overload thresholds. This feature makes the use of overload agents more efficient.

- Logged-in advocate agent counting: The logged-in advocate agent counting feature counts agents toward the advocate agent limit if a service objective, percent allocation, or a reserved skill is assigned to the agent login ID, or if one of the agent skills is assigned least occupied agent or service level supervisor.
- Percent allocation distribution: With this feature, the Communication Manager can distribute calls to auto reserve agents by comparing a reserve agent work time in a skill with the target allocation for that skill.
- Reserve agent time in queue activation: This feature activates a reserve agent if the expected wait time (EWT) exceeds a pre-determined threshold or if the call time in the queue exceeds the administered service level supervisor threshold.

Related links

Avaya Basic Call Management System on page 26

Mobility

Communication Manager supports extensive mobility features — Extensive in-building or in/out building wireless choices and hot desking features like Extension to Cellular (EC500), Personal Station Access (PSA) and Automatic Customer Telephone Rearrangement (ACTR) extend Communication Manager features to users, no matter where they are working.

Communication Manager mobility features include:

- With Administration Without Hardware, you can administer telephones that are not yet physically present on the system. This hastens to setting up and making changes to the telephones on the system.
- With Automatic Customer Telephone Rearrangement (ACTR), you can move a telephone to be unplugged from one location to a different location without additional switch administration. The switch automatically associates the extension to the new port.
- Avaya Wireless Telephone Solutions (AWTS) is fully integrated with Communication Manager and you can have a full access to Communication Manager features from a mobile telephone.

  Note:

  Avaya Wireless Telephone Solutions (AWTS) replaces the DEFINITY Wireless Business System (DWBS).

- The Avaya Extension to Cellular (EC500) feature expands mobile services, including:
  - One-number availability
  - Increased user capacities
  - Flexibility across facilities and hardware
  - More control over unauthorized usage
  - Enhanced enable/disable capability
  - Increased serviceability

- Support of IP trunk facilities

To define call treatment options for EC500 calls, you can use up to 99 configuration sets defined in the system. If you set the **Cellular voice mail detection** field, an EC500 call does not cover the cellular voice mail. When the call server detects that the call is covered to the cellular voice mail, the call server returns the call to the server.

- **Note:**

  In the One-X mobile environment, you can edit the values of the **Cellular voice mail detection** field, and the **Call log notify** field. All other fields are read-only.

Communication Manager 6.3.2 introduces additional security for the EC500/One-X Mobile Lite call (AEFSC) feature. With this feature, when a user calls a Feature Name Extension (FNE) from a cellular phone, the system authenticates the call with the station security code (SSC). The call fails without the valid SSC. When a caller wants to make an EC500 call, the caller must dial the SSC after the FNE number. For example, <FNE> [Dial tone] <SSC> # [Dial tone or confirmation tone] <Subsequent digit or extension>.

The integration of Microsoft Office Communicator (MOC) with Communication Manager through ASAI supports bridging, using two user functions simultaneously. For example, the user can be on an active call on a desk phone and, at the same time, be on an active call on an off-PBX destination, such as a mobile phone.

- E911 ELIN for IP wired extensions automates the process of assigning an emergency location information number (ELIN) through an IP subnetwork (“subnet”) during a 911 call. The ELIN is then sent over CAMA or ISDN PRI trunks to the emergency services network when 911 is dialed.
- With the Personal Station Access (PSA) feature, you can transfer your telephone station preferences and permissions to any compatible telephone. PSA has several telecommuting applications. For example, several telecommuting employees can share the same office on different days of the week. The employees can easily and remotely make the shared telephone “theirs” for the day.
- The SIP Visiting User (SIP VU) feature enables users with the 9620 or 9630 SIP telephone to log in to any SIP telephone in the enterprise and receive their individualized services, including menus, contacts, and buddy lists.

  The SIP Visiting User feature relies on specialized firmware on the telephone, and requires SIP VU administration.
- Use the Terminal Translation Initialization (TTI) feature to merge an X-ported extension to a valid port or separate an extension from a port. You use TTI to move telephones. However, you can also use TTI to connect and move attendants and data modules. Terminal Translation Initialization (TTI) also works with Administration Without Hardware (AWOH).
- The TransTalk 9000 is a single-zone or dual-zone, an in-building wireless system that provides a mobility solution on Communication Manager-based systems. It delivers the benefits and accessibility of a wireless telephone with all the power and functionality of a wired desk telephone.

- X-station mobility enables remote users to access switch features. X-station mobility enables certain OEM wireless telephones remoted over a PRI trunk interface to be controlled by Communication Manager as if the telephones were directly connected to the switch.
- With the Multiple Device Access (MDA) feature, a SIP user can register more than one SIP device with a single extension. For example, a user has a J169 at his desk, a 9641 in his lab, and an Equinox client on his laptop, and all the devices are registered with the same extension 123456. When a call arrives at extension 123456, all the devices are alerted. The user can answer the call from any one of the devices. If required, to bridge the call from one of the idle devices, the user can select an active call appearance. Therefore, the call can be handed off between devices without parking the call.
- The Enterprise Mobility experience (EMX) feature enables the configuration of up to four ring extensions using Avaya Workplace Client. This licensed feature starts with the Communication Manager version 10.1.2. You cannot configure the EMX application if EC500 or ONEX application is configured for a primary station.

Collaboration

Communication Manager contains a variety of features aimed at providing easy ways to collaborate with groups of peers, customers, and partners such as executives, salespeople, and professional specialists. These key workgroups require a high level of effective interaction that Communication Manager delivers.

Conferencing:

- Abort conference: When you press the conference button, and for any reason, you hang up before completing the conference, you must cancel the conference. The original call that was put on soft-hold is put on hard-hold.
- Conference - three-party: The conference button enables single-line telephone users to make up to three-party conference calls without attendant assistance.
- Conference - six-party: The conference button enables multi-appearance telephone users to make up to six-party conference calls without attendant assistance.

  Note:

  For 12 parties to participate in a conference, you must enable the **12–party Conferences** field in the Feature-Related System-Parameters screen.
- Conference or transfer display prompts: Display prompts are based on the user class of restriction (COR), independent of the select line appearance conferencing and no-dial-tone conferencing feature.
- The conference or transfer, or toggle or swap: Use this to toggle between two parties in the middle of setting up a conference call before connecting all parties together, or to consult with both parties before transferring a call.
- The group listen: Simultaneously activates your speaker phone in listen-only mode and your handset or headset in listen-and-speak mode. You can serve as a spokesperson for a group. You can participate in a conversation while everyone else in the room is listening to what is said.

Note:

This feature is not supported on IP telephones.

- Hold or unhold conference: A user can use the Hold button to bring the held party back into the conversation.

Note:

This feature is not available for BRI stations or attendant consoles.

- The Meet-me Conferencing: A person can set up a dial-in conference of up to six parties. The Meet-me Conferencing feature uses call vectoring to process the conference call setup.
- No dial tone conferencing: This feature can eliminate user confusion over receiving dial tone when conferencing two existing calls.
- No hold conference: This feature enables a user to add another party to a conference call automatically while continuing the conversation of the existing call.
- Select line appearance conferencing: If you are in a conversation on line “b”, and another line is on hold, or an incoming call is alerting on line “a”, then pressing the CONF button bridges the calls together. Using the select line appearance feature on Communication Manager, the user can press a line appearance button to complete a conference instead of pressing CONF a second time.
- The selective conference party display: Any user on a digital station with a display or an attendant console can use the display to identify all other parties on a two-party or conference call.
- Selective party drop: User can selectively drop the party currently shown on display with a single button push. This can be useful during conference calls when adding a party that does not answer and the call goes to voicemail.
- Selective conference mute: A conference call participant, who has a display station, can mute a noisy trunk line. Selective conference mute is also known as far-end mute.
- Enhanced SIP Signaling: Using the Enhanced SIP Signaling feature, you can:
  - see a roster of conference participants and drop the selected participants for Communication Manager-based conferences.
  - enable audio conferences, facilitated by Avaya Aura® Conferencing Release 7.0.
  - enhance the behavior of sequenced applications in a Communication Manager Feature Server environment.

Multimedia calling:

Multimedia calls are initiated with voice and video only. Once a call is established, one of the parties may initiate an associated data conference to include all of the parties on the call who can support data.

- Multimedia call early answer on vectors and stations: Early answer is a feature applied to multimedia calls in conjunction with voice conversion.

- Multimedia call redirection to multimedia endpoint: A dual port multimedia station can be a destination of call redirection features such as call coverage, forwarding, and station hunting. The station can receive and accept full multimedia calls or data calls converted to multimedia.
- Multimedia data conferencing (T.120) through an ESM: An adjunct device called an Expansion Services Module (ESM) controls data conference.
- Multimedia hold, conference, transfer, and drop: Station users can activate hold, conference, transfer, or drop on multimedia calls. Multimedia endpoints and voice-only stations can participate in the same conference.
- Multimedia queuing with voice announcement: When multimedia callers queue for an available member of a hunt group, they can hear an audio announcement.

Paging and intercom:

- Code calling access enables attendants, users, and tie trunk users to page with coded chime signals.
- Group paging enables a user to announce to a group of people using speakerphones. The speakerphones are automatically turned on when the user begins the announcement.
- Intercom - automatic: With this feature, users who frequently call each other can do so by pressing one button instead of dialing an extension number.
- Intercom - dial: This feature enables multi-appearance telephone users to call others within an administered group easily. The calling user lifts the handset, presses the dial intercom button, and dials the one-digit or two-digit code assigned to the desired party.
- Loudspeaker paging access provides attendants and telephone users dial access to voice paging equipment. Communication Manager can provide nine paging zones and one zone activates all zones simultaneously.
- Manual signaling enables one user to signal another user. The receiving user hears a two-second ring. The signal is sent each time the signaling user presses the button. The meaning of the signal is prearranged between the sender and the receiver. Manual signaling is denied if the receiving telephone is already ringing from an incoming call.
- Whisper page enables an assistant or colleague to bridge onto your telephone conversation and give you a message without being heard by the other party or parties you are talking to. Whisper page works on certain types of telephones.

Team button:

The Team button feature is used to monitor members of a team of stations. The monitoring station is notified about its general redirection state. Starting from Release 6.3.6 of Communication Manager, direct transfer, transfer upon hang-up, and override SAC/CFWD/EC features can be used with the **Team** button feature.

Call routing

Call routing features are designed to reduce networking costs by effectively using IP Trunking over WAN or LAN links.

Call Routing features include:

- Automatic routing: Communication Manager provides various automatic routing features for public and private networks. Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) are the foundation for these automatic-routing features. They route calls based on the preferred (normally the least expensive) route available when the call is placed.
- Enbloc Dialing and Call Type Digit Analysis: With this feature, users can automatically place outgoing calls based on the telephone number information in the call log of the telephone, without the user modifying the telephone number.
- Generalized route selection: This feature provides voice and data call-routing capabilities. You use it to select the least-cost routing and optimal routing over the appropriate facilities. To enhance AAR and ARS, it provides additional parameters in the routing decision and maximizes the use of the right facility to route the call.
- Multiple Location Support: This feature enables local user time, local ARS Public Analysis Tables for local trunking, automatic Daylight Savings Time, enhances shared resource algorithms (touch tone receivers), and other features, when Avaya Media Gateways are remoted off of a central server at a different location.
- Alternate facility restriction levels: With these levels, Communication Manager can adjust facility restriction levels or authorization codes for lines or trunks. Each line or trunk is normally assigned a facility restriction level. With this feature, Alternate Facility Restriction Levels are also assigned.
- Traveling Class Marks: A mechanism for passing the facility restriction level of a caller from one Electronic Tandem Network switch to another. Traveling Class Marks enables privilege checking to be passed across switches through the Electronic Tandem Network.
- Answer detection: For Call-Detail Recording (CDR), it is important to know when the called party answers a call. Communication Manager provides three ways to determine whether the called party has answered an outgoing call — answer supervision by time-out, call-classifier board, and network answer supervision.
- Source-based routing: With the source-based routing feature, Communication Manager sends the location information of H.323, DCP, and analog stations to Session Manager. Session Manager uses the IP address to select the matching trunk or route pattern and then routes the call to destination stations.
- With QSIG Call Coverage, a call rerouted or forward-switched by QSIG uses the call coverage path of the diverted-to party. Based on the Communication Manager configuration, the greeting of the administered party is played to the caller.
- Delayed drop: You can use the **Interworking of ISDN Clearing with In-Band Tones** field on the SIP Trunk form to communicate the reason for the call drop to the caller. After knowing that the called party will not answer the call, the caller or the Voice Portal agent can decide whether to wait for the announcement to complete or drop the call.
- Inter-Gateway Alternate Routing: IGAR provides enhanced Quality of Service (QoS) to large distributed single-server configurations. You can use IGAR for configurations where the IP network is not reliable enough to carry bearer traffic. If you have multiple IP networks available, you can use H.323 or SIP trunks for IGAR instead of the PSTN. Communication

Manager Release 6.3.5 and earlier supported IGAR for analog, DCP, and H.323 endpoints. From Release 6.3.6 onwards, IGAR support is extended to SIP endpoints.

Telecommuting and Remote Office

Telecommuter capabilities route calls appropriately and give employees access to the full Avaya Aura Communication Manager feature set whether working at home, in the office, or on the road.

Communication Manager supports the following telecommuting features:

- Coverage of calls redirected off-net: With Coverage of calls redirected off-net (CCRON), calls redirected to locations outside of the switch to return to the switch for further processing.
- Extended user administration of redirected calls (telecommuting access): With Extended user administration of redirected calls (also called telecommuting access) enables you to change the lead call coverage path or forwarding extension from any on-site or off-site location.
- Off-premises station: A trunk-data module connects off-premises private-line trunk facilities and Communication Manager.
- Remote access permits authorized callers from remote locations to access the system via the public network and use its features and services. There are a variety of ways of accessing the feature.

Telephony

Communication Manager provides comprehensive end-user telephony features (such as auto attendant, call transfer, call forward) that facilitate effective communications among employees, customers, and partners.

Mid-call features:

Communication Manager ensures that mid-call call telephony features work when Avaya endpoints establish video calls with Radvision endpoints. Customers can use video mute, unmute, transfers, and conferences during a video call.

Exclusion:

Users can maintain the privacy of their telephonic conversations and ensure that unwanted parties cannot join the call. You can use Exclusion with Extension to Cellular, Bridge Call Appearance, Service Observing, and Multiple Device Access.

Concurrent call management:

If the Limit Number of Concurrent Calls (LNCC) feature is enabled on a station, Communication Manager restricts the number of incoming calls to one call at a time. If the user is busy, the subsequent incoming calls receive a busy tone. Communication Manager Release 6.2 and earlier supported this feature on H.323 and DCP telephones. Communication Manager Release 6.3 extends this support to SIP telephones.

Automatic Number Identification (ANI):

Displays the telephone number of the calling party on your telephone. The system uses ANI to interpret calling party information signaled over multifrequency (MF) or Session Initiation Protocol (SIP) trunks. Any display telephone can use ANI.

For H.323 and DCP endpoints, the caller information on the bridged call appearances can be set to be the same as the caller information on the principal station. To enable this feature, set the Match BCA Display to Principal field on page 2 of the Class of Service screen to y.

Call log support

Communication Manager records all missed calls in the missed call log of 94xx deskphones.

Call log support for busy 94xx deskphones

Communication Manager records all incoming calls when a 94xx deskphone is busy because:

- All but one call appearances reserved for incoming calls are in the non-idle state. The last call appearance is reserved for outgoing calls.
- All call appearances are in the non-idle state.
- The Do Not Disturb feature is active on the endpoint.
- One call appearance is busy on a call because a remote user has put the call on hold or started a transfer or a conference call.

Supported number of digits in a call log

For a direct incoming external call from an ISDN or a SIP network, Communication Manager displays up to 21 digits of the calling-party number on a DCP, an H.323, or a SIP endpoint. Earlier, Communication Manager displayed only 7 digits of the calling-party number.

The missed call log and the answered call log of the endpoints display all 21 digits. Communication Manager also stores all 21 digits of an incoming external call from an ISDN or SIP network that is redirected by coverage, forwarding, bridging, or a similar feature in the missed call log and the answered call log of the endpoints

Online/Offline Call Journal (Call History)

With the Online/Offline Call Journal (Call History) feature, the SIP and H.323 phone users can view the call log entries when the user logs in from a different H.323 or SIP device. The SIP and H.323 users receive the logs for all answered and unanswered calls while the phones were in the logged-out state. With this enhancement, the H.323 and SIP desk phones back up all the call logs and restore them when the user logs in.

Communication Manager backs up to 10 calls for the logged out H.323 users. Communication Manager does not back up or restore the log for calls that are answered or unanswered by the H.323 phones when in the logged-in state. The H.323 phones continue to use HTTP for this purpose.

Call notification

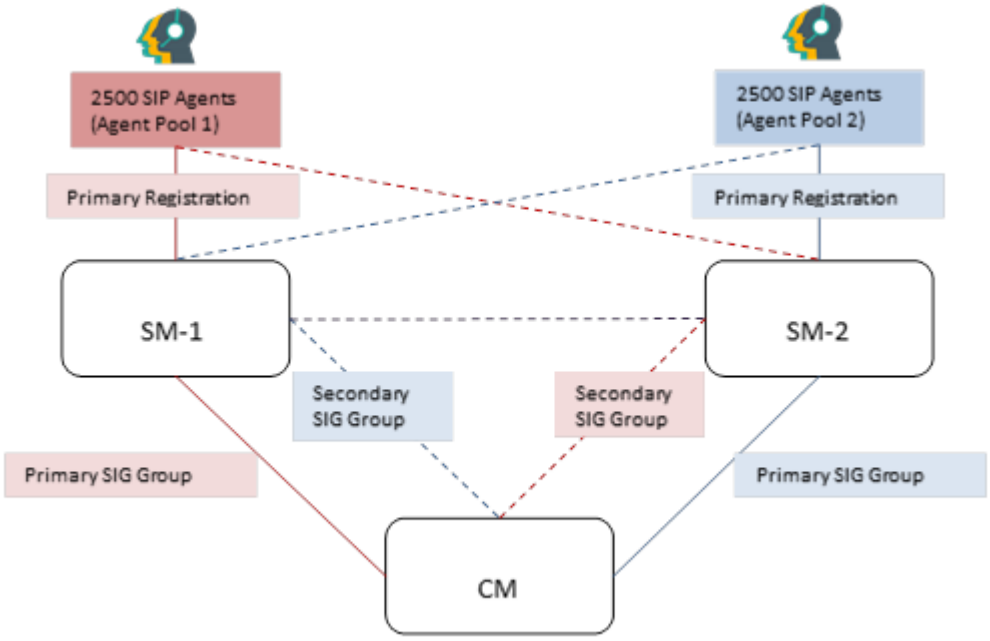
SIP undelivered call notification:

The SIP undelivered call notification feature provides a notification about the undelivered call to the endpoint. Communication Manager initiates the SIP undelivered call notification feature when a SIP endpoint receives a call in one of the following situations:

- All call appearances are busy.
- LNCC is activated, and the endpoint is busy.
- Call Forward Busy or Call Forward All is enabled.
- Enhanced Call Forward (ECF) unconditional or ECF busy is enabled.
- Cover All Calls is enabled.

SIP trunk optimization

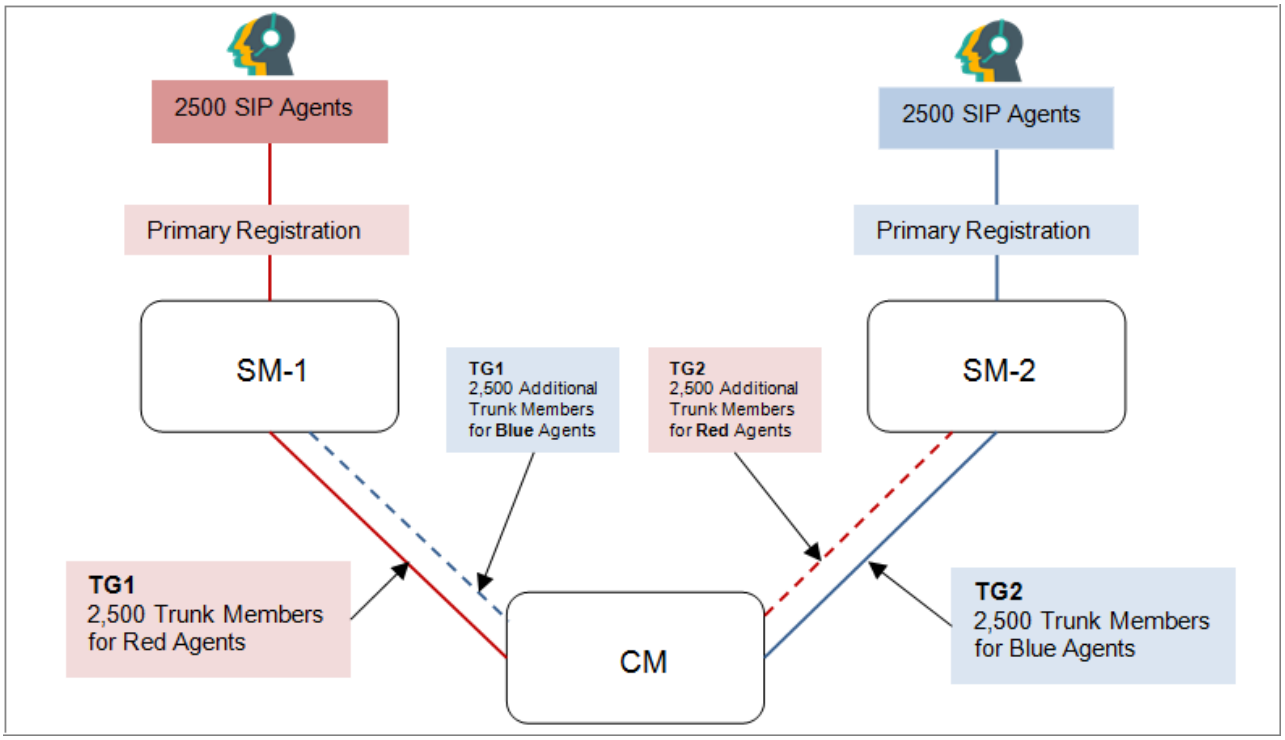
The SIP trunk optimization feature eliminates the need for provisioning trunks for redundancy. This feature frees up trunks so that the available trunks can be used by SIP agents, SIP stations, or PSTN bound SIP trunk calls. The following illustration explains the problem of trunk consumption due to redundancy.



The above figure provides the following two scenarios:

- First scenario: When the connection between Communication Manager and Session Managers work fine.
- Second scenario: When the connection between Communication Manager and Session Manager fails.

In the first scenario, if Communication Manager wants to reach the red agents (agent pool 1), it can do so by utilizing the red trunk between Communication Manager and Session Manager-1. Similarly, if Communication Manager wants to reach the blue agents (agent pool 2), it can do so by utilizing the blue trunk between Communication Manager and Session Manager-2.



In the second scenario, administering additional trunks provide a solution for giving service to red and blue agents, but introduces few other problems.

- The additional trunk members administered for redundancy remain unused in the first scenario when entity links to Session Manager-1 and Session Manager-2 are in service.

  Note:

  When the policy-based assignment is enabled in System Manager, you can administer up to four Session Managers for a SIP station.
- Double the number of trunks must be provisioned to cover a rarely occurring second scenario. Given the limited trunk members on Communication Manager, using trunks for redundancy reduces the trunks required for actual traffic.
- Routing and administration of route patterns become complex.

For provisioning connectivity to Session Manager-1 and Session Manager-2, Communication Manager has to create two signaling groups:

- Signaling group to Session Manager-1: Near-End as procr and Far-End as Session Manager-1
- Signaling group to Session Manager-2: Near-End as procr and Far-End as Session Manager-2

Each signaling must have 5000 trunks provisioned with Session Manager-1 and 5000 trunks to be provisioned with Session Manager-2 as described earlier.

SIP trunk optimization feature enables each signaling group to point to multiple Session Managers. In this particular case, a signaling group will point to both Session Manager-1 and Session Manager-2. This is achieved by pointing the signaling group to a cluster of Session Managers. An SM cluster can have 28 Session Managers. With a Session Manager cluster, it is

assumed that all Session Managers share a similar configuration, and any Session Manager can route a call to the far end station or far-end trunk.

The ability of the signaling group to point to both Session Managers reduces the required trunks to be administered on Communication Manager by half while achieving full redundancy. If the link to Session Manager-1 fails, the Signaling group uses the link to Session Manager-2 to route all the outgoing traffic. The effect of one signaling group pointing to multiple Session Managers is as follows:

- Signaling group remains in service if at least one Session Manager administered in the cluster is reachable.
- Trunk group remains in service, and all members administered in the trunk group can deliver traffic.
- For example, a trunk group with 5000 members in the first scenario can service 2500 agents on Session Manager-1 and 2500 agents on Session Manager-2. If the connectivity between Communication Manager and Session Manager-1 goes down, the same trunk group with 5000 members can service 2500 agents on Session Manager-1 and 2500 agents on Session Manager-1 and 2500 agents on Session Manager-2 through the link between Communication Manager and Session Manager-2. Even if Session Manager-1 goes down and all agents move to Session Manager-2, the same 5000 members can reach all the 5000 agents.

The SIP trunk optimization feature are as follows:

- Number of trunk members is 9,999 for SIP trunk groups.
- Number of SIP agents is 10,000.
- System-wide trunk members is 30,000.
- Measured trunks is 30,000.
- TLS connections for SIP is 56 from 32 to support 28 Session Managers because two links are required to support each Session Manager.
- SIP Station form directly points to its Primary and Secondary Session Manager to support 28 Session Managers because two links are required to support each Session Manager. For more information about the capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

  Note:

  When the policy-based assignment is enabled in System Manager, you can administer up to four Session Managers for a SIP station.
- Look Ahead Routing feature is deprecated for SIP station calls if routed over clustered signaling group.
- Route pattern can now specify a network region.

Survivability specification

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

Survivable core server

With survivable core servers, Communication Manager operates during a network outage. A survivable core server provides survivability support to IP networks and 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 Gateway operating within networks. Survivable remote servers take over segments that lose 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 Branch Gateway when the connection to the core server fails. This survivability option is available for Communication Manager and Session Manager.

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

Note:

If you have an S8300 server configured in embedded CM main, survivable remote, or embedded survivable remote configurations, migrate to Avaya Solutions Platform S8300.

Dial plan specification

The Dial Plan feature supports intra-server dialing for extensions at the main server and 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 a maximum of 16 digits. To extend the extension length to 18 digits, you can 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*.

SIP

SIP provides the foundation for multimedia communications and collaboration for voice, video, and customer contact. SIP-based presence and Instant Messaging (IM) lets users inform others of their status, availability, and provides immediate responsiveness to important business issues.

In conjunction with Avaya Aura® Session Manager, Communication Manager provides complete feature enablement for SIP devices, support for SIP trunking, and integration of third-party SIP solutions.

Emergency calling services

Using Communication Manager, you can manage and respond to unforeseen emergencies. With the Enhanced 911 (E911) feature, you can access your local public safety agency quickly. The public safety agency can dispatch the appropriate response team during fire, accident, crime, or medical agency.

Supported Footprints

For more information about supported footprints, see *Upgrading Avaya Aura® Communication Manager*.

Chapter 3: Interoperability

Supported endpoints

Avaya Aura® Communication Manager supports the following communication devices:

- Analog devices
  - Avaya analog telephones
- Digital devices
  - Avaya digital deskphones and telephones
  - Avaya DECT Handsets
- IP-based devices
  - Avaya IP deskphones
  - Avaya one-X® IP Telephones
  - Avaya IP wireless telephones
  - Avaya IP conference phones
  - 96x1 H.323 and 96x1 SIP Deskphones
  - Avaya Attendant Console
  - Avaya J100 Series IP Phones
  - Avaya Equinox SIP Attendant

For the list of latest supported endpoints, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Supported servers

You can deploy the Communication Manager using the following OVA types:

- **Simplex:** For one Communication Manager server in your environment, use simplex OVA.
- **Duplex:** For a standby Communication Manager server, use duplex OVA. The standby server becomes active when the main server goes down. To deploy the Duplex OVA, install the Duplex OVA on two different hosts.

The following table provides information about servers compatible with each OVA:

OVA type	Server configuration	Supported server (Avaya™ supplied)
Simplex	• Main • Survivable Core • Survivable Remote	• Avaya Solutions Platform S8300 release 5.1.x and later versions • Avaya Solutions Platform 130 Server release 5.1.x and later versions
Duplex	• Main • Survivable Core	• Avaya Solutions Platform 130 Server release 5.1.x and later versions

For more information on customer-provided virtualized environment, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

Note:

If you have an S8300 server configured in embedded CM main, survivable remote, or embedded survivable remote configurations, migrate to Avaya Solutions Platform S8300.

Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. Avaya Solutions Platform future release (Release 6.x) will support ESXi 8.0. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. Updating directly from Dell or VMware's website results in an unsupported configuration.

For information about capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

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

Operating System Capability

For more information on operating system capability, see *What's New in Avaya Aura® Release 10.2*.

Product compatibility

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

Chapter 4: Performance specification

Capacity and scalability specification

For information about system capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

Traffic specification

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

- Static occupancy
- Call processing occupancy
- System management occupancy

As system management functions fluctuate, 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 that agents handle.
- 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 the *Avaya Aura® Core Solution Description* guide.

Chapter 5: Security specification

Communication Manager security, privacy, and safety

Communication Manager provides security features to detect potential breaches, take measures to protect the system, track activities, and for notification. It also provides real-time media encryption for environments where enhanced voice privacy over a LAN or WAN is required.

Communication Manager supports the following:

- Industry Standard Secure Real Time Protocol (SRTP) for authentication and media encryption for audio and voice media streams. Additionally, SRTCP encryption is supported
- Real-Time Media and Signaling Encryption
- Access Security Gateway
- Malicious Call Tracking
- Toll Fraud Protection
- Emergency Calling Services (E911)

Communication Manager supports identity certificates and trusted CA certificates with enhanced signatures, such as SHA2 and 2048 key length. Certificate Management enables receiving and validating both existing certificates with SHA1-1024 signature and new certificates with SHA2-2048 signature.

For more information see: *Administering Avaya Aura® Communication Manager*

You can isolate Communication Manager telephony servers from the rest of the enterprise network to safeguard them from viruses, worms, Denial of Service (DoS), and other attacks. Communication Manager uses the minimum number of services and access ports to reduce susceptibility to malicious attacks. It employs encryption between servers, gateways, and endpoints to secure the voice stream and signaling channels.

Supported media encryption algorithms

The use of AEA and AES is discouraged as these are older Avaya-proprietary-encryption techniques.

Avaya security recommends to use the following types of encryption techniques:

- srtp-aescm128-hmac80
- srtp-aescm128-hmac32

- srtp-aescm256-hmac80
- srtp-aescm256-hmac32
- none (non-encrypted call connection).

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.

Because all the authentication keys are dynamically created and assigned, the system stores these keys only in RAM. Administrators or users cannot access these keys. RTP keys are not escrowed.

SRTCP provides the ability to encrypt the control channel associated with the SRTP media stream. These two channels normally reside on adjacent UDP ports.

Key exchange details

Key agreement is performed using Diffie-Hellman techniques.

TLS connections can now be used between Communication Manager and the H.248 or H.323 endpoint gateways.

Chapter 6: Licensing requirements

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.

- Prior to Communication Manager R10.2.1.1, if the 30-day grace period expires before a valid license file is installed, Communication Manager enters the License Restricted mode. In this mode, the Communication Manager blocks only the system administration activities.
- Beginning with Communication Manager R10.2.1.1, if the 30-day grace period expires before a valid license file is installed, Communication Manager enters the License Restricted mode. In this mode, the Communication Manager blocks call processing, including emergency calls, and system administration activities. This is applicable only for Main Communication Manager server. For Enterprise Survivable Server (ESS) and Local Survivable Processor (LSP), only the system administration activities is blocked.

Communication Manager uses the Avaya PLDS or Product Licensing and Delivery System to manage license entitlements and generate license files. The license file contains information regarding the product, major releases, license features, and capacities. Avaya PLDS provides the ability to move licenses between Communication Manager servers if the support offer and the move policy are followed.

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).

Centralized licensing

The Centralized Licensing feature is available for most Avaya products. You can use the Centralized Licensing feature to 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 on a simplex or a 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 Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Communication Manager server.

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

Licensing in the Communication Manager Distributed Architecture

The new Communication Manager OVA parameters provide for the CM operation in the array mode. The following cluster modes are available:

- Master CM
- Node CM
- Standalone

The Communication Manager shall retrieve this parameter from the */etc/ecs.conf* file.

Note:

If this field is missing in the */etc/ecs.conf* file, the CM assumes that the array mode is standalone.

License activation

The Master CM server consumes the license allocated for it on the WebLM server. Then, it expands the configured features and capacities to the Node CM servers by synching the local copy of the license file (lsfile) in */etc/opt/ecs* directory. If the user updates the license on the Master CM, that update applies to the Node CMs, respectively. A Node CM server does not get a license from the WebLM server because it has no connection to the WebLM server. Instead, the Node CM server enables features and update license limits based on the lsfile it receives from the Master CM.

After it consumes the license from the WebLM server, the Master CM reports back to the WebLM server the capacities it takes, that is the full capacities assigned to the array, except for the AAMS channels, H.323 registrations, and Logged-in Agents.

AAMS Channel license usage

The Master CM server consumes the licensed AAMS channels and passes the capacities with the license file to the Node CMs.

The CMs in the array share their AAMS channel usage with the other CMs in the array. When granting channels to a new call, the total number of channels used by all CMs in the array is applicable. A CM denies channels if their total number exceeds the licensed maximum.

H.323 Registrations

The Master CM server consumes the licensed H.323 registrations and passes the capacities with the license file to the Node CMs. The following are the limits to the registrations the CMs in the array receive:

- Maximum Concurrently Registered IP Stations: *18,000*
- Maximum Concurrently Registered IP eCons: *414*
- Maximum Concurrently Registered Unauthenticated H.323 Stations: *100*

Chapter 7: Resources

Communication Manager documentation

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

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Overview and Specification	Provides an overview of the features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Security Design	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
LED Descriptions for Avaya Aura® Communication Manager Hardware Components	Describes the LED for hardware components of Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware requirements for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Survivability Options	Describes the system survivability options for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Core Solution Description	Provides a high level description for the solution.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides procedures to maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues…

Title	Description	Audience
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides commands to monitor, test, and maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Alarms, Events, and Logs Reference	Provides procedures to monitor, test, and maintain Avaya servers and describes the denial events listed on the Events Report form.	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
Avaya Aura® Communication Manager SNMP Administration and Reference	Describes SNMP administration for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Avaya Aura® Communication Manager Server Options	Describes server options for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Data Privacy Guidelines	Describes how to administer Communication Manager to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager on a software-only environment and Amazon Web Service, Microsoft Azure, and Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

Title	Description	Audience
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
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
Avaya Aura® Communication Manager Screen Reference	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that specific customers request for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.

- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing 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 https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Glossary

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.
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.
Session Manager	An enterprise SIP proxy registrar and router 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. System Manager can also function as a self-signed Root Certificate Authority (CA) or as an intermediate CA. System Manager enables the Simple Certificate Enrollment Protocol (SCEP) application to sign certificates for Avaya deskphones.

Index

O

P

R

S

T

V

W