Avaya Aura® Core Solution Description

Release 10.2.x
Issue 7
May 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.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

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

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction

Purpose

This document describes Avaya Aura® core solution from a holistic perspective focusing on the strategic, enterprise and functional views of the architecture. This document also includes a high-level description of each verified reference configuration for the solution.

This document is intended for people who want to understand how the solution and related verified reference configurations meet customer requirements.

Product compatibility

For the latest and most accurate compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Change history

Issue	Date	Summary of changes
7	May 2025	Updated the following section: • Topology on page 18

Table continues…

Issue	Date	Summary of changes
6	March 2025	Updated the following sections: • Hardware components on page 33 • Avaya Aura Application Enablement Services overview on page 14 • Supported servers for Avaya Aura applications on page 34 • IP/SIP telephones and softphones on page 136 Updated the product name from “Avaya Cloud Office” to “Avaya Cloud Office Hybrid” Deleted the following topics: • Avaya EVAT Assessment Tool - Avaya EVAT overview • Message Networking
5	December 2024	Added the following sections for Release 10.2.1: • Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 39 • Support for KVM components on page 21 • Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10) on page 20 Updated the following sections for Release 10.2.1: • Hardware components on page 33 • Software-only environment overview on page 21 • Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura application OVAs on page 36 • Supported servers for Avaya Aura applications on page 34 • Solution Deployment Manager overview on page 28 • Solution Deployment Manager Client on page 29
4	May 2024	Updated the section: Software-only environment overview on page 21 Updated the section: Hardware components on page 33
3	April 2024	Updated the section: Hardware components on page 33 Updated the section: Avaya Aura applications deployment offers on page 17
2	March 2024	Added the section: CDR information in Avaya Aura core solution on page 30
1	December 2023	Release 10.2.

Chapter 2: Solution overview

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

Topology

The following depicts the Avaya Aura® architecture and various components of Avaya Aura®:

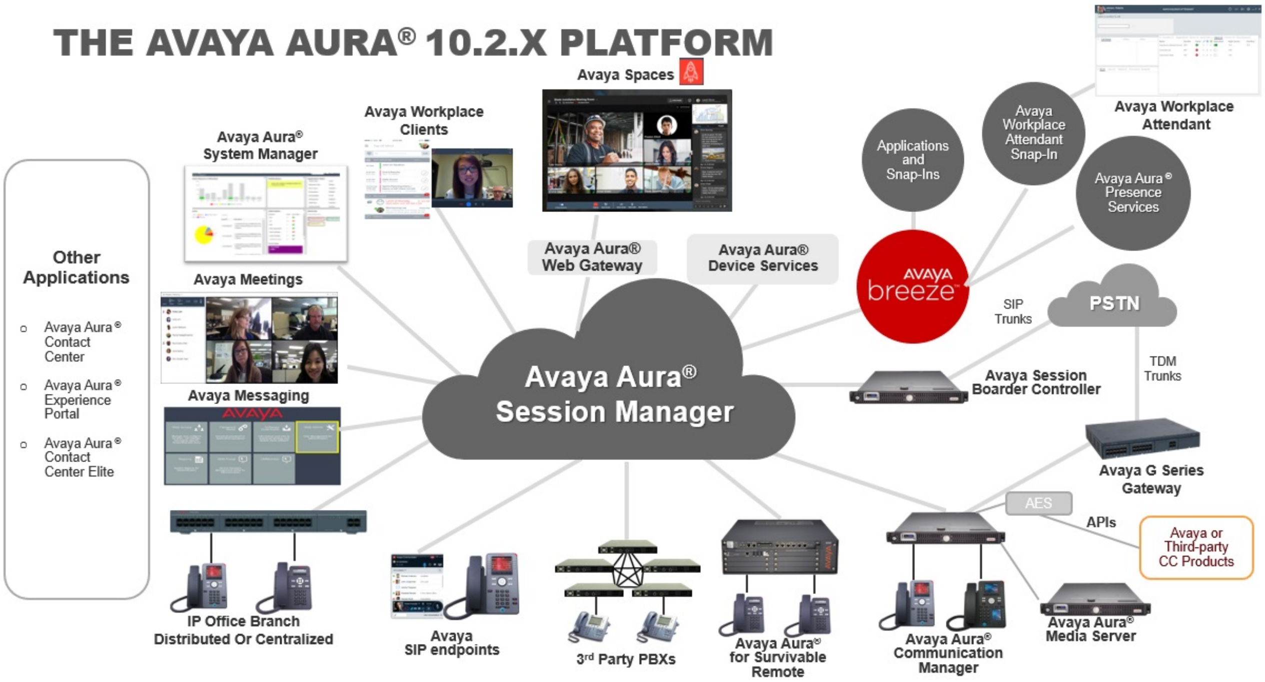

THE AVAYA AURA® 10.2.X PLATFORM
Avaya Spaces
Avaya Workplace Attendant
Avaya Workplace Clients
Avaya Aura® System Manager
Applications and Snap-Ins
Avaya Workplace Attendant Snap-In
Avaya Aura® Presence Services
Other Applications
Avaya Aura® Contact Center
Avaya Aura® Experience Portal
Avaya Aura® Contact Center Elite
Avaya Meetings
Avaya Aura® Web Gateway
Avaya Aura® Device Services
AVAYA breeze
SIP Trunks
PSTN
Avaya Messaging
Avaya Aura® Session Manager
Avaya Session Boarder Controller
TDM Trunks
Avaya G Series Gateway
AES
APIs
Avaya or Third-party CC Products
IP Office Branch Distributed Or Centralized
Avaya SIP endpoints
3rd Party PBXs
Avaya Aura® for Survivable Remote
Avaya Aura® Communication Manager
Avaya Aura® Media Server

Figure 1: Avaya Aura® Architecture

A standard Avaya Aura® architecture consists of the following core components:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services
- Avaya Aura® Media Server
- Avaya Aura® Presence Services

System Manager provides a common console to manage the Avaya Aura® applications. System Manager also enables to bulk import and export users, including user profiles and global settings such as public contacts lists, shared addresses, and presence access control lists.

Session Manager provides core SIP routing and integration services that provide communication between SIP-enabled entities, for example, PBXs, SIP proxies, gateways, adjuncts, trunks, and applications across the enterprise. Session Manager is configured from System Manager and uses centralized, policy-based routing to provide integration services. It also sends and receives SIP notifications and SIP Publish messages to and from various endpoints and Presence Services.

Endpoints registered to Session Manager use Communication Manager for feature support. Endpoints that use H.323 protocol register to Communication Manager over IP. Digital and analog endpoints are directly connected to their respective digital and analog media modules on a Branch Gateway, for example, G450.

Communication Manager is an extensible, scalable, and secure telephony application that connects to private and public telephone networks, ethernet LANs, and the internet. Communication Manager organizes and routes voice, data, image, and video transmissions.

Application Enablement Services is a software platform that leverages the capabilities of Avaya Aura® Communication Manager to enterprise applications. By using Application Enablement Services, the Application Enablement Services Collector component within Presence Services enables Presence Services to report telephony presence from Communication Manager endpoints. The Application Enablement Services Collector collects Presence from H323, DCP, analog, and SIP telephones administered as OPTIM extensions.

The Avaya Aura® Media Server delivers advanced multimedia processing features to a broad range of products and applications. Utilizing the latest open standards for media control and media processing, the highly scalable software based solution deploys on standard server hardware, running Linux or Windows operating systems.

Presence Services collects, aggregates, and publishes presence information from and to multiple sources and clients.

Avaya Aura® core components

Avaya Aura® contains the following core components:

- Avaya Aura® System Manager Release 10.2.x
- Avaya Aura® Communication Manager Release 10.2.x
- Avaya Aura® Session Manager Release 10.2.x
- Avaya Aura® Application Enablement Services Release 10.2.x
- Avaya Branch Gateway Release 10.2.x
- Avaya Aura® Media Server Release 10.1.x
- Avaya Aura® Presence Services Release 10.1.x
- Avaya WebLM Release 10.1.3.1

Note:

From Release 10.2 and later, Avaya Aura® does not support Avaya Device Adapter Snap-in.

System Manager overview

Avaya Aura® System Manager is a central management system that provides a set of shared management services and a common console. All shared and element-specific management for Avaya Aura® applications that System Manager supports is performed from the common console. System Manager provides the following key capabilities:

- Centralized software management solution to support deployments, migrations, upgrades, and updates to the suite of Avaya Aura® applications.

- Avoid duplicate data entry through shared management services.
- Centralized access to all Avaya Aura® applications through a browser-based management console with single sign on.
- Optimization of IT skill sets with consistency of management functions across Avaya solutions.
- Integration with enterprise IT infrastructure, such as identity management, authentication, authorization, security, and enterprise directory

Communication Manager overview

Communication Manager is an extensible, scalable, and secure telephony application that connects to private and public telephone networks, Ethernet LANs, and the Internet. Communication Manager organizes and routes voice, data, image, and video transmissions.

Key features

- Robust call processing capabilities
- Application integration and extensibility
- Advanced workforce productivity and mobility features
- Built-in conferencing and contact center applications
- E911 capabilities
- Centralized voice mail and attendant operations across multiple locations
- Connectivity to a wide range of analog, digital, and IP-based communication devices
- Support for SIP, H.323, and other industry-standard communications protocols over different networks
- More than 700 powerful features
- High availability, reliability, and survivability

Session Manager overview

Avaya Aura® Session Manager is a SIP routing tool that integrates all SIP devices across the entire enterprise network. Session Manager simplifies the existing communication infrastructure by combining existing PBXs and other communications systems, regardless of the vendor, into a cohesive and centrally managed SIP-based communications network.

Session Manager supports the following features:

- Integration with third-party equipment and endpoints to normalize disparate networks.
- Centralized routing of calls using an enterprise-wide numbering plan.
- Centralized management through System Manager, including configuration of user profiles and deployment of enterprise-wide centralized applications.
- Interconnection with Communication Manager and Avaya Communication Server 1000 to provide multiple feature support for SIP and non-SIP endpoints.

- Interconnection with IP Office through SIP to provide feature support for SIP endpoints.
- Third-party E911 emergency call service for enterprise users.
- Centralized Presence Services for scalability and reduced network complexity with a variety of endpoints and communication servers.
- Support for converged voice and video bandwidth management.
- Application sequencing capability to incrementally deploy applications without needing to upgrade the PBX.
- Geographic redundancy.
- Mobility of SIP telephones and enterprise mobility for SIP users.
- Support for call reconstruction to allow Call Preservation for SIP calls, which provides mid-call features to be invoked after a failover.
- Support to carry Presence Information Data Format Location Object (PIDF-LO) as a Multipurpose Internet Mail Extensions (MIME) body/attachment in a SIP message. Session Manager can also pass the PIDF-LO information in the SIP message.

Avaya Aura® Application Enablement Services overview

Avaya Aura® Application Enablement Services (AE Services) is a software platform that leverages the capabilities of Avaya Aura® Communication Manager. AE Services provides an enhanced set of Application Programming Interfaces (APIs), protocols, and web services that expose the functionality of Avaya Communication solutions to corporate application developers, third-party independent software vendors, and system integrators.

Note:

AE Services supports existing Communication Manager standalone implementations and Avaya Aura® Session Manager configurations with Communication Manager as an Access Server. AE Services does not support Communication Manager as a Feature Server.

AE Services runs on a Linux server and is tightly integrated with Communication Manager and Avaya Contact Center solutions. AE Services provides an open platform for supporting existing applications and serves as a catalyst for creating the next generation of applications and business solutions.

Branch Gateways

Branch Gateways work with Communication Manager software installed on any of the following servers to help deliver communication services to enterprises:

- Avaya Solutions Platform S8300

  You can migrate from Appliance Virtualization Platform Release 8.1.x on a S8300E server to Avaya Solutions Platform S8300 6.0 or later.
- Customer-provided server
- Infrastructure as a Service (IaaS)

- Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660

Branch Gateways connect telephone exchange and data networking by routing data and VoIP traffic over the WAN or LAN. Branch Gateways provide support for IP, digital, and analog devices.

Branch Gateways are controlled by Communication Manager operating either as External Call Controller (ECC) or Internal Call Controller (ICC). In a configuration that includes both ICC and ECC, ICC acts as a survivable remote server (SRS). ICC takes over call control when ECC fails or the WAN link between the main office and the branch office is down.

Branch Gateways also provide the standard local survivability (SLS) when the connection to the primary ECC fails and an SRS is not available. This feature is available only for IPv4 setups.

G430 Branch Gateway

G430 Branch Gateway can support up to 150 users when deployed as a branch gateway in a medium to large enterprise. The configuration requires Communication Manager to be installed on the Avaya Solutions Platform S8300 server or either of Avaya Solutions Platform 130 servers, customer-provided server, Infrastructure as a Service (IaaS), or Software-only environment.

G450 Branch Gateway

G450 Branch Gateway supports up to 450 users in a medium to large enterprise and up to 2400 users when deployed as a campus gateway. Both configurations require Communication Manager to be installed on the Avaya Solutions Platform S8300 server or either of Avaya Solutions Platform 130 server, customer-provided server, Infrastructure as a Service (IaaS), or Software-only environment.

Avaya Aura® Media Server overview

Avaya Aura® Media Server (MS) is a software-based media application platform. Avaya Aura® MS performs all multimedia processing using software rather than using dedicated hardware-based DSP resources. Avaya Aura® MS is designed to run on general purpose operating systems and Commercial Off-The-Shelf (COTS) hardware. Avaya Aura® MS forms the backbone of a flexible communications system for growing companies. Using Avaya Aura® MS, your company can take advantage of the increased functionality of an IP network without replacing the existing infrastructure. Avaya Aura® MS works with media gateways to provide a streamlined voice and data network throughout the enterprise. Avaya Aura® MS and media gateways provide a network built on an industry standard operating system that supports distributed IP networking and centralized call processing. The benefits of Avaya Aura® MS are increased productivity, efficiency, and economic benefits for the enterprise. As Avaya Aura® MS consolidates multiple systems into a single server, you can manage the entire communications infrastructure from one location. Avaya Aura® MS provides scalability, redundancy, and high availability.

Avaya Aura® MS supports SIP TLS, SRTP, VoiceXML 2.1, CCXML 1.0, MRCP, QOS Monitoring, Audio, Video, MLPP, IM, and Webpush features.

Avaya Aura® MS powers diverse applications such as voice messaging, consumer conferencing, self service, contact centers, basic media services, and communication applications.

Presence Services overview

Avaya Aura® Presence Services indicates the presence of a user through the presence states, such as Busy, Away, or Do Not Disturb. The presence is an indication of the availability of the user and the readiness to communicate across services, such as telephony, instant messaging (IM), and video.

The presentity is the visibility of a user on a shared communication network. The users who are a part of the presentity group have access to the presence status of another user. A watcher is a user who monitors the presentity of another user. The watcher must subscribe to Presence Services to receive presence updates for a presentity.

Presence Services supports collecting presence information from diverse sources. This information is aggregated for a user and then made available to the presence-aware applications. When an application subscribes to Presence Services, the application receives presence change notifications that contain the aggregated presence for a user and the communication resources available to the user. By using this information, the application can provide a visual indication about the presence of the user.

Presence Services is compatible with the client software from Microsoft®, IBM® Domino®, and open source. Users can utilize the following collectors to use the core Presence Services capabilities with other presence sources:

- Application Enablement Services collector: To collect telephony presence information from devices that are not presence capable, such as H323, and DCP endpoints administered as OPTIM extensions.
- Exchange collector: To collect the calendar and out-of-office information from Exchange mailboxes.
- Domino collector: To collect the calendar and out-of-office information from Domino mailboxes.

The Avaya Breeze® platform

Avaya Breeze® platform provides a virtualized and secure application platform where workflow developers and Java programmers can develop and dynamically deploy advanced collaboration capabilities. These capabilities extend the power of Avaya Aura®, Avaya Oceana®, and Avaya Professional Services custom development. Customers, Business Partners, and Avaya developers can use Avaya Breeze® platform to deploy snap-ins.

WebLM overview

Avaya provides a Web-based License Manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

WebLM supports two configurations models:

- WebLM standard model. In this model, a single WebLM server supports one or more licensed products. The WebLM standard model supports the Standard License File (SLF) and Enterprise License File (ELF) types.
- WebLM enterprise model. This model includes multiple WebLM servers. One WebLM server acts as a master WebLM server and hosts the license file from PLDS. The remaining WebLM servers act as the local WebLM servers and host the allocation license files from the master WebLM server. You require an ELF to set up the WebLM enterprise model. PLDS generates license files that are SLFs or ELFs.

  Note:

  The master and local WebLM servers must be deployed on the same major release. The master WebLM server must be on same or latest service pack than the local WebLM server resides on.

  For example, if the local WebLM server is on Release 7.1, the master WebLM server must be on Release 7.1, 7.1.1, 7.1.2, or 7.1.3. The master WebLM server cannot be higher than Release 7.1.x.

You can purchase two products and choose the enterprise model of licensing for one product and the standard model of licensing for the other product. PLDS generates a separate license file for each product.

The license file is an SLF or ELF based on how the product is configured in PLDS. Verify the installation options that the product supports before you install the WebLM server. To configure the standard licensing, you can use an ELF or SLF. To configure enterprise licensing, you must have an ELF. After you install the license file on the WebLM server, a product with an ELF can have multiple instances of the WebLM server. However, a product with an SLF can have only one instance of the WebLM server.

The license file of a software product is in an XML format. The license file contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After you purchase a licensed Avaya software product, you must activate the license file for the product in PLDS and install the license file on the WebLM server.

Avaya Aura® applications deployment offers

Avaya Aura® supports the following deployment offers:

- Avaya Aura® Virtualized Environment (VE): Avaya Solutions Platform 130 (Dell PowerEdge R640, ESXi 7.0), Avaya Solutions Platform S8300 (ESXi 7.0), and Customer-provided VMware infrastructure.

  Avaya Solutions Platform 130 R6.0 (Avaya-Supplied KVM on RHEL R8.10) or Avaya Solutions Platform S8300 R6.0 (Avaya-Supplied KVM on RHEL R8.10).

- Software-only and Infrastructure as a Service environment: Deployment on the Red Hat Enterprise Linux operating system.

  Note:

  The deployment of Avaya Aura® applications as software only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as software only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Virtualized Environment overview

You can deploy the Avaya Aura® Release 10.2.x applications in one of the following Virtualized Environment:

- Avaya Solutions Platform 130 Release 5.1 (Dell PowerEdge R640) is a single host server with preinstalled ESXi 7.0 Standard VMware License.
- Avaya Solutions Platform S8300 with a preinstalled ESXi 7.0 Foundation License for Communication Manager and Branch Session Manager.
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660) is a single host server with preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- VMware in customer-provided Virtualized Environment.

Note:

For more information about deploying application, see the product-specific Software-Only and Infrastructure as a Service guide.

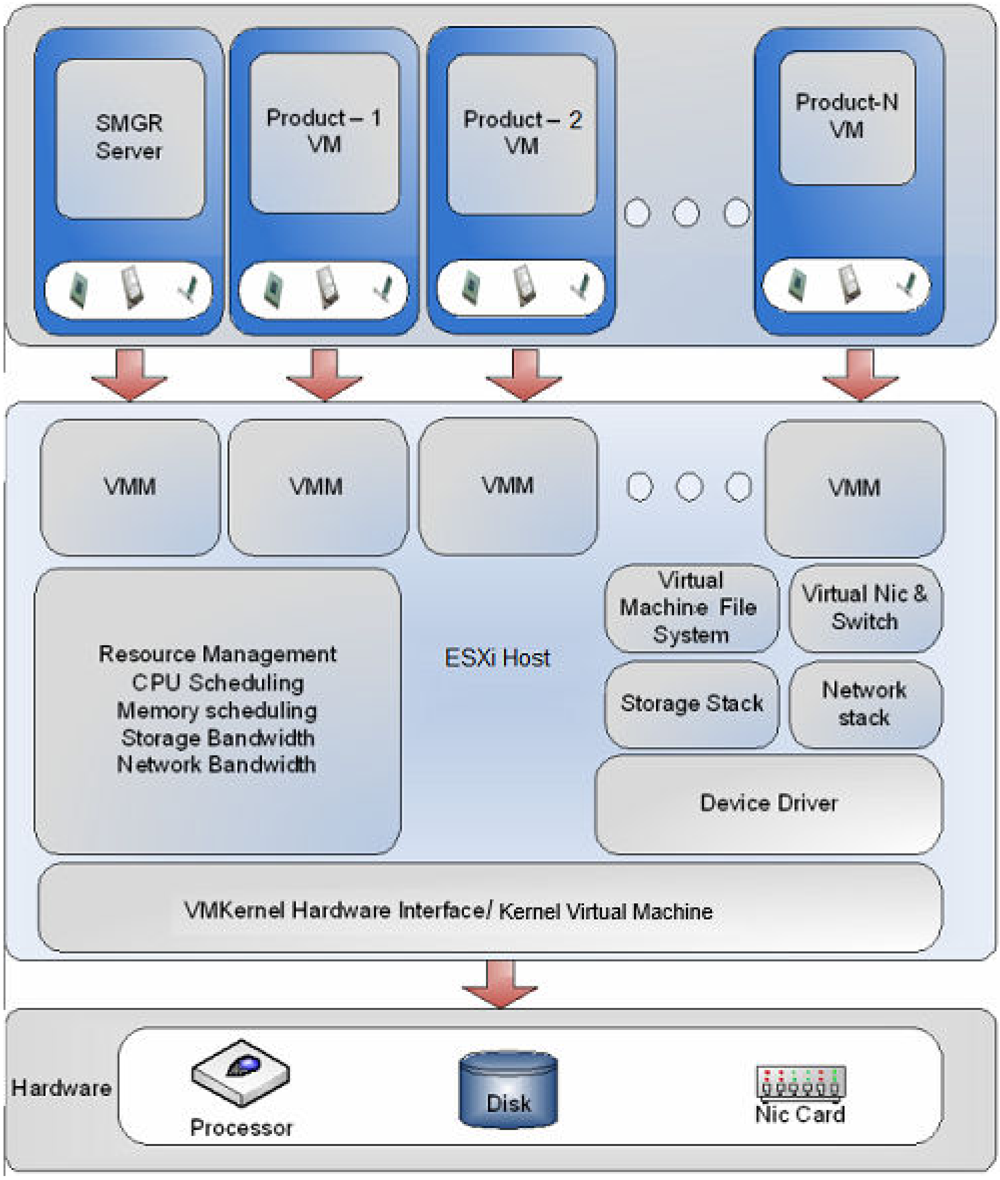
Supported applications in Virtualized Environment

- Avaya Aura® System Manager Release 10.2.x
- Avaya WebLM Release 10.1.3.x
- Avaya Aura® Session Manager Release 10.2.x
- Avaya Aura® Communication Manager Release 10.2.x
- Avaya Aura® Application Enablement Services Release 10.2.x
- Avaya Aura® Media Server Release 10.2.x

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Topology

The following is an example of a deployment infrastructure for System Manager on VMware.



Virtualized Environment components for VMware

Virtualized component	Description
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.
Customer-provided VMware or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) or Avaya Solutions Platform S8300	
ESXi	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.

Table continues…

Virtualized component	Description
ESXi Embedded Host Client	The ESXi Embedded Host Client is a native HTML and JavaScript application and is served directly from the ESXi host.
vSphere Client (HTML5)	Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion. This is not applicable for Avaya Solutions Platform 130 or Avaya Solutions Platform S8300.

Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10)

Virtualized component	Description
Avaya Solutions Platform 130 (Avaya-Supplied KVM on RHEL R8.10) or Avaya Solutions Platform S8300 (Avaya-Supplied KVM on RHEL R8.10)	
KVM Cockpit	Cockpit is a system administration tool that provides a user interface for monitoring and administering servers through a web browser. Cockpit administrators can create and manage KVM-based virtual machines on the host system

Support for VMware components

Avaya Aura® Release 10.2.x supports deployment and upgrades on the following VMware components in Virtualized Environment.

- VMware® vSphere ESXi 7.0
- VMware® vCenter Server 7.0
- VMware® vSphere ESXi 8.0
- VMware® vCenter Server 8.0

Note:

- Avaya Aura® Release 10.2 and later does not support vSphere ESXi 6.7.
- Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.
- Avaya Aura® Release 8.1.x and later supports KVM on RHEL Release 8.10 hypervisor.

  For more information about upgrading from RHEL 8.4 to RHEL 8.10, see:

  - *Upgrading Avaya Aura® Communication Manager*
  - *Upgrading Avaya Aura® Session Manager*
  - *Upgrading Avaya Aura® System Manager*
  - *Upgrading Avaya Aura® Application Enablement Services*

Support for KVM components

Avaya Aura® Release 10.2.x supports deployment and upgrades on the following KVM component in Virtualized Environment.

- KVM on RHEL 8.10

Software-only environment overview

In a software-only installation, the customer owns the operating system and must provide and configure the operating system for use with Avaya Aura® application. With the software-only offer, the customer can install and customize the operating system to meet the requirements to install the Avaya Aura® application.

You must run the software-only offer on the supported environments to enable the use of Avaya approved third-party applications for anti-virus, backup, and monitoring.

Customers and/or Service Providers must procure a server or virtual machine that meets the recommended hardware requirements and the appropriate version of Red Hat Enterprise Linux® Operating System.

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

Avaya Communication Manager Security Service Packs (SSP) can be incompatible or fail to install on a customer controlled operating system.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system. For the list of supported third-party software applications in Release 10.1 and later, see Avaya Product Support Notices.

Avaya Aura® Software-Only environment RPMs

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

For information about RPM updates for the Red Hat Enterprise Linux operating system and required changes to operating system files on Software only installation, see *Avaya Aura® Software Only White paper* on the Avaya Support website.

With Release 10.1 and later, there are no separate Kernel Service Packs (KSP), and Linux Security Update (LSU).

Supported platforms

You can deploy the Avaya Aura® application software-only *ISO image* on the following:

- On-premise platforms:
  - VMware
  - Kernel-based Virtual Machine (KVM)
  - Hyper-V
  - Nutanix 6.5 and later
- Cloud platforms:
  - Amazon Web Services
  - Google Cloud Platform
  - Microsoft Azure
  - IBM Cloud for VMware Solutions

    Specifications for Avaya Aura® applications on IBM Cloud for VMware Solutions is same as that of the Virtualized Environment offer.

    For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Note:

Branch Session Manager is not supported on Amazon Web Services, Google Cloud Platform, and Microsoft Azure.

Supported applications in Software-only Environment

- Avaya Aura® System Manager Release 10.2.x
- Avaya WebLM Release 10.1.3.x
- Avaya Aura® Session Manager Release 10.2.x
- Avaya Aura® Communication Manager Release 10.2.x
- Avaya Aura® Application Enablement Services Release 10.2.x
- Avaya Aura® Media Server Release 10.2.x

Infrastructure as a Service environment overview

Infrastructure as a Service (IaaS) environment enables enterprises to securely run applications on the virtual cloud. The supported Avaya Aura® applications on IaaS can also be deployed on-premises. Avaya Aura® application supports the following platforms within this offer:

- Amazon Web Services

  Note:

  With Release 10.1.x and later, Avaya Aura® will no longer have the Amazon Web Services OVA. Deployment on Amazon Web Services is supported through the software only offer.

- Microsoft Azure
- Google Cloud Platform
- IBM Cloud for VMware Solutions

  For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

The Infrastructure as a Service environment supports the following offers:

Offer	Supported environments
ISO	Simplex • Amazon Web Services • Microsoft Azure • Google Cloud Platform • IBM Cloud for VMware Solutions Duplex • Amazon Web Services • Microsoft Azure • Google Cloud Platform • IBM Cloud for VMware Solutions

Supporting the Avaya Aura® applications on the IaaS platforms provide the following benefits:

- Minimizes the capital expenditure on infrastructure. The customers can move from capital expenditure to operational expense.
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.
- Allows you to pay per-use licensing.
- Allows you to upgrade at a minimal cost.
- Supports mobility to move from one network to another.
- Allows you to stay current with latest security updates provided by the service provider.

You can connect the following applications to the Avaya Aura® IaaS instances from the customer premises:

- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway and G450 Branch Gateway

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

Avaya Communication Manager Security Service Packs (SSP) can be incompatible or fail to install on a customer controlled operating system.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system. For the list of supported third-party software applications in Release 10.1 and later, see Avaya Product Support Notices.

Amazon Web Services overview

Amazon Web Services is an Infrastructure as a Service platform that enables enterprises to securely run applications on the virtual cloud. The key components of Amazon Web Services are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Microsoft Azure overview

Microsoft Azure is an Infrastructure as a Service platform that enables enterprises to securely deploy and manage applications through a global network of Microsoft-managed data centers.

Google Cloud Platform overview

Google Cloud Platform is a suite of public cloud computing services offered by Google.

IBM Cloud for VMware Solutions overview

IBM Cloud for VMware Solutions is a suite of public cloud computing services offered by IBM.

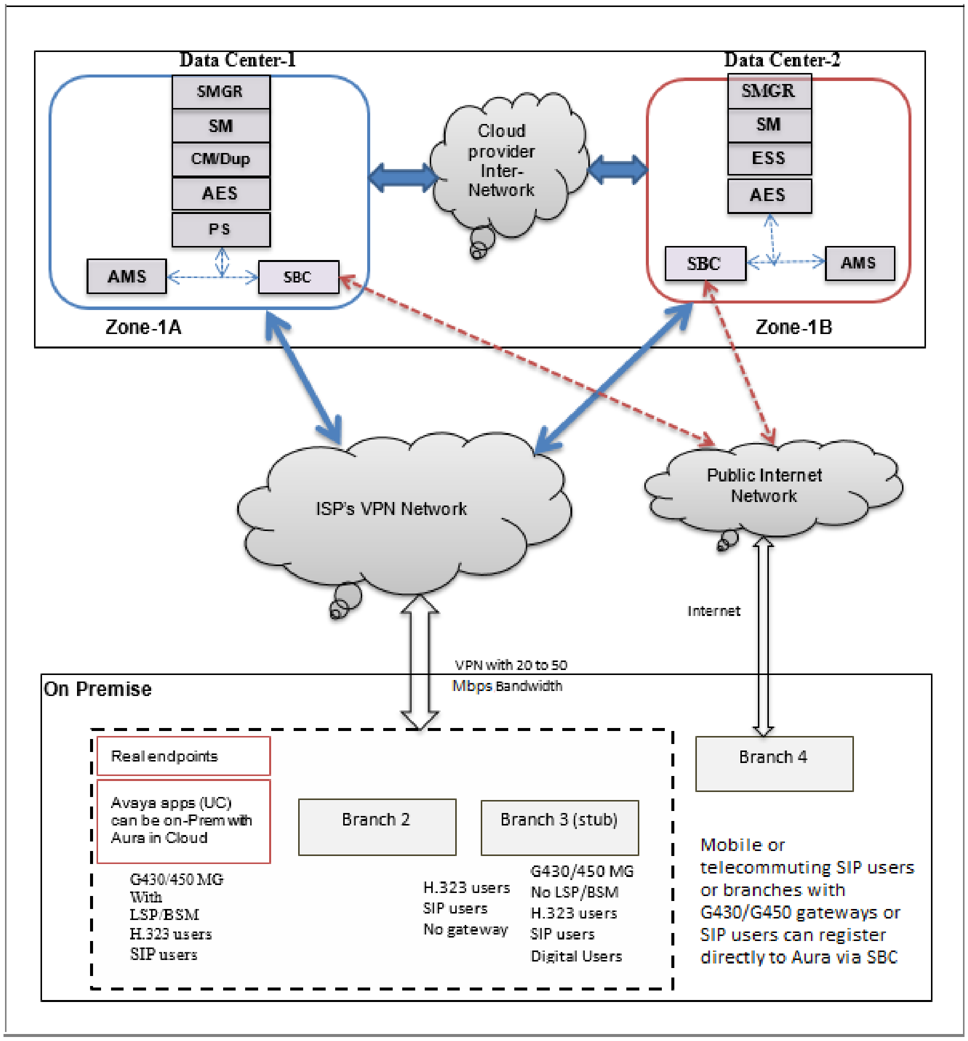
For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Topology

The following diagram depicts the architecture of the Avaya applications on the Infrastructure as a Service platform. This diagram is an example setup of possible configuration offered by Avaya.

Important:

The setup must follow the Infrastructure as a Service deployment guidelines, but does not need to include all the applications.


Data Center-1
SMGR
SM
CM/Dup
AES
PS
AMS
SBC
Zone-1A
Cloud provider Inter-Network
Data Center-2
SMGR
SM
ESS
AES
SBC
AMS
Zone-1B
ISP's VPN Network
Public Internet Network
Internet
VPN with 20 to 50 Mbps Bandwidth
On Premise
Real endpoints
Avaya apps (UC) can be on-Prem with Aura in Cloud
G430/450 MG With LSP/BSM H.323 users SIP users
Branch 2
H.323 users SIP users No gateway
Branch 3 (stub)
G430/450 MG No LSP/BSM H.323 users SIP users Digital Users
Branch 4
Mobile or telecommuting SIP users or branches with G430/G450 gateways or SIP users can register directly to Aura via SBC

Supported applications in Infrastructure as a Service Environment

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Avaya Aura® System Manager	Release 10.2.x	Y	Y	Y
Avaya WebLM	Release 10.1.3.x	Y	Y	Y
Avaya Aura® Session Manager	Release 10.2.x	Y	Y	Y
Avaya Aura® Communication Manager	Release 10.2.x	Y	Y	Y
Avaya Aura® Application Enablement Services (Software only)	Release 10.2.x	Y	Y	Y

Table continues…

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Presence Services using Avaya Breeze® platform	Release 10.1.x	Y	—	—
Avaya Aura® Media Server (Software only)	Release 10.2.x	Y	Y	Y

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Benefits of deploying the Avaya Aura® platform

Improve business agility

SIP architecture with centralized management and control provides businesses the agility to take advantage of new networking capabilities, deploy new applications, and deliver new levels of customer service.

Reduce costs

Avaya Aura® solution helps in effective handling of traffic and PSTN usage with a single enterprise-wide dial plan and intelligent routing policies. Administrative costs are reduced with simpler management and infrastructure.

Increase productivity

The Avaya Aura® platform enables easy deployment of services to users, independent of location or network connection. Employees can use unified communications tools to work effectively.

Improve customer service

With the Avaya Aura® platform, workers can have improved access to services, information, and expertise.

Centralize user administration

System Manager provides a centralized location for adding users in Communication Manager and Session Manager.

Integrate multi-vendor and business application

Customers can easily integrate the Avaya Aura® solution with the third-party applications.

Improve scalability

The Avaya Aura® platform provides support for up to 35,000 IP endpoints for each Communication Manager instance and support for up to 250,000 endpoints on 28 Session Manager instances.

Avaya Aura® Suite Licensing V2

Avaya Aura® provides Avaya Aura® Suite Licensing V2 for Unified Communications (UC) applications. This suite provides:

- Simplified Unified Communications licensing for customers and channels.
- New products and capabilities in an easily scalable structure.

Product	Core Suite	Power Suite
Communication Manager, System Manager, Session Manager, Survivability	Y	Y
Application Enablement Services Unified Desktop	Y	Y
Avaya Breeze® platform	Y Concurrent user Right To Use	Y Concurrent user Right To Use
Avaya Aura® Presence Services (Instant Messaging and Presence)	Y	Y
Avaya Multimedia Messaging	Basic	Enhanced
Voice Messaging • Avaya Aura® Messaging • Avaya Messaging	Basic VM • Avaya Aura® Messaging - Basic license • Avaya Messaging	Enhanced VM • Avaya Aura® Messaging - Mainstream license • Avaya Messaging
Avaya Workplace Client - for Windows	Y	Y
Avaya Workplace Client for Skype for business	Y	Y
Avaya Workplace Client - for Android and iOS	Y	Y
Avaya Session Border Controller Remote Worker and SIP Trunking Sessions	One High Availability Remote Worker license and One High Availability SIP Session for every 7 Core Suite licenses	One High Availability Remote Worker license and One High Availability SIP Session for every 7 Power Suite licenses
AvayaLive Video	Right to purchase one Video Meeting Room at a discount for every 25 Core Suite licenses	Right to purchase one Video Meeting Room at a discount for every 25 Power Suite licenses
Avaya Aura® Conferencing (Audio, Video and Web)	Optional	Y
Multidevice Access (MDA) for SIP Devices/users	10	10
Peer to Peer Video	Y	Y
Extension to Cellular (EC500)	Y	Y

Solution Deployment Manager

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on the customer's Virtualized Environment and the Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager supports migration of Virtualized Environment-based 8.1.x or 10.1.x applications to Release 10.2.x in the customer's Virtualized Environment. For migrating to Release 10.2.x and later, you must use Solution Deployment Manager Release 10.2.x and later.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager with Solution Deployment Manager runs on:

- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.
- Software-Only environment: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.
- Avaya Solutions Platform 130: Avaya Aura® applications are deployed on the Avaya provided hardware.

Note:

- Solution Deployment Manager does not support that application deployment on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 Release 6.0.
- Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

With Solution Deployment Manager, you can do the following in Virtualized Environment, Avaya Solutions Platform 130, and Avaya Aura® Virtualized Appliance Release 8.x or earlier models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.

  Note:

  When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application.

  For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website.
- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, and media modules

  - Session Manager
  - Branch Session Manager
  - AE Services

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 10.2.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Solution Deployment Manager Client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client must be installed 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 Virtualized Environment, or Software-only environment.

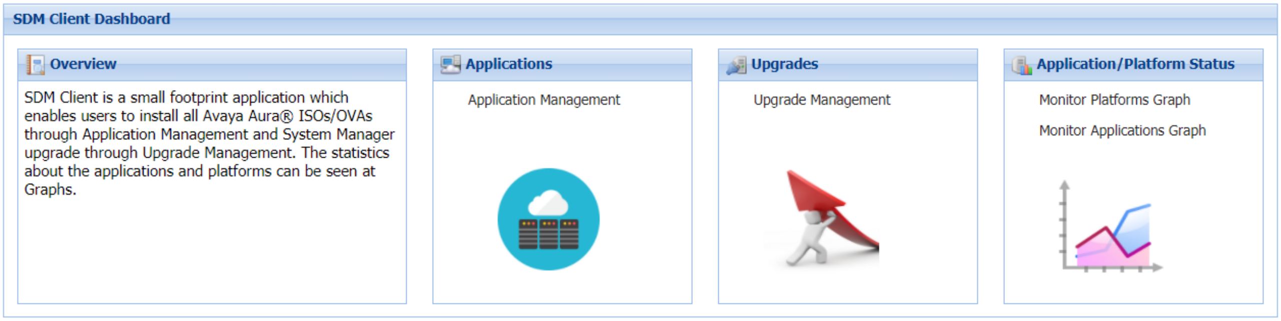
A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances, VMware-based Virtualized Environment, and Software-only environment.
- Upgrade VMware-based System Manager from Release 8.1.x or 10.1.x to Release 10.2 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
- Generate the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze® platform.

Note:

- You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.
- You must always use the latest Solution Deployment Manager client for deployment.
- Solution Deployment Manager does not support that application deployment on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 Release 6.0.
- Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.



SDM Client Dashboard

Overview

SDM Client is a small footprint application which enables users to install all Avaya Aura® ISOs/OVAs through Application Management and System Manager upgrade through Upgrade Management. The statistics about the applications and platforms can be seen at Graphs.

Applications

Application Management

Upgrades

Upgrade Management

Application/Platform Status

Monitor Platforms Graph

Monitor Applications Graph

Figure 2: Solution Deployment Manager Client dashboard

CDR information in Avaya Aura® core solution

The following components support Call Detail Recording (CDR) generation:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® Session Border Controller

Note:

- Branch Gateway can be traditional or Internet-friendly.
- Avaya Aura Communication Manager may not report about the SIP call path before entering one of its endpoints. For example, Communication Manager may not report about the IVR handle times for the SIP calls transferred to agents.
- Session Manager may not have the details of calls that do not involve any SIP endpoints.

The following table summarizes the comparative analysis of different types of calls that are recorded, including the source and termination of calls.

Voice call		Call path visibility		
Initiated	**Disconnected**	**Communication Manager**	**Session Manager**	**Session Border Controller**
ISDN trunk (Using Branch Gateway)	Analog phone	Yes	No	No
	Digital phone	Yes	No	No
	Avaya Aura Experience Portal (AAEP) IVR	Yes	Yes	No
	Voicemail	Yes	Yes	No
	SIP phone	Yes	Yes	Yes
SIP trunk (Using Session Border Controller)	Analog phone	Yes	Yes	Yes
	Digital phone	Yes	Yes	Yes
	Avaya Aura Experience Portal (AAEP) IVR	No	Yes	Yes
	Voicemail	No	Yes	Yes
	SIP phone	Yes	Yes	Yes
Analog phone (on Branch Gateway)	Analog phone	Yes	No	No
	Digital phone	Yes	No	No
	Avaya Aura Experience Portal (AAEP) IVR	Yes	Yes	No
	Voicemail	Yes	Yes	No
	SIP phone	Yes	Yes	Yes
	SIP trunk	Yes	Yes	Yes
	ISDN trunk	Yes	No	No
Digital phone (on Branch Gateway)	Analog phone	Yes	No	No
	Digital phone	Yes	No	No
	Avaya Aura Experience Portal (AAEP) IVR	Yes	Yes	No
	Voicemail	Yes	Yes	No
	SIP phone	Yes	Yes	Yes
	SIP trunk	Yes	Yes	Yes
	ISDN trunk	Yes	No	No
SIP phone (on Session Manager)	Analog phone	Yes	Yes	Yes
	Digital phone	Yes	Yes	Yes

Table continues…

Voice call		Call path visibility		
Initiated	**Disconnected**	**Communication Manager**	**Session Manager**	**Session Border Controller**
	Avaya Aura Experience Portal (AAEP) IVR	Yes	Yes	Yes
	Voicemail	Yes	Yes	Yes
	SIP phone	Yes	Yes	Yes
	SIP trunk	Yes	Yes	Yes
	ISDN trunk	Yes	Yes	Yes

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.

Discontinued support for Avaya Device Adapter Snap-in

From Release 10.2 and later, Avaya Aura® does not support Avaya Device Adapter Snap-in.

Chapter 3: Hardware and software components

Hardware components

The Avaya Aura® solution supports the hardware devices such as servers, gateways, desk telephones, and video devices.

Servers

Avaya software applications are installed on the following supported servers:

- Avaya S8300E Server, embedded servers that reside in G430 and G450 Branch Gateways.

  Note:

  Avaya Aura® Release 10.1 and later support Avaya Solutions Platform S8300 Release 5.1.

  The Avaya Solutions Platform S8300 Release 5.1 is only supported on an S8300E server and not in the earlier versions of the S8300 server such as S8300C and S8300D.

- Standalone servers that come in a 1U configuration:

  Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660

Gateways

The Avaya Aura® solution uses the following supported gateways:

- Branch gateways
  - Avaya G430 Branch Gateway: a gateway that provides H.248 connectivity and houses media modules.
  - Avaya G450 Branch Gateway: a gateway that provides H.248 connectivity and houses media modules.
- AudioCodes M3000 Gateway, a high-density SIP trunk gateway that provides SIP connectivity to Communication Manager and Session Manager.

Media modules

Communication Manager uses branch gateways. The G430 and G450 Branch Gateways house media modules.

For more information on media modules, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

Telephones, endpoints, video devices, and software client

The Avaya Aura® solution supports the following IP telephones, devices, and software client:

- Avaya J129 IP Phone
- Avaya J139 IP Phone
- Avaya J159 IP Phone
- Avaya J179 IP Phone
- Avaya J189 IP Phone
- Avaya 9641GS IP Deskphone
- Avaya B189 IP Conference Phone
- Avaya B199 Conference Phone
- Avaya K155 Vantage Deskphone
- Avaya K175 Vantage Deskphone
- Avaya Wireless Handset 3700 Series
- Avaya Workplace Client for Mac, Android, iOS, and Windows
- Avaya Aura® X for Zoom Workplace
- Avaya Cloud Office Hybrid

For more information on the support of the telephones, endpoints, and video devices, see Product Compatibility Matrix.

Supported servers for Avaya Aura® applications

The following table lists the Avaya sourced supported servers for the Avaya Aura® applications:

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
S8300D	Y	N	N	N	N
S8300E[1]	Y	Y	Y	Y	Y
HP ProLiant DL360 G7 (CSR1)	Y	N	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	N	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	N	N
Dell™ PowerEdge™ R610 (CSR1)	Y	N	N	N	N

Table continues…

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	N	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	N	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	Y	Y	N	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660 [3]	N	Y	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.1/6.x
Avaya Solutions Platform S8300 [4]	N	N	N	Y Release 5.1	Y Release 5.1/6.x

[1] You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 6.x. For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* on the Avaya Support website.

[2] Avaya Solutions Platform 120 Appliance uses Appliance Virtualization Platform to support virtualization.

[3] You can migrate the Avaya Solutions Platform 120 Appliance to Avaya Solutions Platform 130 Appliance Release 6.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

Avaya Solutions Platform 130 Appliance 5.1.x uses VMware vSphere ESXi software to support virtualization. Avaya Solutions Platform 130 Appliance 6.x uses KVM on RHEL software to support virtualization.

[4] Avaya Solutions Platform S8300 5.1.x supports virtualization using VMware vSphere ESXi foundation license for Communication Manager and Branch Session Manager. Avaya Solutions Platform S8300 6.x supports virtualization using KVM on RHEL 8.10 software.

Avaya Solutions Platform 130 Appliance R4/5 uses VMware vSphere ESXi Standard License to support virtualization

Note:

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.

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

  However, in Release 10.2.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 6.0.
- From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

With the introduction of Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), you no longer need a specific license key as was the case with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs

The following table lists the supported embedded Red Hat Enterprise Linux operating system versions of Avaya Aura® application OVAs.

Red Hat Enterprise Linux operating system	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
Linux operating system Release 6.5 with 64-bit					
Linux operating system Release 7.2 with 64-bit	Y **Note:** Utility Services Release 7.1 uses the Red Hat Enterprise Linux operating system Release 7.3 with 64-bit.				

Table continues…

Red Hat Enterprise Linux operating system	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.4 with 64-bit		Y ✱ **Note:** System Manager Release 8.0.x only supports the Red Hat Enterprise Linux operating system Release 7.5 with 64-bit.			
Linux operating system Release 7.6 with 64-bit			Y		
Linux operating system Release 8.4 with 64-bit				Y	Y
Linux operating system Release 8.10 with 64 bit					Y (R10.2.1 onwards)

Supported Red Hat Enterprise Linux operating system versions for Software-only Environment

The following table lists the supported Red Hat Enterprise Linux operating system versions for deploying or upgrading Avaya Aura® applications in Software-only Environment.

Red Hat Enterprise Linux operating system	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.4 with 64-bit			

Table continues…

Red Hat Enterprise Linux operating system	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.6 with 64-bit	Y **Note:** Session Manager Release 8.1.1 and later support the Red Hat Enterprise Linux operating system Release 7.6 through 7.9 with 64-bit.		
Linux operating system Release 8.4 with 64-bit		Y	Y
Linux operating system Release 8.10 with 64 bit			Y

Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications:

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

Note:

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.
- Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2.

Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-801-release-notes/index.html.

- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

  For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.
- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0 and 8.0 Update 2 (U2) deployments.

Supported ASP R6.0.x (KVM on RHEL 8.10) version

The following table lists the supported KVM versions of Avaya Aura® applications:

Avaya Solutions Platform (KVM on RHEL 8.10)	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
KVM Release 8.10	Y	Y Not supported for Session Manager Not supported for System Manager	Y

Note:

- Please check the release notes for the availability of 8.1 and 10.1.
- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x are Avaya-supplied KVM on RHEL 8.10. The Avaya Solutions Platform 130 can be either a Dell R660 or Dell R640. The Dell R660 only ships with and supports KVM on RHEL 8.10. The initial Release of Avaya Solutions Platform 130 Release 4.0 supported Avaya-supplied

ESXi 6.5 and Avaya Solutions Platform 130/S8300 R5.x supported Avaya-supplied ESXi 7.0.

- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x software is KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R660 server only supports KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R640 and the ASP S8300 S8300E support both ESXi 7.0 and KVM on RHEL 8.10. Avaya Solutions Platform 130 Dell R640 Release 4.0 supported ESXi 6.5
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660) is a single host server with preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- Avaya Solutions Platform130 Release 6.0.x (Dell PowerEdge R640, R660, S8300E) is a single host server with preinstalled KVM on RHEL R8.10 software.
- With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific license key needed as was present with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Supported gateways

The following table lists the supported gateways of Avaya Aura® applications.

Supported gateways	**Avaya Aura® Release**				
	7.1.x	**8.0.x**	**8.1.x**	**10.1.x**	**10.2.x**
G430 Branch Gateway	Y	Y	Y	Y	Y
G450 Branch Gateway	Y	Y	Y	Y	Y
G650 Media Gateway	Y	Y	Y		

Note:

From Avaya Aura® Release 10.2 and later, G650 Media Gateway is no longer functional.

Software components

The Avaya Aura® solution consists of several Avaya software applications in addition to the core components. The following products are part of the Avaya Aura® solution:

- Avaya Session Border Controller
- Avaya Workplace Client Conferencing
- Avaya Communication Server 1000

Avaya Aura® supports several software mobility endpoints including:

- Extension to Cellular (EC500)
- Avaya Workplace Client

Avaya Aura® core also supports wide range of third-party elements.

Chapter 4: Solution specification

Reference configurations

This chapter covers the following sample configurations that can be deployed in customer environment. The sample configurations can be integrated with third-party applications for complete network interconnections.

- Messaging
- Avaya Workplace Client Solution: Equinox Conferencing
- Survivability
- Avaya Aura® in a virtualized environment
- Avaya Breeze® platform

Avaya Messaging

For information about Avaya Messaging, see Avaya Messaging documentation on the Avaya Support website.

Avaya Meetings Server overview

Avaya Meetings Server is an audio, video and web conferencing offer converging on a single platform the best of Avaya capabilities for scalable audio conferencing and rich web collaboration with the best of Avaya capabilities for video processing and transcoding, standards-based video room system integration, and the broad range of remote access capabilities for desktop and mobile devices.

Capabilities of the Avaya Meetings Server offer include:

- WebRTC for easy conference participation by guests on web browser with zero download
- Avaya Workplace Client for Android, iOS, Mac, and Windows with its rich user capabilities for deployment of Unified Communications
- Avaya Breeze® platform with its Software Development Kit that allows to embed conferencing and collaboration features in business processes and applications.

The result is the software-based Avaya Meetings Server deployable in a virtualized environment:

- You do not need a dedicated appliance taking up rack space for each function. Less boxes or appliances mean it is considerably more efficient.
- End users have a single conferencing system to learn.
- IT managers have one system to support and one vendor to call for assistance.
- Avaya sales and partners have a single conferencing solution to sell.

Avaya Meetings Server is a single platform for:

- Avaya Meetings Server for Team Engagement with Avaya Aura® components
- Avaya Meetings Server for Over The Top for customers who want their conferencing solution to be a standalone entity and not integrated with Avaya Unified Communications
- Service Provider offerings

  Avaya has enhanced the room system product line for much easier deployment in enterprise applications. For service providers, this means easy bundling of our endpoints with services, while enterprise customers can enjoy much simpler installation and administration. You do not need an expert or technical resource to install or provision a room system. Anyone who can hook up the cables, connect the components together, and turn on the power can get a room system operational without an onsite technical resource. For example, the general facilities personnel.

As an open mobile enterprise engagement company, Avaya continues to extend its solutions portfolio to address a wider set of customer challenges and areas of higher value. Avaya solutions, innovation roadmap, and channel development plans position the company to address trends over the coming years, including:

- Video becoming mainstream
- Increasing mobility demands driven by smartphones and tablets
- IT consumerization
- Demand for open, flexible platforms
- Common place adoption of communication-enabled business processes
- Context-driven communications
- Federation of communications across enterprise boundaries.

Related links

Solution specifications for large enterprises on page 43
Solution specifications for medium to large enterprises on page 47
Solution specifications for small to medium enterprises on page 50

Solution specifications for large enterprises

Avaya has created this conferencing solution for large enterprises and Service Providers. The solution offers the full range of Avaya Meetings Server features, particularly multiple simultaneous conferences. The solution is called Avaya Meetings Server for Over The Top when it functions as a standalone infrastructure without Avaya Aura® components. A solution that integrates with Avaya Aura® is called Avaya Meetings Server for Team Engagement .

The following figures illustrate examples of distributed deployments:

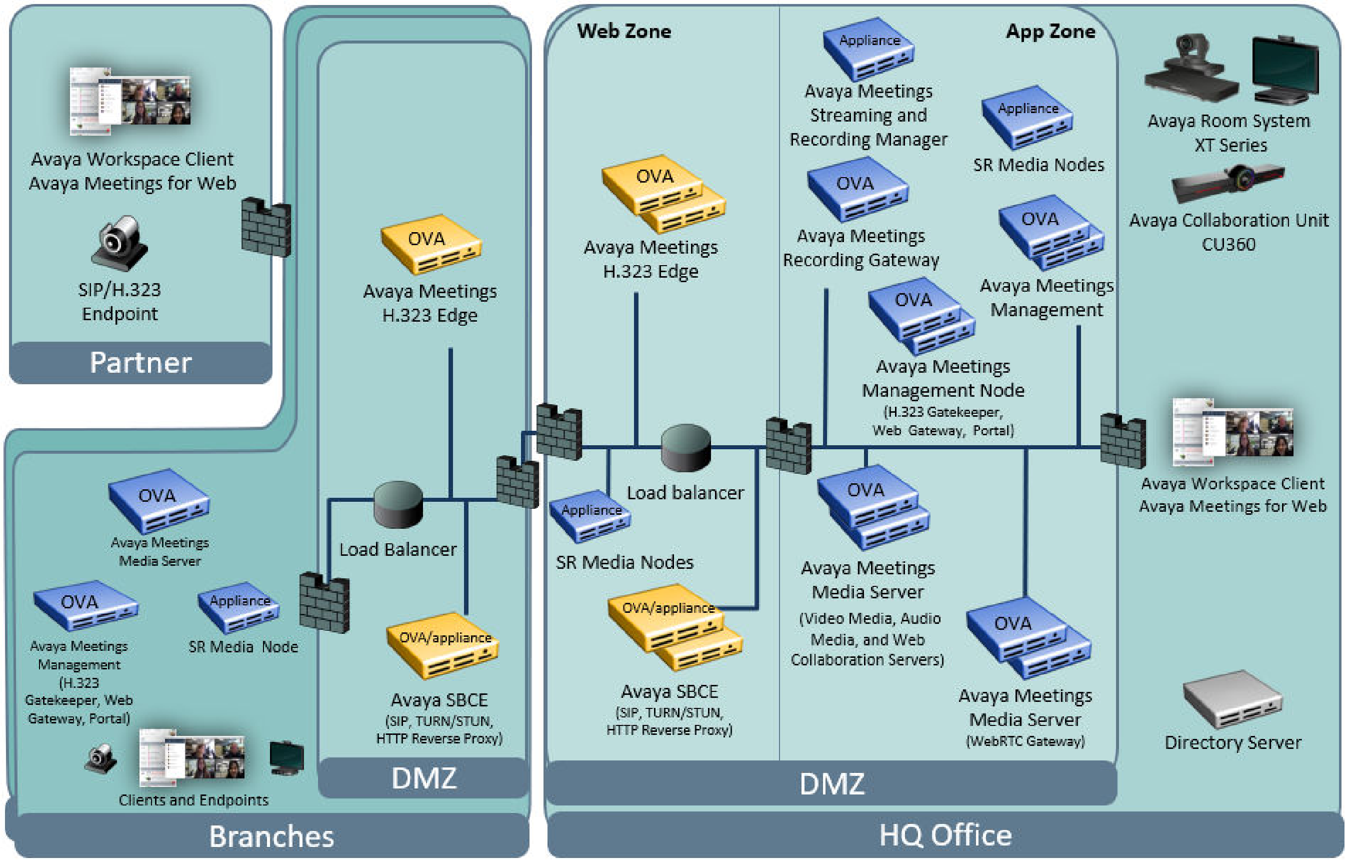


Figure 3: Large distributed configuration for Over The Top

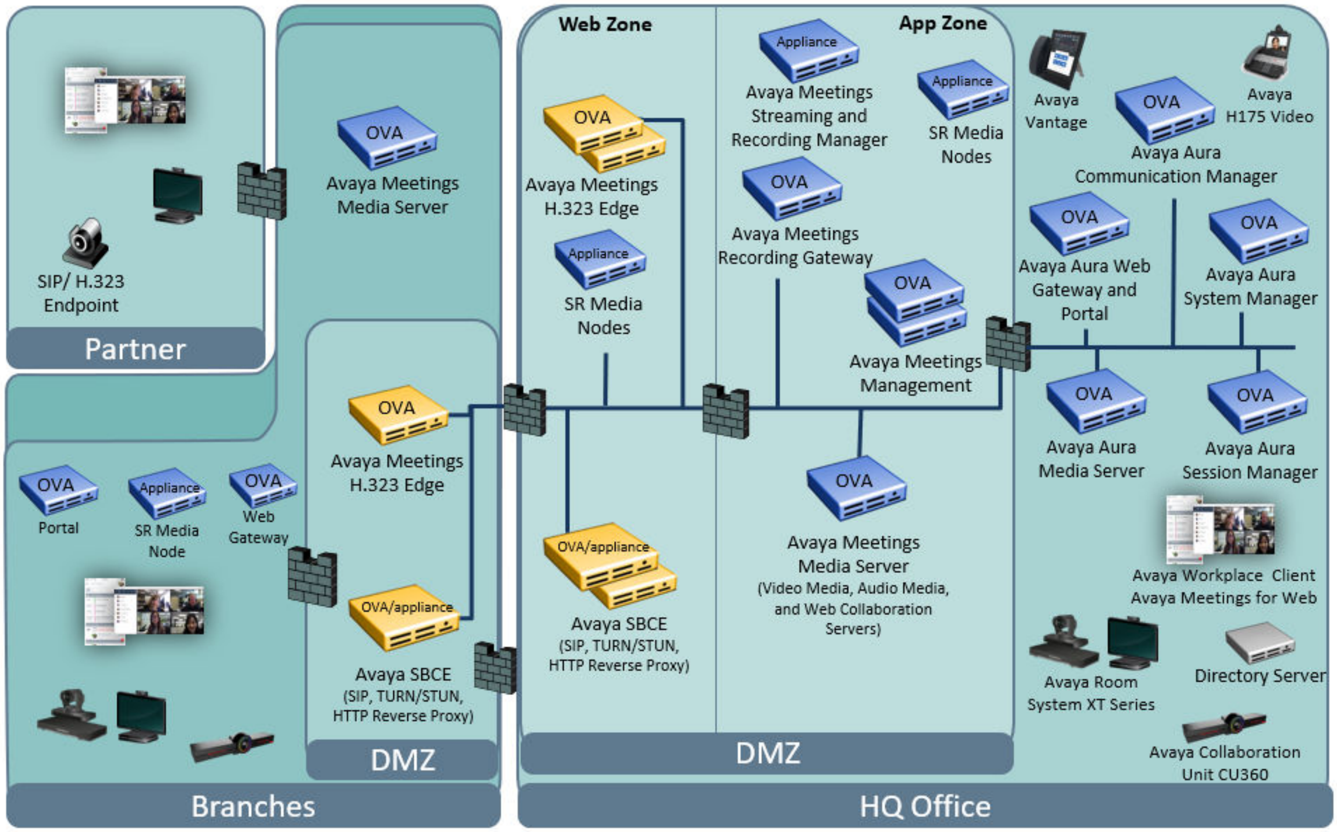

Partner
SIP/ H.323 Endpoint
OVA
Avaya Meetings Media Server
Branches
OVA
Portal
Appliance
SR Media Node
OVA
Web Gateway
DMZ
OVA
Avaya Meetings H.323 Edge
OVA/appliance
Avaya SBCE
(SIP, TURN/STUN, HTTP Reverse Proxy)
Web Zone
OVA
Avaya Meetings H.323 Edge
Appliance
SR Media Nodes
OVA/appliance
Avaya SBCE
(SIP, TURN/STUN, HTTP Reverse Proxy)
App Zone
Appliance
Avaya Meetings Streaming and Recording Manager
Appliance
SR Media Nodes
OVA
Avaya Meetings Recording Gateway
OVA
Avaya Meetings Management
OVA
Avaya Meetings Media Server
(Video Media, Audio Media, and Web Collaboration Servers)
DMZ
Avaya Vantage
Avaya H175 Video
OVA
Avaya Aura Communication Manager
OVA
Avaya Aura Web Gateway and Portal
OVA
Avaya Aura System Manager
OVA
Avaya Aura Media Server
OVA
Avaya Aura Session Manager
Avaya Workplace Client
Avaya Meetings for Web
Avaya Room System XT Series
Directory Server
Avaya Collaboration Unit CU360
HQ Office

Figure 4: Large distributed configuration for Team Engagement in Unified Communications

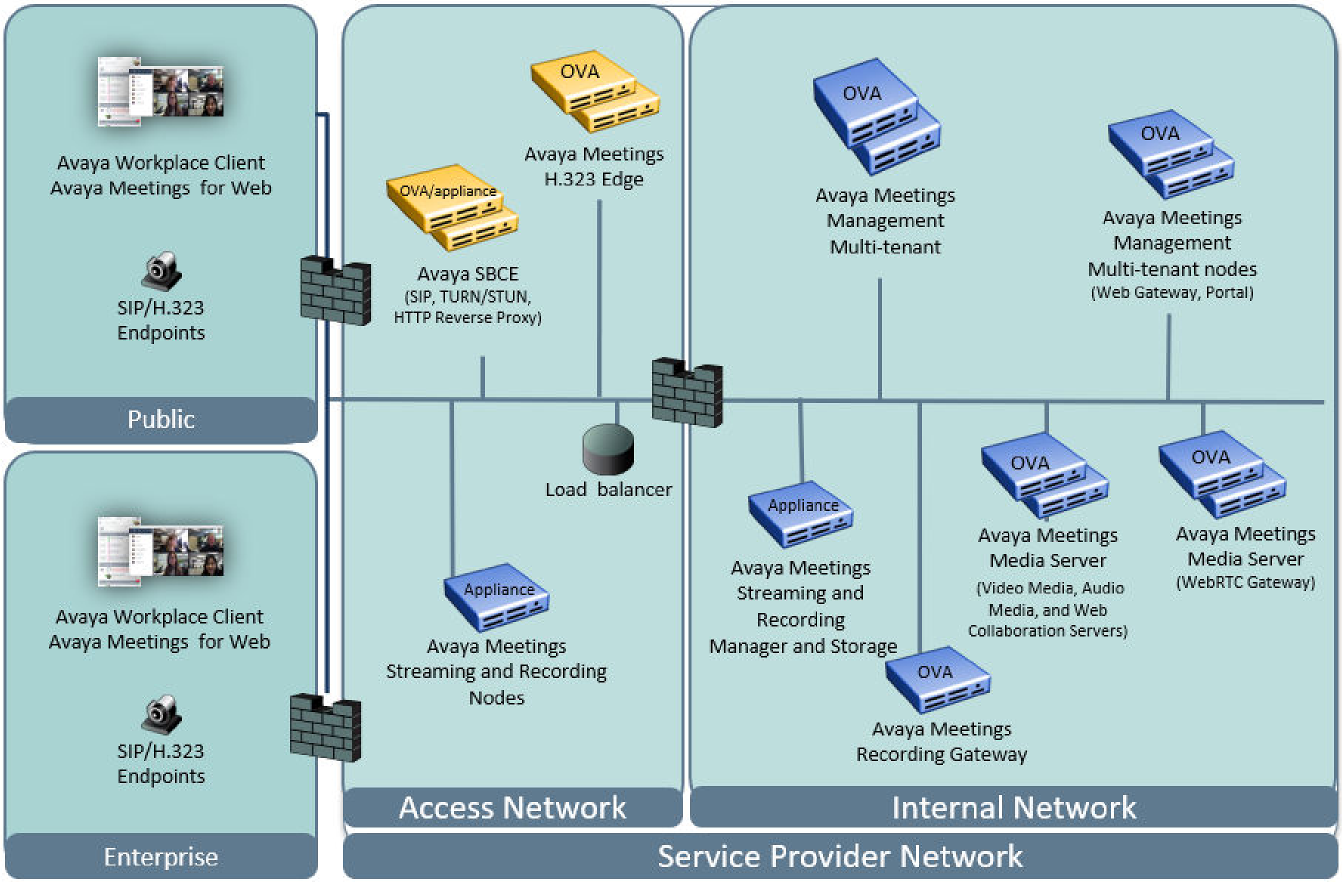

Avaya Workplace Client
Avaya Meetings for Web
SIP/H.323 Endpoints
Public
Avaya Workplace Client
Avaya Meetings for Web
SIP/H.323 Endpoints
Enterprise
OVA
Avaya Meetings H.323 Edge
OVA/appliance
Avaya SBCE (SIP, TURN/STUN, HTTP Reverse Proxy)
Load balancer
Appliance
Avaya Meetings Streaming and Recording Nodes
Access Network
OVA
Avaya Meetings Management Multi-tenant
OVA
Avaya Meetings Management Multi-tenant nodes (Web Gateway, Portal)
Appliance
Avaya Meetings Streaming and Recording Manager and Storage
OVA
Avaya Meetings Media Server (Video Media, Audio Media, and Web Collaboration Servers)
OVA
Avaya Meetings Media Server (WebRTC Gateway)
OVA
Avaya Meetings Recording Gateway
Internal Network
Service Provider Network

Figure 5: Configuration for Service Providers in Over The Top

This conferencing solution:

- Targets up to 150,000 registered users.
- Supports up to 7,500 concurrent sessions.
- Requires port-based licenses when deployed as Avaya Meetings Server for Over The Top , and Avaya Aura® Power Suite user licenses when set up for Avaya Meetings Server for Team Engagement.
- Requires a virtual room based license when Avaya delivers conferencing services.
- Recommends the use of two DMZ zones with three firewalls: the web zone for publicly accessed servers; the application zone for application servers.
- Includes Avaya Meetings Management for managing the organization's network, web services, and signaling/control components. This virtual application, which is delivered as an OVA, fully integrates with the enterprise active directory and provides intelligent cross-zone bandwidth management regardless of protocols being used for calls.

  Avaya Meetings Management includes these modules: Management, User Portal + Web Gateway for web services, SIP B2BUA for signaling and control, Avaya Meetings Control, and H.323 Gatekeeper.

- Adds the Avaya Meetings Management node for specific loads and geographic distribution requirements. Usually, the customer must distribute User Portal + Web Gateway in large deployments when numerous users access the portal to join conferences, download client plugin, and schedule meetings. Likewise, a large deployment with numerous H.323 calls requires a distributed H.323 Gatekeeper. The node includes these modules that can be installed in one of the following ways:
    - H.323 Gatekeeper
    - User Portal + Web Gateway
    - User Portal, when Web Gateway is disabled. This occurs in base upgrades or migrations, or in non-encrypted versions of the core Avaya Meetings Management.
- Deploys Avaya Meetings Media Server that provides rich audio, video, and data conferencing functionalities to the solution. The server includes: HD video transcoding Media Server for processed video, High Scale Audio engine, and Web Collaboration engine. The server supports two working modes per single OVA: video, audio, and web collaboration; high capacity audio and web collaboration. The administrator can switch the working mode from the Avaya Meetings Management interface. Avaya Meetings Media Server cannot work in a mixed mode. For a solution with both working modes, the deployment must include two Avaya Meetings Media Server: one for Full Audio, Video, Web Collaboration, and one for High Capacity Audio and Web Collaboration. For WebRTC, the Avaya Meetings Media Server uses Avaya Aura® Media Server as a WebRTC Gateway.

  To handle WebRTC calls in Over The Top from release 9.1 SP3, Avaya Meetings Media Server instances are configured to run as a WebRTC Gateway and front other Avaya Meetings Media Servers.
- Deploys Avaya Meetings H.323 Edge. The server provides firewall and NAT traversal for Avaya remote H.323 video HD room systems and standard third-party rooms. The server is installed as an OVA.
- Supports Avaya Session Border Controller or an Avaya-approved edge device, as an option. Avaya SBC provides SIP firewall traversal, HTTP Reverse proxy, and STUN/TURN firewall traversal. Avaya SBC is deployed as an OVA, or as an appliance with pre-installed software.
- Adds the Avaya Meetings Streaming and Recording facility as an option. It is deployed as a pre-installed appliance on Avaya Solutions Platform server.

Related links

Avaya Meetings Server overview on page 42

Solution specifications for medium to large enterprises

Avaya has created this conferencing solution for medium-size enterprises. The solution offers the full range of Avaya Meetings Server features, particularly multiple simultaneous conferences. The solution is suited for enterprises with a single main branch containing several meeting rooms, or for enterprises structured as a headquarter and several branches.

The solution is called Avaya Meetings Server for Over The Top when it ties to the customer existing infrastructure and provides services over the top of this infrastructure without requiring it to be upgraded or replaced.

The solution that tightly integrates with Avaya Aura® components is called Avaya Meetings Server for Team Engagement and is deployed in medium and large enterprises.

The following figures illustrate distributed deployments:

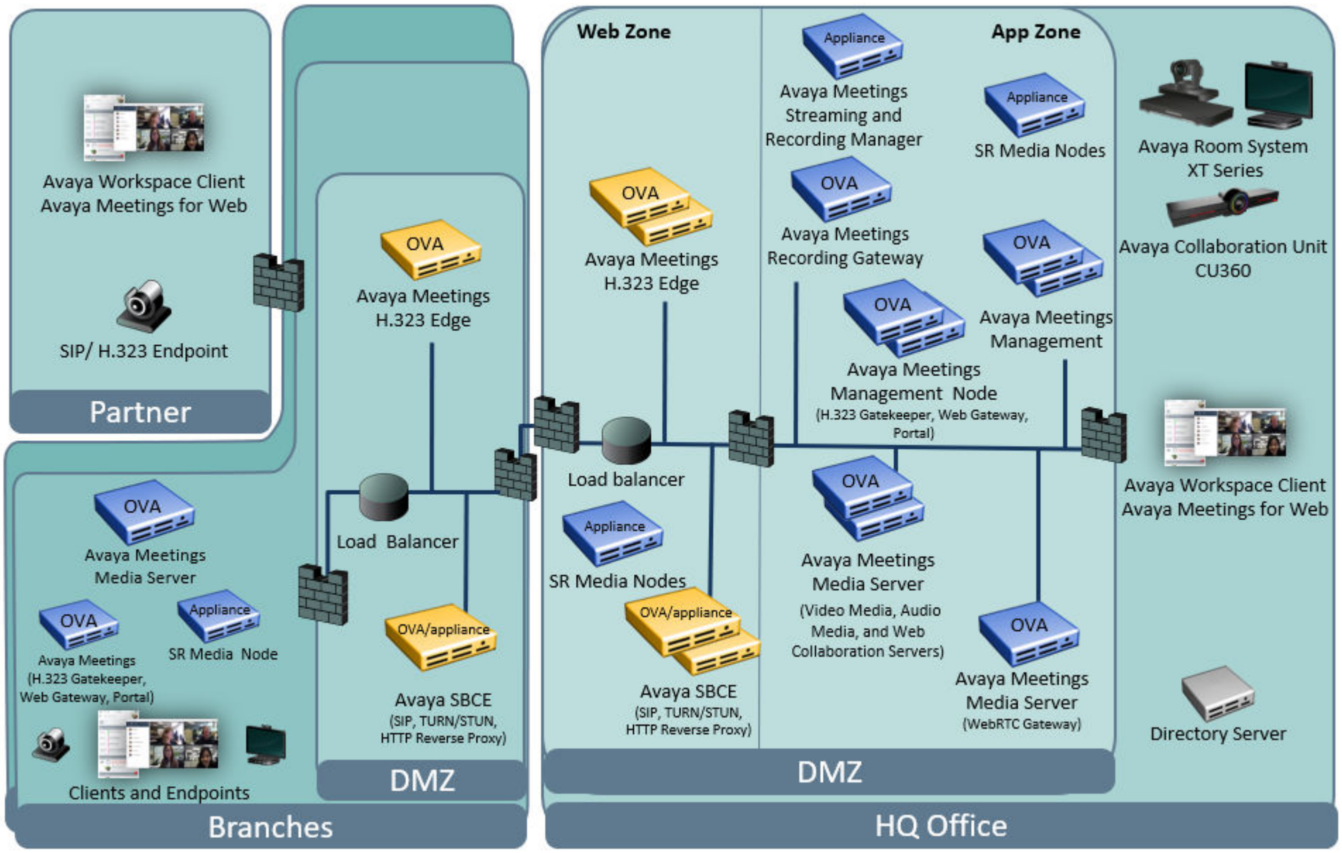


Figure 6: Over The Top deployment for medium to large enterprises

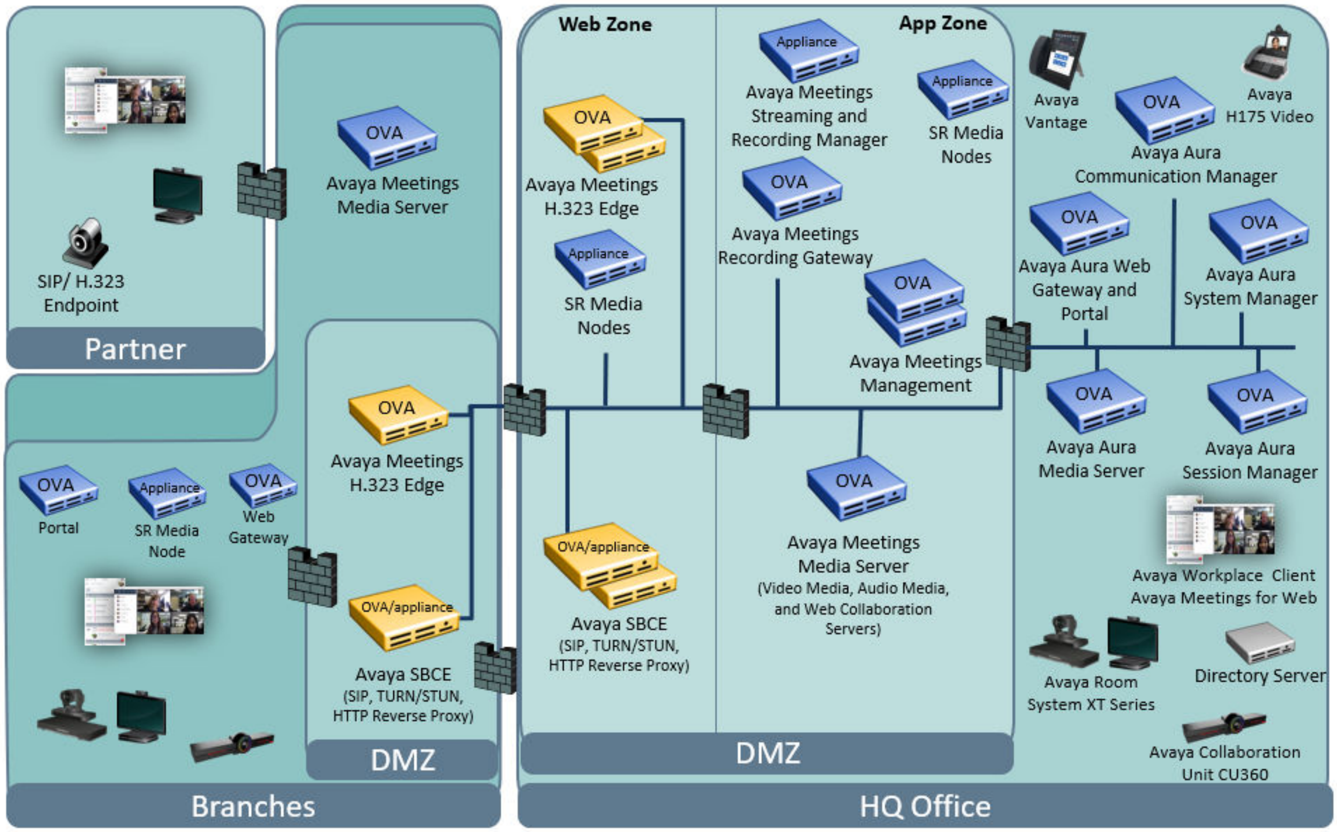

Partner
SIP/ H.323 Endpoint
OVA
Avaya Meetings Media Server
Branches
OVA
Portal
Appliance
SR Media Node
OVA
Web Gateway
DMZ
OVA
Avaya Meetings H.323 Edge
OVA/appliance
Avaya SBCE (SIP, TURN/STUN, HTTP Reverse Proxy)
Web Zone
OVA
Avaya Meetings H.323 Edge
Appliance
SR Media Nodes
OVA/appliance
Avaya SBCE (SIP, TURN/STUN, HTTP Reverse Proxy)
App Zone
Appliance
Avaya Meetings Streaming and Recording Manager
Appliance
SR Media Nodes
OVA
Avaya Meetings Recording Gateway
OVA
Avaya Meetings Management
OVA
Avaya Meetings Media Server (Video Media, Audio Media, and Web Collaboration Servers)
DMZ
HQ Office
Avaya Vantage
OVA
Avaya Aura Communication Manager
Avaya H175 Video
OVA
Avaya Aura Web Gateway and Portal
OVA
Avaya Aura System Manager
OVA
Avaya Aura Media Server
OVA
Avaya Aura Session Manager
Avaya Workplace Client
Avaya Meetings for Web
Avaya Room System XT Series
Directory Server
Avaya Collaboration Unit CU360

Figure 7: Team Engagement deployment for medium to large enterprises

This solution:

- Targets up to 30,000 registered users.
- Supports up to 2,000 concurrent sessions.
- Requires port-based licenses when deployed as Avaya Meetings Server for Over The Top , and Avaya Aura® Power Suite user licenses when set up for Avaya Meetings Server for Team Engagement.
- Recommends the use of two DMZ zones with three firewalls: the web zone for publicly accessed servers; the application zone for application servers.
- Includes Avaya Meetings Management for managing the organization’s network, web services, and signaling/control components. This virtual application, which is delivered as an OVA, fully integrates with the enterprise active directory and provides intelligent cross-zone bandwidth management regardless of protocols being used for calls.

  Avaya Meetings Management includes these modules: Management, User Portal + Web Gateway for web services, SIP B2BUA for signaling and control, Avaya Meetings Control, and H.323 Gatekeeper.
- Adds the Avaya Meetings Management node for specific loads and geographic distribution requirements. Usually, the customer must distribute User Portal + Web Gateway in large deployments when numerous users access the portal to join conferences, download client

plugin, and schedule meetings. Likewise, a large deployment with numerous H.323 calls requires a distributed H.323 Gatekeeper. The node includes these modules that can be installed in one of the following ways:

  - H.323 Gatekeeper
  - User Portal + Web Gateway
  - User Portal, when Web Gateway is disabled. This occurs in base upgrades or migrations, or in non-encrypted versions of the core Avaya Meetings Management.

- Deploys Avaya Meetings Media Server that provides rich audio, video, and data conferencing functionalities to the solution. The server includes: HD video transcoding Media Server for processed video, High Scale Audio engine, and Web Collaboration engine. The server supports two working modes per single OVA: video, audio, and web collaboration; high capacity audio and web collaboration. The administrator can switch the working mode from the Avaya Meetings Management interface. Avaya Meetings Media Server cannot work in a mixed mode. For a solution with both working modes, the deployment must include two Avaya Meetings Media Server: one for Full Audio, Video, Web Collaboration, and one for High Capacity Audio and Web Collaboration. For WebRTC, the Avaya Meetings Media Server uses Avaya Aura® Media Server as a WebRTC Gateway.

  To handle WebRTC calls in Over The Top from release 9.1 SP3, Avaya Meetings Media Server instances are configured to run as a WebRTC Gateway and front other Avaya Meetings Media Servers.

- Deploys Avaya Meetings H.323 Edge. The server provides firewall and NAT traversal for Avaya remote H.323 video HD room systems and standard third-party rooms. The server is installed as an OVA.
- Supports Avaya Session Border Controller or an Avaya-approved edge device, as an option. Avaya SBC provides SIP firewall traversal, HTTP Reverse proxy, and STUN/TURN firewall traversal. Avaya SBC is deployed as an OVA, or as an appliance with pre-installed software.
- Adds the Avaya Meetings Streaming and Recording facility as an option. It is deployed as a pre-installed appliance on Avaya Solutions Platform server.

Related links

Avaya Meetings Server overview on page 42

Solution specifications for small to medium enterprises

Avaya has created this centralized conferencing solution for small enterprises. The solution offers the full range of Avaya Meetings Server features, particularly multiple simultaneous conferences. The solution is suited for enterprises with a single main branch containing several meeting rooms.

The solution is called Avaya Meetings Server for Over The Top when it ties to the customer existing infrastructure and provides services over the top of this infrastructure without requiring it to be upgraded or replaced.

The following figure illustrates a basic Over The Top deployment.

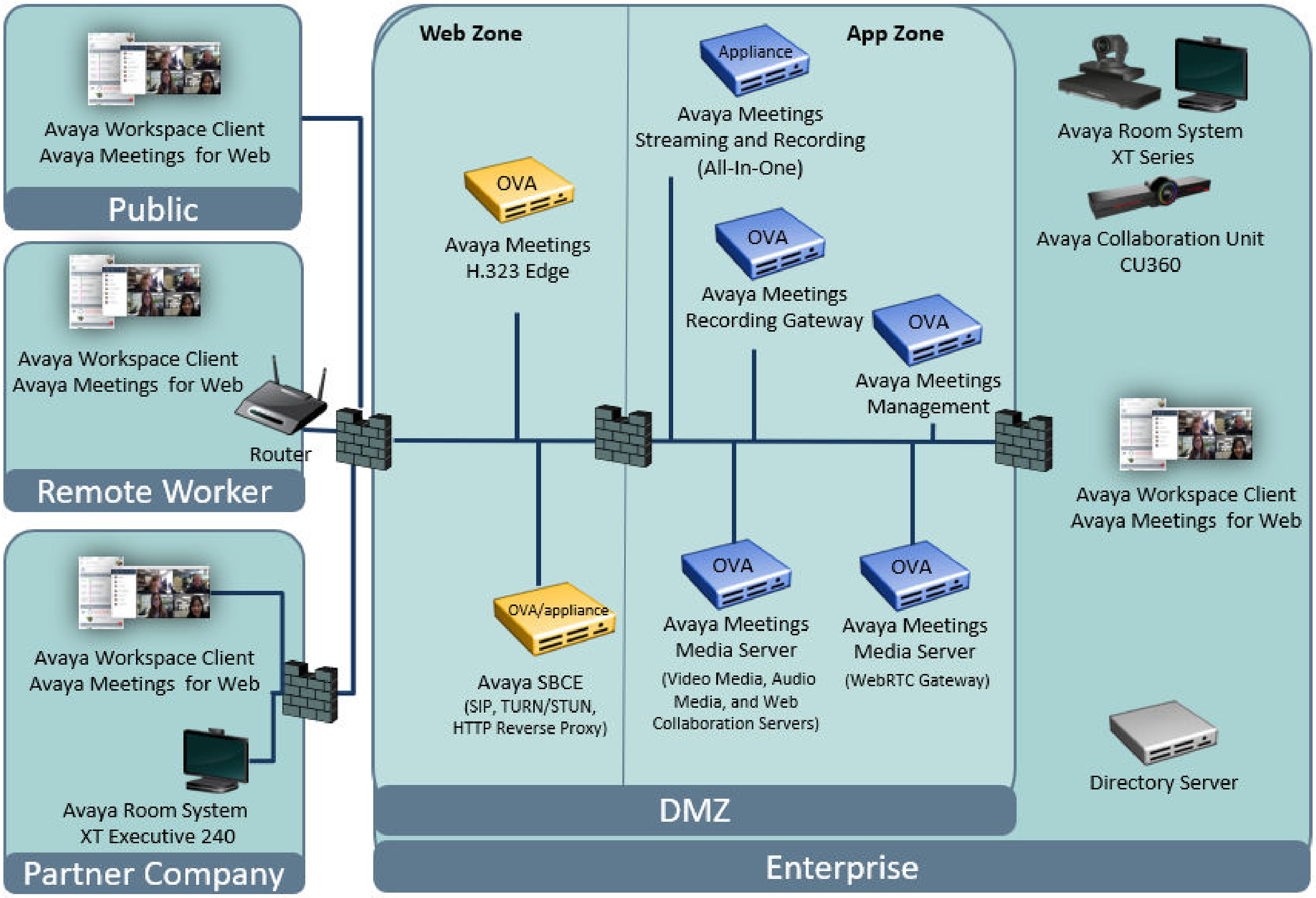


Figure 8: Example of a complete centralized solution

This complete centralized conferencing solution:

- Targets up to 5,000 registered users.
- Supports up to 500 concurrent sessions.
- Requires port-based licenses
- Recommends the use of two DMZ zones with three firewalls: the web zone for publicly accessed servers; the application zone for application servers.
- Includes Avaya Meetings Management for managing the organization's network, web-services, and signaling/control components. The virtual application fully integrates with the enterprise active directory and provides intelligent cross-zone bandwidth management regardless of protocols being used for calls. The application deploys as an All-In-One Open Virtualized Appliance (OVA). All its modules (Management, SIP B2BUA, H.323 Gatekeeper, Avaya Meetings Control, Web Gateway, User Portal) are installed on the same virtual machine.
- Deploys Avaya Meetings Media Server that provides rich audio, video, and data conferencing functionalities to the solution. The server includes: HD video transcoding Media Server for processed video, High Scale Audio engine, and Web Collaboration engine. The server

supports two working modes per single OVA: video, audio, and web collaboration; high capacity audio and web collaboration. The administrator can switch the working mode from the Avaya Meetings Management interface. Avaya Meetings Media Server cannot work in a mixed mode. For a solution with both working modes, the deployment must include two Avaya Meetings Media Server: one for Full Audio, Video, Web Collaboration, and one for High Capacity Audio and Web Collaboration. For WebRTC, the Avaya Meetings Media Server uses Avaya Aura® Media Server as a WebRTC Gateway.

To handle WebRTC calls in Over The Top from release 9.1 SP3, Avaya Meetings Media Server instances are configured to run as a WebRTC Gateway and front other Avaya Meetings Media Servers.

- Deploys Avaya Meetings H.323 Edge. The server provides firewall and NAT traversal for Avaya remote H.323 video HD room systems and standard third-party rooms. The server is installed as an OVA.
- Supports Avaya Session Border Controller or an Avaya-approved edge device, as an option. Avaya SBC provides SIP firewall traversal, HTTP Reverse proxy, and STUN/TURN firewall traversal. Avaya SBC is deployed as an OVA, or as an appliance with pre-installed software.
- Adds the Avaya Meetings Streaming and Recording facility as an option. It is deployed as a pre-installed appliance on Avaya Solutions Platform server.

Related links

Avaya Meetings Server overview on page 42

Survivability

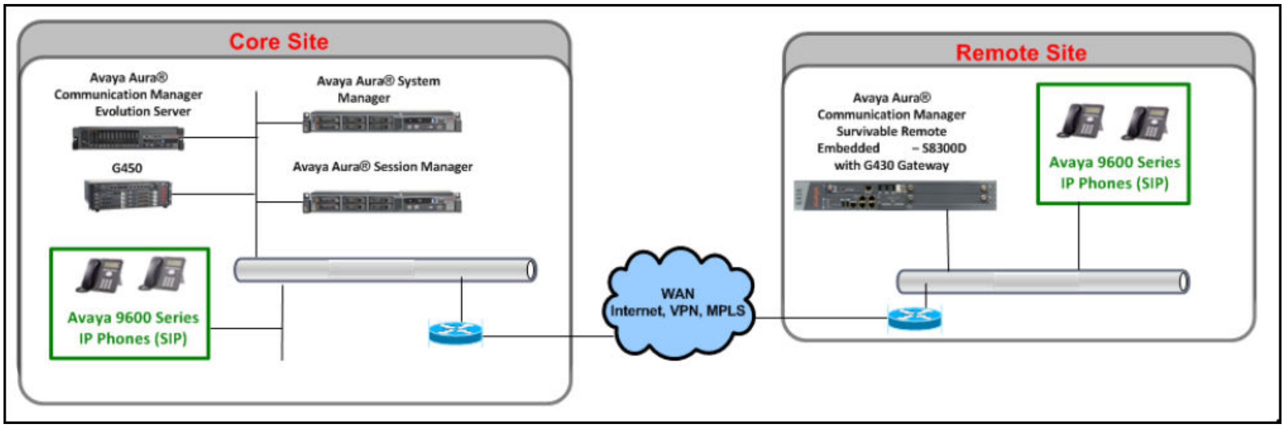

Core Site
Avaya Aura® Communication Manager Evolution Server
G450
Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya 9600 Series IP Phones (SIP)
WAN Internet, VPN, MPLS
Remote Site
Avaya Aura® Communication Manager Survivable Remote Embedded – S8300D with G430 Gateway
Avaya 9600 Series IP Phones (SIP)

Figure 9: Avaya Aura® with Embedded Survivable Remote

The Embedded Survivable Remote solution supports survivable local call processing and SIP routing for a branch when the connection with the core site fails. Branch Session Manager provides a SIP-enabled branch survivability solution. When the core Session Manager is unreachable, SIP phones receive Communication Manager features from Avaya Aura® that is installed on the Embedded Survivable Remote server. Branch Session Manager provides services to the SIP endpoints when the connection with the core site is fails.

The sample configuration consists of the Embedded Survivable Remote server, Branch Session Manager, and an Avaya Aura® 8.x infrastructure.

The embedded survivable remote template is installed on an Avaya S8300E server with G430 Branch Gateway and G450 Branch Gateway.

The site where the embedded survivable remote server is installed includes:

- Session Manager
- Branch Session Manager
- Communication Manager
- AVP Utilities (Formerly known as Utility Services)

Component	Software version
• Communication Manager • G450 Branch Gateway	• Communication Manager Release 8.0 • G450 Branch Gateway Firmware 40.x.x
• Communication Manager • Survivable Remote embedded with Session Manager • G430 Branch Gateway	• Communication Manager Release 8.0 • Branch Session Manager Release 8.0 • G430 Branch Gateway Firmware 40.x.x
System Manager on Appliance Virtualization Platform	• System Manager Release 8.0 • Appliance Virtualization Platform 8.0
Session Manager	Session Manager Release 8.0
Avaya 96x1 Series IP telephone — SIP	Release 7.0.1

Avaya Aura® in a virtualized environment

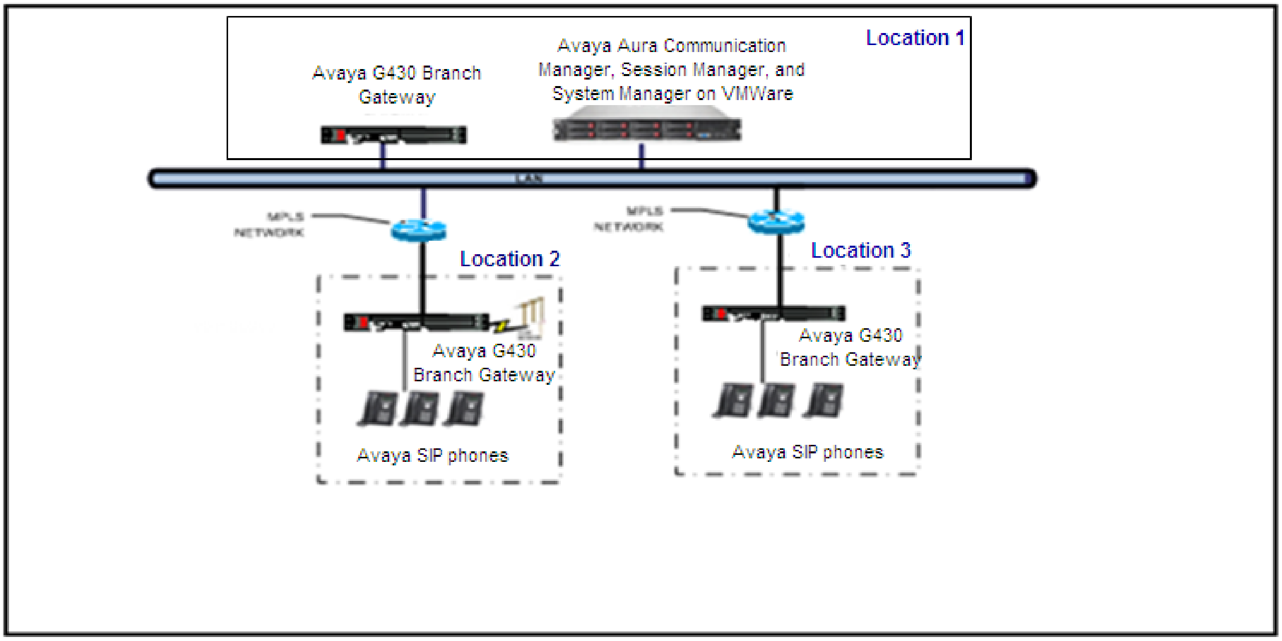

Location 1
Avaya G430 Branch Gateway
Avaya Aura Communication Manager, Session Manager, and System Manager on VMWare
LAN
MPLS NETWORK
Location 2
Avaya G430 Branch Gateway
Avaya SIP phones
MPLS NETWORK
Location 3
Avaya G430 Branch Gateway
Avaya SIP phones

Figure 10: Avaya Aura® on VMware

The Avaya Aura® core setup is in the head office, Location 1. The head office connects to Location 2, a branch office, which is the parts warehouse. Location 2 requires a new setup for 150 users. Location 2 uses SIP endpoints. The network environment uses POE. The communication system requires a 30–channel ISDN PRI trunk for inbound and outbound calling. The branch office connects over WAN to the head office.

The second branch office, Location 3, requires a setup to support up to 40 users. The branch office uses SIP endpoints and a 30–channel ISDN PRI trunk for inbound and outbound calls. The branch office connects over WAN to the head office.

Proposed solution

Location 1

The Location 1 datacenter consists of Communication Manager, Session Manager, and System Manager. Virtualized Environment is on customer-provided hardware and VMware. The servers are installed on VMware. Location 1 uses one G430 Branch Gateway for media resources. The Location 1 system hosts all the licenses and provides services and control over WAN to Location 2 and Location 3. The Location 1 system has licenses for 190 users, 150 for Location 2 and 40 for Location 3. Number of EC-500 licenses are available as a startup are 20.

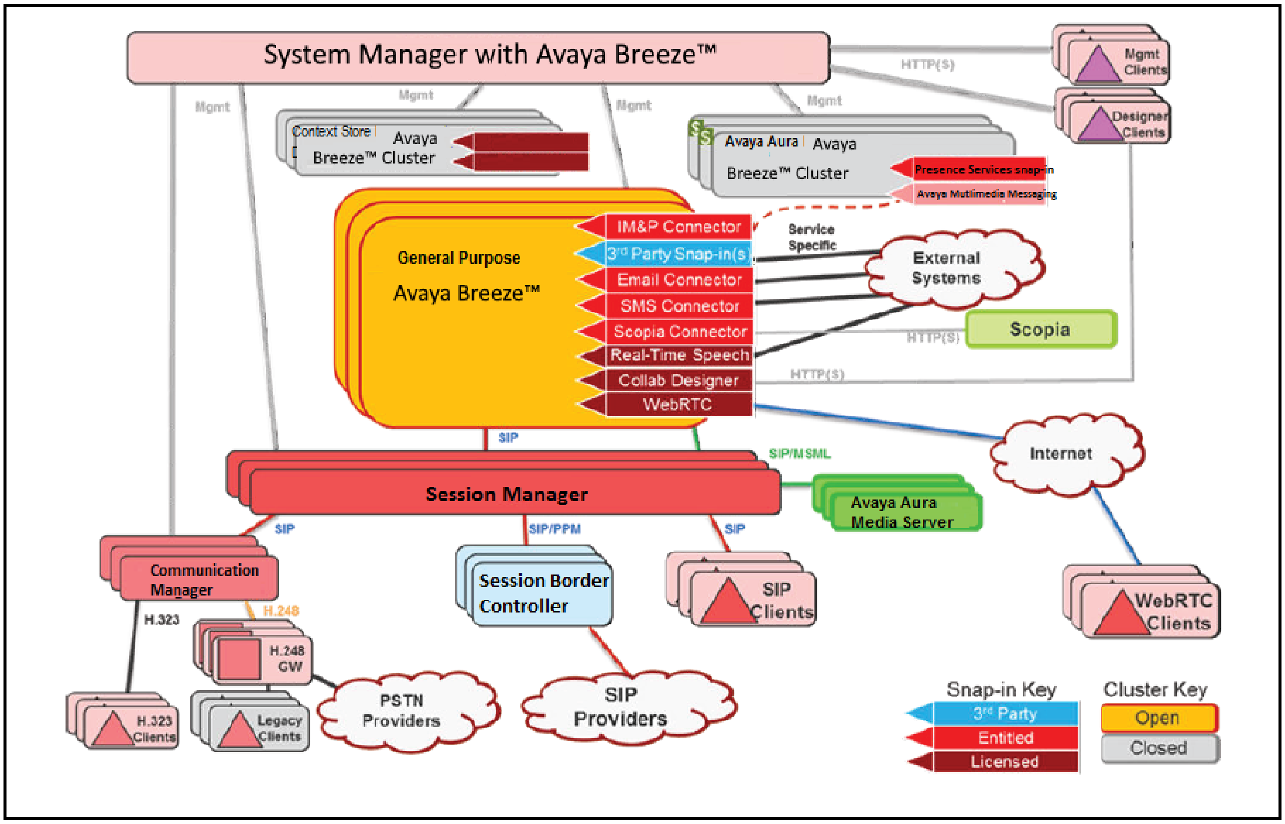
Location 2

Location 2 uses G430 Branch Gateway for media resources. The branch office uses 150 Avaya 9608 IP and SIP telephones and a 30-channel ISDN PRI card for PSTN connectivity. All endpoints work on POE and do not require local power supply. G430 Branch Gateway connects to the head office over WAN. The system uses Branch Session Manager and Survivable Remote in case of a connectivity failure at the head office.

Location 3

Location 3 uses G430 Branch Gateway for media resource and local connectivity. Location 2 uses 40 Avaya 9608 IP and SIP Phones. Location 3 uses a 30-channel PRI card for PSTN connectivity. All endpoints use POE and do not require local power supply. G430 Branch Gateway connects over WAN to Avaya servers in the head office . The setup uses the standard survivability capabilities with limited survivability features.

Avaya Breeze® platform



Solution overview

The Avaya Breeze® platform server runs in the Avaya Aura® environment. Avaya Breeze® platform complements and expands the core communication capabilities of Session Manager and Communication Manager. System Manager manages Avaya Breeze® platform that interoperates with Communication Manager 7.0.

Traditional H.248 gateways provide access to the PSTN and support for H.323 and legacy endpoints. Connection to SIP service provider trunks is provided through Avaya Session Border Controller to Session Manager.

All incoming and outgoing PSTN calls use Call Intercept services that run on Avaya Breeze® platform, regardless of the type of endpoint and the type of trunk. For ISDN trunks, Communication Manager routes outbound PSTN calls first to Session Manager and then to the ISDN trunk. Similar configuration is required for incoming calls over an ISDN trunk. Station-to-station calls cannot run Call Intercept services even if the endpoints are SIP endpoints.

Avaya Breeze® platform is deployed on one of the following:

- In Avaya appliance offer, on Appliance Virtualization Platform.
- In customer Virtualized Environment, on VMware™

Chapter 5: Security

Security philosophy

This section describes the security-related considerations, features, and services for the Avaya Aura® solution and its various components. Avaya Aura® needs to be resilient to attacks that can cause service disruption, malfunction or theft of service. Avaya‘s products inherit a number of mechanisms from legacy communications systems to protect against toll fraud or the unauthorized use of communications resources. However, Unified Communications capabilities, which converge telephony services with data services on the enterprise data network, have the additional need for protections previously specific only to data networking. That is, telephony services need to be protected from security threats such as:

- Denial of Service (DoS) attacks
- Malware (viruses, worms and other malicious code)
- Theft of data
- Theft of service

To prevent security violations and attacks, Session Manager uses Avaya‘s multilayer hardening strategy:

- Secure by design
- Secure by default
- Secure communications

For more information on security design for the various Avaya Aura® components, see the following documents:

- *Avaya Aura® Session Manager Security Design*
- *Avaya Aura® Communication Manager Security Design*
- *Avaya Aura® System Manager Security Design*
- *Avaya Aura® Messaging Security Design*

Secure by design

Secure by design encompasses a secure deployment strategy that separates Unified Communications (UC) applications and servers from the enterprise production network. Since all SIP sessions flow through Session Manager, being the SIP routing element, it is able to protect the UC applications and servers from network, transport, and SIP Denial of Service (DoS) attacks, as well as protect against other malicious network attacks. For customers that deploy SIP trunks to SIP service providers, use Avaya Aura® Session Border Controller to provide an additional layer of security between the SIP service provider and Session Manager.

The architecture is related to the trusted communication framework infrastructure security layer and allows for the specification of trust relationships and the design of dedicated security zones for:

- Administration
- Gateway control network
- Enterprise network
- Adjuncts
- SIP Elements

For Communication Manager, Avaya isolates assets such that each of the secure zones is not accessible from the enterprise or branch office zones. The zones are like dedicated networks for particular functions or services. They do not need to have access from or to any other zones because they only accommodate the data they are built for. This provides protection against attacks from within the enterprise and branch office zone.

Gateways with dedicated gatekeeper front-end interfaces (procr) inspect the traffic and protect the server zone from flooding attacks, malformed IP packets, and attempts to gain unauthorized administrative access of the server through the branch gateways. This architecture and framework can also flexibly enhance the virtual enterprise and integrate branch offices into the main corporate network. The security zone from the branch office can terminate at the central branch gateway interfaces, again protecting the heart of Communication Manager.

Secure by default

Secure by default is a security strategy of ensuring Avaya products only install software, services required for the operation of the product. For Avaya turnkey products, this includes a hardened configuration of the operating system, and wherever possible the default configuration of the product is to by default enable security features of the product.

In many cases, for Avaya products that run on the Linux operating system, modified kernels are used. The Linux operating system limits the number of access ports, services, and executables and helps protect the system from typical modes of attack. At the same time, the reduction of Linux services limits the attack surface.

Secure communications

Secure communications uses numerous features and protocols to protect access to and the transmissions from Avaya communications systems. Avaya uses media encryption to ensure privacy for the voice stream. Alongside media encryption, integrated signaling security protects and authenticates messages to all connected SIP elements, IP telephones, and gateways, and minimizes an attacker's ability to tamper with confidential call information. These features protect sensitive information like caller and called party numbers, user authorization, barrier codes, sensitive credit card numbers, and other personal information that is keyed in during calls to banks or automated retailers.

Critical adjunct connections are also encrypted. IP endpoints additionally authenticate to the network infrastructure by supporting supplicant 802.1X protocols. Network infrastructure devices like gateways or data switches act as an authenticator and forward this authentication request to a customer authentication service.

Trust management

Various protocols are used for inter-element communication within a deployment. These protocols include SIP, HTTPS, RMI (Remote Method Invocation), and JMX (Java Management Extensions). The common method for securing these protocols is TLS (Transport Layer Security). TLS will be used to secure the communication channel to prevent eavesdropping and message tampering. In addition, credentials used to establish these mutually authenticated TLS sessions can be leveraged to provide element–level authentication and authorization.

Identity (endpoint or Server) and Trusted (Root) Certificates are integral in establishing such TLS sessions. PKI (Public Key Infrastructure) is a commonly used and scalable technology to facilitate provisioning and remote management of these certificates and establish trust domains for a deployment.

The Trust Management Service delivered via the System Manager Centralized Management System is responsible for,

- Participating in a customer’s Public Key Infrastructure (PKI), if one exists.
    - For customers that do have a PKI within their enterprise but would like to create a separate domain of trust (derived from their Root CA) for Avaya components OR use a third-party (e.g., Verisign) as their trust provider.
- Lifecycle management of identity certificates for Avaya products,
    - Secure storage of Private Keys
    - Issuance of Certificates
    - Renewal of Certificates
    - Revocation of Issued Certificates

- Publish revocation information for issued certificates.
- Centralized Management (view, add and delete) of Trusted Certificates.

Avaya products interact with the System Manager Trust Management Service using the SCEP protocol for certificate enrollment, and by providing a web service interface and a JMX interface to enable remote management of certificates by System Manager’s Trust Management Service.

Certificate management

For detailed information about certificate management, refer to the following sections:

- “Certificate Management” in *Administering and Maintaining Avaya Aura® Application Enablement Services*.
- “Security configuration” in *Implementing and Administering Avaya Aura® Media Server*.
- “Managing certificates” in *Administering Avaya Aura® System Manager*.
- “Certificate management” in *Administering Avaya Aura® Session Manager*.
- “Certificate management” in *Administering Avaya Aura® Communication Manager*.
- “Certificate management” in *Avaya Aura® Presence Services Snap-in Reference*.

Authentication

The Avaya Aura architecture defines authentication as the process of verifying an identity which may belong to a user, an application or system.

The Avaya Aura Architecture’s Session Manager provides the SIP Registrar/Proxy function referred to in this section. Devices connecting to a SIP Registrar/Proxy can be divided into two categories:

- *Un-trusted:* The SIP Proxy/Registrar will NOT accept PAI from devices in un-trusted realm. Any entity or device not identified in the SIP Registrar/Proxy’s trusted host list falls into this category.
- *Trusted:* The SIP Proxy/Registrar will accept PAI from trusted entities or devices. A trusted device is also referred to as a trusted host. To be trusted there must be a corresponding entry in the SIP Registrar/Proxy’s trusted host list. To identify trusted hosts, the following authentication mechanisms will be applied.

Authorization

Avaya Aura Session Manager is responsible for authentication of other SIP entities and acts as a portal to the Aura. All service requests are dispatched through the portal and orchestrated across applications to validate and complete each request. Asynchronous event responses are delivered to clients by marshalling then through Session Manager.

Thus, client access authentication centralized and pivoted at Session Manager. However, access control to resources and operations are distributed through the system depending on the granularity of control.

Coarse-grained (high-level) access controls are enforced at the service portal, service type handlers or interface handlers.

Finer-grained Access Control, however, is distributed through services where the requested action is executed - where knowledge (context) for application-specific decisions is available.

Chapter 6: Management of system and network outages

Management of system and network outages

The Avaya Aura® solution offers several methods to ensure its reliability. Avaya has a long-standing commitment to high availability in hardware and software design and the architectural strength.

This section describes availability and its significance to a communications system. Hardware-design considerations, software-design and recovery considerations, and IP and SIP telephone and remote branch gateway recovery. The reliability methods include duplicated systems and backup systems available if there is a problem with the main system or a network outage.

This section covers the following methods:

- Reliability
- Availability
- Survivability
- Redundancy
- Recovery after an outage

Reliability

Customers need the full reliability of their traditional voice networks, including feature richness and robustness, and they want the option of using converged voice and data infrastructures. With the convergence of voice and data applications that run on common systems, a communications failure could bring an entire business to a halt. Enterprises are looking to vendors to help them design their converged infrastructure to meet their expected availability level.

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.

Availability

Availability is an associated service implementation that ensures a prearranged level of operational performance during a time period. For the Avaya Aura® solution it means users want their telephones and video devices to be ready to serve them at all times.

In this context, the term availability describes the use of duplicated servers. The term high availability describes specifically Appliance Virtualization Platform use of duplicated servers.

Communication Manager availability

High availability communications require the system to work reliably with pre-existing transport infrastructures and to integrate with a wide variety of external connectivity options. As a result, the underlying architecture must be designed to support reliable performance at every level. Communication Manager uses a variety of techniques to achieve this high reliability and availability.

Communication Manager automatically and continually assesses performance, and detects and corrects errors as they occur. The software incorporates component to subassembly self-tests, error detection and correction, system recovery, and alarm escalation paths. The maintenance subsystem of Communication Manager manages hardware operation, software processes, and data relationships.

Servers running the duplex template provide server redundancy, with call preserving failover, on the strength of the Linux operating system.

For more information about availability assessment and methodologies, see:

- The white paper, *Avaya Communication Manager Software Based Platforms: High Availability Solutions, Avaya Aura® Media Servers and Gateways*, available on the Avaya Support website, https://support.avaya.com.
- The white paper, *Building Survivable VoIP for the Enterprise*, available on the Tolly Group website https://tolly.com.

Communication Manager availability consists of providing a duplicated server pair that can be collocated or separated. These servers contain the same system and data files and work in an active/standby mode. When the active server fails, the servers interchange roles, and the standby server becomes the active server.

Collocated servers are generally in the same rack in the same room and connected by a crossover cable or through customer LAN using software duplication. With server separation, the two servers can be geographically separated. Server separation offers an improved survivability option by allowing the servers to reside in two different buildings across a campus or a small Metropolitan Area Network.

Server interchange

Server interchange is the process within a duplex server pair of a standby server becoming an active server. An arbiter process analyzes the state-of-health of both the active and standby servers and initiates a server interchange if the state of health of the active server is less than the state of health of the standby server. During this process, the standby server sends a request for the alias address. The ARP module resolves the IP address and sends an ARP reply packet with its Ethernet MAC address. The active server is seen by all the devices in the same subnet.

Each server has a unique IP address for the Processor Ethernet interface. A separate shared alias IP address is assigned to this interface on the active server and is used for connections to the Processor Ethernet interface on the active server. As part of the operations for a server interchange, the alias address is removed from the Processor Ethernet network interface on the server going standby, and it is added to the Processor Ethernet network on the server going active. After the interchange, a gratuitous ARP message is sent out from the Processor Ethernet interface on the server going active to update the MAC address in the ARP data cache stored in the IP endpoints on the local LAN that need to be connected to the PE interface.

The IP connection for the Processor-Ethernet-connected endpoints is not available during the server interchange. This is similar to a network outage. After the interchange, the Processor-Ethernet-connected endpoints use a short network IP address of the active server.

Fast server interchange

The fast server interchange process is available only for the devices connected to the Processor Ethernet on duplicated servers. The branch gateways and IP telephones must have the updated firmware. The active server preserves information about all the connections and connects to IP telephones and branch gateways before resuming normal operation. The IP telephones and branch gateways accept the incoming connection to replace the old connection.

In a scenario where some of the branch gateways and IP telephones are upgraded and others are not, the following statements are true:

- The upgraded branch gateways and telephones reconnect faster
- The other branch gateways and telephones take longer time to reconnect
- The other branch gateways and telephones may negatively impact the performance of the server following the server interchange

Connection preserving upgrades for duplex servers

This feature preserves stable bearer connections for TDM endpoints and IP stations during an upgrade of duplex servers. TDM and IP connection of branch gateways, with the duplex servers being the main call controller, are also preserved.

This feature is supported on all duplex servers and all port networks. It applies when upgrading to a newer release of Communication Manager.

This feature is not call preserving and only preserves connection on stable calls. Connection preservation does not apply to calls involving H.323 IP trunks; these are H.323 IP calls and SIP calls. Connection preservation does not apply to IP trunks and ISDN-BRI stations and trunks using branch gateway resources.

NIC teaming modes

Appliance Virtualization Platform supports two modes of NIC teaming: Active-Standby and Active.

Active-Standby

In normal operation all the traffic goes through the active NIC setup. If this connection fails, the other standby link is activated and all the traffic uses the standby link. The settings for active and standby setup are:

- Network failover detection: Link status only
- Notify Switches: Yes
- Failback: Yes. If the active NIC becomes available again, you can use the active NIC over the standby NIC.

Active-Active

This is an active setup that uses route based load balancing based on the originating virtual port ID. This is a basic form of load balancing that may not provide full capacity of both links.

- Load Balancing: Route based on the originating virtual port ID
- Network failover detection: Link status only
- Notify Switches: Yes
- Failback : Yes

Teaming NICs from CLI

About this task

You can configure the NIC teaming and NIC speeds on Appliance Virtualization Platform from the web interface of the Solution Deployment Manager client and System Manager Solution Deployment Manager. For more information, see *Administering Avaya Aura® System Manager*. Avaya recommends the use of Solution Deployment Manager web interface for configuring the NIC settings.

With Appliance Virtualization Platform, you can team NICs together to provide a backup connection when the server NIC or the Ethernet switch fails. You can also perform NIC teaming from the command line on Appliance Virtualization Platform.

Appliance Virtualization Platform supports Active-Standby and Active-Active modes of NIC teaming. For more information, see “NIC teaming modes”.

You cannot perform NIC teaming for S8300E server.

Procedure

1. Log in to the Appliance Virtualization Platform host command line, and type `# /opt/avaya/bin/nic_teaming list`.

   The system displays the current setup of the system, and lists all vmnics.

   For example:

   ```
   Current Setup:
   Name: vSwitch0
   Uplinks: vmnic0
   Name: vSwitch1
   Uplinks: vmnic1
   Name: vSwitch2
   Uplinks: vmnic2
   List of all vmnics on host:
   vmnic0
   vmnic1
   vmnic2
   vmnic3
   ```

2. To add a free vmnic to a vSwitch, type `# /opt/avaya/bin/nic_teaming add <vmnic> <vSwitch>`.

   The command changes the links to the active standby mode.

   For example, to add eth3 to the public virtual switch, type `# /opt/avaya/bin/nic_teaming add vmnic3 vSwitch0`. To verify the addition of eth3, type `esxcli network vswitch standard policy failover get -v vSwitch0`.

   The system displays the following message:

   ```
   Load Balancing: srcport
   Network Failure Detection: link
   Notify Switches: true
   Failback: true
   Active Adapters: vmnic0
   Standby Adapters: vmnic3
   Unused Adapters:
   ```

3. To add eth3 to the list of active adapters, type `# esxcli network vswitch standard policy failover set -v vSwitch0 --active-uplinks vmnic0,vmnic3`.

   The command changes the vmnic3 to the active mode.

4. To verify the mode of eth3, type `# esxcli network vswitch standard policy failover get -v vSwitch0`.

   The system displays the following message:

   ```
   Load Balancing: srcport
   Network Failure Detection: link
   Notify Switches: true
   Failback: true
   Active Adapters: vmnic0, vmnic3
   ```

```
Standby Adapters:
Unused Adapters:
```

5. To remove a vmnic from a vSwtich, type `# /opt/avaya/bin/nic_teaming remove <vmnic> <vSwitch>`.
6. To move an additional vmnic back to standby mode, type `# esxcli network vswitch standard policy failover set -v vSwitch0 --active-uplinks vmnic0 --standby-uplinks vmnic3`

   This puts the additional NIC back to standby mode.
7. To verify if the vmnic is moved to standby, type `# esxcli network vswitch standard policy failover get -v vSwitch0`.

   The system displays the following:

   ```
   Load Balancing: srcport
   Network Failure Detection: link
   Notify Switches: true
   Failback: true
   Active Adapters: vmnic0
   Standby Adapters: vmnic3
   Unused Adapters:
   ```

   Warning:

   The management and virtual machine network connections might be interrupted if you do not use correct network commands. Do not remove or change vmnic0, vmnic1, and vmnic2 from vSwitches or active modes.

Survivability

Survivability is the ability of the components within the Avaya Aura® solution to function during and after a natural or man-made disturbance. Avaya qualifies survivability for a given range of conditions over which the solution will survive.

This section addresses Session Manager and Communication Manager survivability options.

Communication Manager survivability

Communication Manager offers two survivability options: survivable core and survivable remote. Survivable core servers ensure business continuity in the event of connection failure or events leading to total failure of main server complex, such as natural disaster. Survivable remote servers enhance redundancy for branch gateways within networks. Survivable remote servers take over segments that have been disconnected from their primary call server and provide those segments with Communication Manager operation until the outage is resolved.

Branch gateways and IP endpoints

Branch gateways and H.323 endpoint registration on a survivable core server is allowed if you administer the **Enable PE for H.248 Gateways** and **Enable PE for H.323 Endpoints** fields on the Survivable Processor screen of the main server.

In the event of failure of a main server, the branch gateways and IP endpoints that are directly connected to the Processor Ethernet of the main server reregister to the Processor Ethernet on the survivable core or survivable remote server. See IP device with Processor Ethernet on page 69.

Note:

Two IP addresses are available to the IP endpoint: the IP address of the main server and the IP address of the survivable server. If the IP endpoint loses connectivity to its current primary gatekeeper, the IP device uses the alternate gatekeeper list for automatic recovery of service.

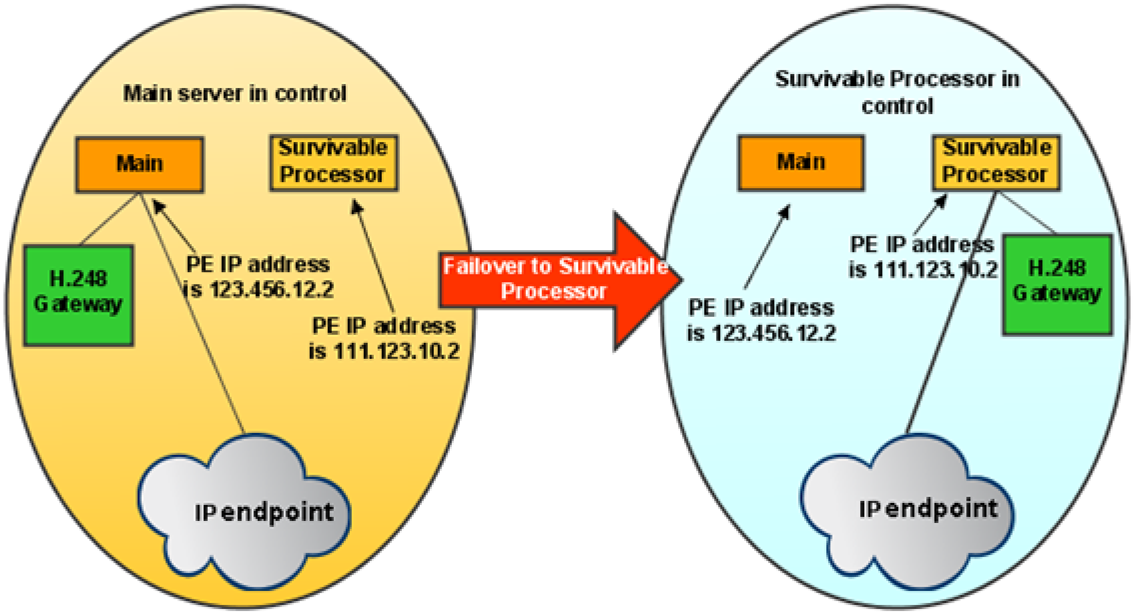

Main server in control
Main
Survivable Processor
H.248 Gateway
PE IP address is 123.456.12.2
PE IP address is 111.123.10.2
IP endpoint
Failover to Survivable Processor
Survivable Processor in control
Main
Survivable Processor
PE IP address is 111.123.10.2
H.248 Gateway
PE IP address is 123.456.12.2
IP endpoint

Figure 11: IP device with Processor Ethernet

IGAR and survivability

Inter-Gateway Alternate Routing (IGAR) enables systems with distributed gateways and distributed Call Centers an alternative means of providing bearer connection between port networks and branch gateways when the IP-WAN is incapable of carrying the bearer traffic. IGAR may request that bearer connections be provided by the PSTN under the following conditions:

- VoIP RTP resource exhaustion in a MG/PN is encountered.
- A codec set is not specified between a network region pair.
- Forced redirection between a pair of network regions is configured.

- The number of calls allocated or bandwidth allocated via Call Admission Control–Bandwidth Limits (CAC-BL) are reached.

IGAR takes advantage of existing public and private-network facilities provisioned in a network region.

Most trunks in use today are used for IGAR. Examples of the better trunk facilities for use by IGAR would be:

- Public or Private ISDN PRI/BRI
- R2MFC

IGAR is the next logical step in providing Quality of Service (QoS) to large distributed single-server configurations.

IGAR relies on Call Admission Control. When all VoIP RTP resources have been used, the next attempt to get a VoIP RTP resource results in denial of the VoIP connection. Communication Manager attempts to use existing applications and features to redirect the call accordingly. Each IP audio stream requires a VoIP RTP resource from either a G4xx media gateway or a branch gateway. Exactly how many audio streams can be supported by these resources depends on the codec selection. Upon hitting the VoIP RTP resource limit, IGAR immediately attempts to use an alternative path for a bearer connection to the network region of the called party using PSTN facilities allocated for use by the IGAR feature.

Survivable remote server

The survivable remote server provides survivability to IP and SIP telephones and one or more branch gateways when communication to the core is lost. The survivable remote server provides survivability for both Communication Manager and Session Manager.

A typical survivable remote solution contains the following components:

- Survivable Session Manager that provides service to users in case there is a WAN failure between branch and core.
- Survivable remote server (Communication Manager) for the branch gateway. The survivable remote server starts to work when the branch gateway loses connectivity with main Communication Manager and register itself to survivable remote server.
- Branch gateway that provides the ability to connect the branch to the PSTN and media services as conferencing, tones, and announcements.
- End user devices (telephones and video devices) that register themselves to core Session Manager as a primary controller, but uses the survivable Session Manager as a third controller in case of WAN failure.

The survivable remote server template can be installed on a simplex standalone server or on an embedded server.

Communication Manager

For Communication Manager the survivable remote server takes control of branch gateways that has its address in the Media Gateway Controller (MGC) list. The IP telephones use an Alternate Gateway List (AGL) for branch gateway addresses. These addresses are automatically generated by Communication Manager and sent to the IP telephones upon registration. Because the survivable remote server does not manage the procr, it cannot control port networks.

In a survivable remote environment, each IP endpoint and branch gateway is manually configured with a list of call controllers during initialization. If for any reason, the communication between a branch gateway and its primary controller stops, the branch gateways and the IP endpoints register with a call controller on its list. If the survivable remote server is in the list of call controllers, the branch gateway and the IP endpoint registers with the survivable remote server. The branch gateway registers with the survivable remote server first before the IP telephone registers with the survivable remote server.

For more information on the survivable remote servers as it relates to Communication Manager, see *Avaya Aura® Communication Manager Survivable Options*.

Session Manager

Session Manager for Survivable Remote is a set of software packages that acts as SIP routing and user relation elements when in survivable mode. It is built with the same specifications as the core Session Manager, providing survivability services for trunks, SIP stations and applications.

In the branch office are the branch SIP endpoints and a branch gateway. The endpoints are registered to both the core Session Managers and the survivable Session Manager. The endpoints have the concept of an active controller. The active controller is defined as the Session Manager to which the endpoints currently have subscriptions established. In sunny day operations, the core Session Manager is always the active controller. The survivable Session Manager receives no call traffic. The branch gateway is registered with the main Communication Manager. In rainy day operations, the survivable Session Manager is always the active controller. Currently, the only supported network outage is a complete branch WAN outage where all devices in the branch have lost contact with all devices in the core. Partial network outages are not guaranteed to exhibit desired redundancy behaviors.

For more information on the survivable remote server as it relates to Session Manager, see *Administering Avaya Aura® Session Manager*.

Telephone perspective

Session Manager supports simultaneous registration of telephones, a method that provides the greatest robustness using the SIP-outbound semantics. This means that SIP telephones simultaneously register with core Session Managers and the survivable Session Manager. The telephones accept incoming calls from any of these servers and automatically perform active controller selection according to existing algorithms. This means that although SIP telephones can receive calls from any of the registered controllers, telephones initiate calls through only the highest priority controller, the *active* controller. With an active controller outage, telephones mark the next controller in the list as the active controller for outbound services. Upon detecting the revival of the highest priority server, telephones move back to the revived controller as the active controller.

Alternate routing during rainy day

During a rainy day scenario, the survivable Session Manager provides the following three major tasks:

- Connects branch users to each other.

- Connects users to other non-survivable Session Manager users that reside on different branch.
- Connects users to other branches using PSTN trunks, such as emergency numbers and other branches.

Messaging during rainy day

Calls to a user on a survivable Session Manager

If a call comes into the core Session Manager because of centralized trunking, and the core cannot reach the user within the branch, the call goes to the user's coverage path and to voice mail, if administered as part of the coverage path. If a call comes in directly to the survivable Session Manager, there is no local messaging support.

Access to voice mail for survived users

There are two ways to access the voice messaging system when in survivable remote mode:

- Direct call to voice messaging system.
- A coverage method using special characters through which station-to-station calls from a branch location to the main location can be redirected over a PSTN trunk. Here is a description of the special characters:
    - The character *L* at the beginning of a coverage remote entry ensures that only the survivable core or remote server uses the entry. The main server considers this entry as unavailable.
    - The character *%* signifies *wait for answer.*
    - The character , instructs Communication Manager to pause, which is useful after a *wait for answer* to ensure the far-end is prepared to receive subsequent digits.
    - The character *D* denotes the called party's extension and allows the same coverage path and coverage remote entry to be used by many users sharing common characteristics.

Survivability for branch gateways

Branch Gateway recovery via survivable remote server

If the link between the remote branch gateway and the branch gateway controller is broken or the controller is down, the survivable remote server activates and assume call processing for the branch gateway. The branch gateway controller can be any simplex or duplex server. The strategy by which the branch gateways change control from the primary to the survivable remote controller is driven by the gateway using the branch gateway controller list.

When main server is a standalone server

The connectivity path between the remote branch gateway and the Call Controller are direct to the server Processor Ethernet interface.

The connectivity path directly to the Processor Ethernet interface of the server is as follows:

```
branch gateway ⇔ IP network ⇔ PE interface of the server
```

Link connectivity between the main call controller and the branch gateway is monitored through the exchange of keep-alive messages between the two components. If the link between the active call controller and the branch gateway breaks, the branch gateway tries to reestablish the link using the alternate gatekeeper list. The alternate gatekeeper list is divided into primary and secondary addresses. The primary addresses receive priority over the secondary addresses.

In the event of a WAN failure, any IP endpoint or branch gateway that cannot reach the primary controlling server registers with a survivable remote server controller in survivable mode. In the duplex server/branch gateway configuration, up to 50 survivable remote servers are available and ready for the fail-over process. The survivable remote server is always ready to acknowledge service requests from IP telephones and branch gateways that can no longer communicate with their main controller. Once the telephones and the branch gateway are registered, end users at the remote site have full feature functionality. This failover process usually takes less than 3 minutes. After failover, the remote system is stable and autonomous.

When main server is embedded server

In this configuration, the connectivity path between the branch gateway and the embedded S8300E server is:

```
Endpoint ⇔ IP Network ⇔ S8300E server
```

The link failure discovery and recovery process is the same as above. In this configuration, up to 10 survivable remote servers can back up the branch gateways that are controlled by the S8300E server.

Auto fallback to main server for branch gateways

Auto fallback to main server for branch gateways allows a branch gateway being served by a survivable remote server to automatically return to its primary gatekeeper. This feature is connection preserving; that is, stable bearer connections do not drop during this process.

The auto fallback process

Although the survivable remote server is the acting call controller, the branch gateway attempts to register with the main server every 30 s or whenever there are no active calls. This signaling also acts as keep-alive messages to the main server. The first registration request with the main server sets up encryption on the TCP link for H.248 messages. The branch gateway keeps the survivable remote registration until the branch gateway is accepted by the main server. Once registered with the main server, the branch gateway drops the survivable remote link. Once all branch gateways have migrated from the survivable remote server, that server unregisters all IP endpoints, which automatically reregister with the main server.

This automatic migration of branch gateways to the main server is administered to happen immediately (default), when there are no active calls, or at a scheduled time of a day.

Connection preserving failover/failback for branch gateways

This feature allows existing stable calls to be preserved when the branch gateway fails over to another server, or a survivable remote server, or returns to its main server. It is supported on all branch gateways. It applies to the failover and fallback of branch gateways to or from a survivable remote server and to or from a survivable core server.

During the failover/fallback process the bearer connection of stable calls are preserved. These include analog stations and trunks, DCP stations, digital trunks, IP stations using branch gateway resources, ISDN-PRI trunks, calls between gateways, IGAR, and previous connection-preserved calls.

Branch gateway standard local survivability

Standard local survivability (SLS) is survivable call processing engine that provides service to the branch gateway when the branch gateway cannot reach Communication Manager. This engine is resident in the branch gateway firmware and provides basic telephony functions at the branch without being registered to Communication Manager.

The SLS features are:

- Local station and outbound PSTN calling
- Inbound calls over the trunks to be delivered to available stations
- An H.323 gatekeeper for local IP phones to register
- Call Detail Recording in a syslog format

During transition to survivability mode, only local IP-IP calls are preserved.

The link recovery process follows these steps:

1. While SLS is enabled and processing, the branch gateway continues to seek an alternative branch gateway controller.
2. If Communication Manager accepts the registration, then the active IP-to-IP calls that shuffle are preserved.
3. The SLS application stops processing any new calls and goes to inactive mode.

Redundancy

Geographic Redundancy overview

Avaya Aura® provides System Manager Geographic Redundancy, a resiliency feature that handles scenarios where the primary System Manager server fails or the data network partially loses connectivity. In such scenarios, the system manages and administers products such as Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the customer enterprise using the secondary System Manager server.

For customers who need highly fault-tolerant deployments, System Manager supports System Manager Geographic Redundancy deployments that can provide the Active-Standby mode of resiliency.

From Release 8.0.1, System Manager also supports Geographic Redundancy in a mixed deployment environment.

From Release 7.0.1, System Manager supports deployment on different server types and different deployment modes in Geographic Redundancy. System Manager supports mixed:

- Servers from any combination of Avaya Supplied Avaya Solutions Platform 130 severs supported for System Manager.
- The primary System Manager server running as the only Avaya application on the server, while the secondary System Manager running along with other Avaya applications on another server and vice-versa.
- Servers from both customer-provided virtualized environment and Avaya Solutions Platform 130.

  For example, the primary System Manager server can be on Avaya Solutions Platform 130 and the secondary System Manager server can be on a customer-provided virtualized environment.

The following are some key differences between Geographic Redundancy and High Availability (HA) solutions:

Geographic Redundancy	HA
Addresses sudden, site-wide disasters.	Addresses server outages due to network card, hard disk, electrical, or application failure.
Distributed across WAN.	Deployed within a LAN.
Manual	Automated

You must deploy System Manager on both the standalone servers with separate IP addresses and configure Geographic Redundancy. If a managed product that supports the Geographic Redundancy feature loses connectivity to the primary System Manager server, the secondary System Manager server provides the complete System Manager functionality. However, you must manually activate the secondary System Manager server.

Note:

Only the system administrator can perform Geographic Redundancy-related operations.

You must reconfigure the elements that do not support Geographic Redundancy so that the elements can interact with the secondary System Manager server to receive configuration information. For more information about configuring elements that do not support Geographic Redundancy, see *Geographic Redundancy-unaware elements overview*.

During the installation of GR-unaware elements such as Presence Server, you must specify whether you want to enable the Geographic Redundancy feature on the element.

Out of Band Management in a Geographic Redundancy setup

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

Recovery

Network recovery

Conventional wisdom holds that network reliability is typically 3-9s (99.9%) on a LAN, and 2-9s (99%) on a WAN. The leading causes of network failure are a WAN link failure, administrator error, cable failure, issues that involve connecting new devices or services, and malicious activity, including DoS attacks, worms, and viruses. Somewhere lower down on the list are equipment failures. To achieve the highest levels of availability, it is important that a strong change control policy and network management strategy be implemented.

There are numerous techniques for improving the reliability of data networks, including spanning tree, self-healing routing protocols, network management, and change control.

Related links

Change control on page 76
Dial backup on page 78
Convergence times on page 79

Change control

Change control describes a process by which an organization can control nonemergency network changes and reduce the likelihood of administrator errors that cause network disruption. It involves carefully planning for network changes (including back-out plans), reviewing proposed changes, assessing risk, scheduling changes, notifying affected user communities, and performing changes when they will be least disruptive. By implementing a strict change control process, organizations can reduce the likelihood of administrator errors, which are a major cause of network disruption, and increase the reliability of their networks.

Related links

Network recovery on page 76

Layer 2 mechanisms to increase reliability

Spanning tree

IEEE 802.1D spanning tree is an Ethernet loop avoidance protocol. It allows network managers to connect redundant network links within their networks. Before the advent of spanning tree, loops within a switched Ethernet network would forward traffic around the loop forever, which saturated the network and prevented new traffic from getting through. Spanning tree selects one switch as a root and creates a loop-free topology connecting to the root. If loops are discovered, one switch blocks that port until its alternate path to the root is disrupted. Then the blocked port is brought back into service. There are several drawbacks to spanning tree:

- By default, all switches have the same priority, which means that root bridge selection can be suboptimal in a network.
- Spanning tree is slow to converge. It typically takes at least 50 s from link failure for a backup link to become active. As Layer 2 complexity increases, so does convergence time.

- Although there are mechanisms for speeding up spanning tree, most are proprietary.
- Traditional spanning tree is not VLAN aware. Thus, it will block links even if VLAN provisioning would have prevented a loop.

To solve these issues, the IEEE has recently introduced 802.1s and 802.1w enhancements. 802.1w introduces rapid spanning tree protocol (RSTP). RSTP uses active handshaking to speed up convergence times. 802.1s introduces multiple spanning trees (MST), which is a way of grouping different VLANs into different spanning tree instances.

Related links

Network recovery on page 76

Link aggregation groups

Link aggregation groups (LAGs) is a mechanism for combining multiple real interswitch links (typically four; Avaya products are configurable from two to eight) into one point-to-point virtual interswitch link. The advantage of this mechanism over spanning tree is that an organization can have the redundant links in if a failure occurs in one of the LAG links, the two switches will quickly discover it and remove the failed link from the LAG. This reduces the convergence time to nearly instantaneous. Not all implementations interoperate, so care must be taken when the LAG connects switches from multiple vendors. Also, LAG links are a point-to-point technology. They cannot be used to connect a backup switch in case the primary fails. When available, this is a very good mechanism for improving the resiliency of LANs.

Related links

Network recovery on page 76

Layer 3 availability mechanisms

Routing protocols

Routing protocols allow routers to dynamically learn the topology of the network. Should the topology of the network change, routing protocols update their internal topology table, which allows them to route around failure.

There are two types of routing protocol, distance vector and link state. Distance vector protocols, including RIP and IGRP, exchange their entire routing table periodically. To each route, they add their metric (for RIP, this is hop count) and insert it in the routing table. If updates fail to arrive before the router’s timer expires, it purges the route and looks for another path. These protocols are usually slow to converge. See Sample convergence times (single link failure) on page 79.

Link-state protocols, such as OSPF, take a more holistic view of the network. They compute the entire topology of the network and insert the best path to a destination in the routing table. Link state protocols exchange their routing tables only once, when routers first establish a relationship. After that, they only send updates. They also send hello messages periodically to ensure that the other routers are still present. Link state protocols converge much more quickly than distance vector protocols, and thus are generally better suited to networks that require high availability.

Related links

Network recovery on page 76

Virtual router redundancy protocol

Virtual router redundancy protocol (VRRP) and the related Cisco proprietary hot standby router protocol (HSRP) provide a mechanism to deal with router failure without disrupting endpoints on the network. In essence, these protocols work by assigning a virtual IP address and MAC address for the routers. This address is given to endpoints as their default gateway. The two routers send periodic hello messages marked with a priority value between each other. The high-priority router assumes the virtual address, and traffic flows through it. If the primary router fails or its capabilities become degraded (such as if a WAN link fails), the secondary router takes over. This is a useful mechanism to protect endpoints from router failures, and works with IP Telephony endpoints.

Related links

Network recovery on page 76

Multipath routing

Modern routers and Layer 3 switches allow multiple routes for a particular destination to be installed in the routing table. Depending on the implementation, this can be as high as six routes. Some implementations require that all routes that are inserted in the routing table have the same metric, while others allow unequal metric routing. In cases where the metric for all installed routes are the same, the router will load balance traffic evenly across each path. When the metric for multiple routes vary, the traffic is load balanced in proportion to the metric (in other words, if one path is twice as good as another, two-thirds of the traffic travels down the good path, and one-third of the traffic selects the other one). Asymmetric routing is suboptimal for voice, so route-caching (described earlier) should be considered in this environment.

In addition to using all (up to 6) active paths and optimally using available bandwidth, multipath routing greatly improves convergence time. As soon as a router detects a path failure, it remove it from the routing table, and sends all traffic over the remaining links. If this is a physical link failure, the detection time is nearly instantaneous. Therefore, you must use multipath routing, where available, across multiple links to a particular location.

Related links

Network recovery on page 76

Dial backup

One cost-effective technique for installing backup WAN links is to use dial backup. This can be done using either ISDN-BRI or analog lines. ISDN lines typically take 2 s to connect, while 56-kbps analog modems take approximately 1 min. Although this strategy is effective for data traffic, it is less effective for voice. First, the bandwidth may have been greatly reduced. If this is the case, the number of voice channels that can be supported might have been reduced proportionally. Also, if QoS is not properly applied to the backup interface, high packet loss and jitter can adversely affect voice quality. Finally, the time that is required to establish the new link can be up to 1 minute, which disrupts active calls. However, providing that these considerations are taken into account, proper QoS is applied, and a compressed codec is chosen, dial backup can be an effective solution for two to four users.

Related links

Network recovery on page 76

Convergence times

Convergence is the time that it takes from the instant a failure occurs in the network until a new path through the network is discovered, and all routers or switches are aware of the new path. Convergence times vary, based on the complexity and size of a network. Sample convergence times (single link failure) on page 79 lists some sample convergence times that are based on a single link failing in a relatively simple network. They reflect update and/or hello timers expiring. Dialup *convergence* times reflect the time that it takes to dial, connect, and authenticate a connection. These times do not take into account LAG, fast spanning tree, or multipath routing, which speed up convergence. This table shows the importance of carefully planning for fail-over in a network. For example, both OSPF and EIGRP (Layer 3) protocols converge faster than spanning tree (Layer 2). When designing a highly available data network, it is more advantageous to use Layer 3 protocols, especially link-state (OSPF) or hybrid (EIGRP) protocols, than Layer 2 (spanning tree).

Table 1: Sample convergence times (single link failure)

Protocol	Approximate convergence time (in seconds)
EIGRP (Cisco)	2
OSPF	6 to 46
RIP	210
Rapid spanning tree RSTP	10
Spanning tree (Layer 2)	50+
ISDN dialup (connect + authentication)	2
56-k dialup (connect + authentication)	60

Related links

Network recovery on page 76

IP endpoint recovery

Avaya's distributed IP-based systems experience increased availability by virtue of the alternate gatekeeper feature. When IP telephones register with Communication Manager, they are given a list of alternate gatekeepers to which they can re-register in the event of a failure.

The Avaya servers have a scalable architecture with different server components. These components provide processing and relay signaling information between Communication Manager and the Avaya IP endpoints. The system architecture is inherently distributed, providing the scalability to support a large number of endpoints and the flexibility to work in various network configurations.

This distributed nature of the architecture introduces additional complexity in dealing with endpoint recovery, since failure of any element in the end-to-end connectivity path between an IP endpoint and the switch software can result in service failure at the endpoint.

The recovery algorithm outlined here deals with detection and recovery from the failure of signaling channels for IP endpoints. Such failures are due to connectivity outages between the server and the endpoint, which could be due to failure in the IP network or any other component between the endpoint and the server.

The connectivity path between the endpoint and the server is:

```
Endpoint ⇔ IP network ⇔ Server PE interface
```

In this configuration, IP endpoints directly register to the server Processor Ethernet interface.

Recovery algorithm

In this configuration, the telephone registers to the server's Processor Ethernet Interface and the IP endpoint connects directly to the server Processor Ethernet. The connectivity path between the telephone and the server is:

```
Endpoint ⇔ IP network ⇔ Server
```

To discover connectivity failure, keep-alive messages are exchanged between the IP endpoint and the server. When the endpoint discovers that it no longer has communication with its primary gatekeeper, it looks at the next address on its list. If the next address is for a survivable remote server, then that server accepts the registration and begins call processing as long as media resources are available.

While the survivable server is not call preserving, the fail-over from primary gatekeeper to survivable server is an automatic process and does not require human intervention. The failback from a survivable server to a primary gatekeeper, however, is not currently automatic and requires a system reset on the survivable server. During the fallback to the primary gatekeeper, all calls are dropped with the exception of IP-to-IP calls.

IP endpoint time to service

The Time to Service (TTS) feature improves the time required to bring an IP endpoint into service by reducing the amount of required signaling for a telephone to reach the in-service state. Once a telephone is registered, TTS keeps the registration persistent for a relatively long Time to Live (hours) regardless of TCP connection failure, network outages, or even restarts of the endpoint. This significantly reduces the number of times that IP telephones need to re-register with Communication Manager due to outages. As a result, the TTS feature improves system availability after a network outage.

There are two functions in TTS that improves the availability of IP endpoints. One function is that the IP Endpoint Time-To-Service feature changes the way IP endpoints register with their gatekeeper, reducing the time to come into service. In the current Communication Manager architecture, there are two activities to bring the IP endpoints into service. The H.323 IP endpoint must register with Communication Manager and then it must establish a TCP socket connection between the server and the endpoint for call signaling. Since all the IP endpoints in a system strive to get into service as quickly as possible after an outage, the main server can be flooded with activity. In a system with a large number of IP endpoints, this flooding leads to delays not only for telephones trying to get into service but also for endpoints already in service trying to make calls.

The TTS separates the timing of the H.323 registration process from the timing of the TCP socket-connection setup process. This decoupling of the steps considerably improves the time for telephones to be in-service.

With TTS, after all the IP telephones within a system register to Communication Manager, the TCP socket is established when the processor occupancy level returns to normal. However, when the main processor occupancy level is high, the TCP socket is established on demand (when users make a first call or when a call needs to be delivered to a user) or via background maintenance. Once the TCP socket is established, the socket remains up for subsequent calls. In addition, with TTS, Communication Manager, rather than the IP endpoint, initiates the establishment of the TCP socket resulting in faster establishment of TCP sockets.

The second function of TTS significantly reduces the number of times that IP endpoints need to reregister with Communication Manager. This feature provides the capability to persist IP endpoint registrations across many network failures and other outages. Currently, whenever TCP sockets are dropped, the IP endpoints must reregister. With TTS, IP endpoints do not usually need to reregister for network outages that do not cause the system to failover to an survivable core or remote server. Since most issues with registration delays in the past have been after short network outages, this capability dramatically reduces the number of times that an IP endpoint needs to reregister with Communication Manager.

If reregistration is not required, only the re-establishment of the TCP socket is needed, which is also done in an on-demand fashion. Currently, in a call center environment, the agents must always log in again whenever the endpoint becomes unregistered. As a consequence of not requiring reregistrations after most outages, the agents' log-ins persist and they do not need to log in again.

Note that reregistration is still required for outages that cause the IP endpoints to failover to an survivable server (and then again when they recover back to the main server). In addition, a Communication Manager reset of level 2 (or higher) or a power cycle on the IP endpoints also requires IP endpoints to reregister because the information for the registration is erased under these conditions. For security reasons, IP endpoints also need to reregister with Communication Manager if they have not been able to communicate with Communication Manager over the RAS signaling channel for an extended period of time.

Changes in IP endpoints

Time to Service (TTS) features work only if corresponding changes are made to the Avaya H.323-based IP endpoints. The TTS algorithms are implemented in the IP endpoints. These TTS-enabled endpoints continue to support previous link recovery algorithms when communicating with a server that does not support TTS or does not have TTS enabled.

The TTS features works seamlessly with older IP endpoints. However, the benefits of the features are limited to the number of TTS-capable endpoints that support TTS deployed with Communication Manager.

Note:

16xx-series endpoints do not support TTS.

Operation with NAT/firewall environment

With the Time to Service (TTS) algorithm, the TCP connection for the call signaling channel is initiated by the server, not by the endpoints. With server-based NAT or firewall environments, the firewalls must be configured appropriately to allow TCP connections from the server to the endpoints.

Chapter 7: Performance engineering

Performance metrics

The following are Network Readiness Assessment requirements for VoIP specific to quality of a call.

Metric	Recommended	Acceptable
One-way Network Delay	< 80 milliseconds	< 180 milliseconds
Network Jitter	< 10 milliseconds	< 20 milliseconds
Network Packet Loss (Voice)	1.0%	3.0%
Network Packet Loss (Video)	0.1%	0.2%
QoS Enabled	Required	Required

Voice quality network requirements

This chapter lists some important network parameters that affect voice quality. In addition to endpoints, there are several network parameters that can influence voice quality. IP Telephony quality can be engineered and administered to several different levels to accommodate different business needs and budgets. Avaya provides network requirement options that can help customers to choose the best-suited voice quality for their organization.

Before implementing IP Telephony, you must measure the latency, jitter, and packet loss to ensure that all values are within bounds.

Network delay

In IP networks, packet delay (latency) is the length of time for a packet to traverse the network. Each element of the network, such as switches, routers, WAN circuits, firewalls, and jitter buffers, adds to packet delay.

Delay can have a noticeable effect on voice quality, but can be controlled in a private environment, such as a LAN or a WAN. Enterprises can reduce packet delays by managing the network infrastructure or by agreeing on a Service Level Agreement (SLA) with their network provider. An enterprise has less control over the delay when using the public Internet for VoIP.

Previously, ITU-T suggested 150 ms one-way delay as a limit for conversations. However, this value was largely misinterpreted as the limit to calculate a network delay budget for connections.

Depending on the desired voice quality, network designers can choose to increase or decrease this number for their network.

Customers must consider the following issues when designing a VoIP network:

- One-way delays of more than 250 ms can cause the well-known problem of *talk-over*. Talk-over occurs when both parties talk at the same time as the delay prevents them from realizing that the other person has already started talking.
- In some applications, delays less than 150 ms can impact the voice quality, particularly when the voice is accompanied with an echo.
- Long WAN networks is a major contributor to the network delay budget, averaging approximately 10-20 ms per 1000 miles. Some transport mechanisms, such as Frame Relay, can add additional delay. Additionally, staying within 150 ms, end to end, cannot be possible for all types of connections.
- One-way delays of over 400 ms on signaling links between port networks and the S8300E server can cause port network instability.

Again, there is a trade-off between voice quality and the technical and monetary constraints which businesses must consider. For this reason, the following guidelines assist customers for configuring one-way LAN/WAN delay between endpoints, not including IP telephones:

- 80 ms delay or less provides the best quality.
- 80 ms to 180 ms delay provides Business Communication quality. This delay range is better than cell phone quality if echo is properly controlled and well suited for a majority of businesses.
- Delays exceeding 180 ms can be acceptable depending on customer expectations, analog trunks used, codec type, and the presence of echo control feature in endpoints or network equipment.

Codec delay

In addition to packet delays, codecs also add some delay in the network. The delay of the G.711 codec is minimal. However, the G.729 codec, for example, adds approximately 10 ms of algorithmic delay in each direction, another 5 ms look-ahead, and signal processing delays.

The compression algorithm in G.723.1 uses multiple blocks, called frames, of 30 ms voice samples per packet, resulting in an increased latency over codecs configured to use 20 ms or less samples per packet.

The G.722 codec adds a 0.82 ms delay.

Jitter

Jitter is the difference in the time between the arrival of packets in an IP network. To compensate for jitter, VoIP endpoints contain a de-jitter buffer also called as a jitter buffer. Jitter buffers hold incoming packets for a specified duration so that voice samples can play at a normal rate to the user. In doing so, the jitter buffer also adds packet delay.

Excessive jitter can add to delay if the jitter still fits the size of the jitter buffer. Excessive jitter can also result in packet discard creating voice quality problems when the variation is greater than the jitter buffer size. The size of the static jitter buffers must be twice the largest statistical variance between packet arrivals. Dynamic jitter buffers give the best quality. However, the resizing algorithm of dynamic buffers must not result in adverse effects. Dynamic jitter buffering can exacerbate problems in an uncontrolled network. The network topology can also affect jitter. Multiple paths between endpoints with and routers enabled with load balancing can contribute significant amounts of jitter.

The following Avaya products have dynamic jitter buffers to minimize delay by automatically adjusting the jitter buffer size:

- Avaya G430 and G450 Branch Gateways and Avaya Aura® Media Server (MS)
- Avaya IP SoftPhone software

Packet loss

Packet loss occurs when the jitter buffer of an endpoint does not receive packets or receives the packets too late for processing. A longer delay or disordered packets can also amount to packet loss. Also, the network might appear to be losing packets when the network intentionally discards the packets because of late arrival at the endpoint. Unintentional packet loss in the network and discarded packets in the jitter buffers of the receiving endpoints characterize the quality of IP networks.

Packet loss can be bursty or more evenly distributed. Bursty packet loss has a greater effect on voice quality than distributed packet loss. Therefore, a 1% bursty loss has a more adverse effect than a 1% distributed loss.

The following are some effects of packet loss on a VoIP network:

- Every codec has a Packet Loss Concealment (PLC) method and because of the PLC, it becomes difficult for the network to detect packet loss. Therefore, a PLC-enabled compression codec, such as the G.729A, provides better voice quality than a full bandwidth G.711 codec without a PLC.
- Packet loss is more noticeable for tones such as fax tones or modem tones (other than DTMF) than for voice. The human ear can most likely detect packet loss during a tone, which uses a consistent pitch, than during speech, which uses a variable pitch.
- Packet loss is more noticeable for contiguous packet loss than for random packet loss over time. For example, the effect of losing 10 contiguous packets is worse than losing 10 packets evenly spaced over an hour.
- Packet loss is usually more noticeable with larger voice payloads per packet than with smaller packets, because more voice samples are lost in a larger payload.
- In the presence of packet loss, the time for a codec to return to normal operation depends on the codec type.
- Even minimal packet loss such as 0.12% can greatly affect the capability of a TTY/TDD device meant for people who are hard of hearing.
- Packet loss for signaling traffic increases network traffic substantially when the loss exceeds 3%, possibly impacting voice quality.

Network packet loss

Avaya offers customers a tiered approach to deal with network packet loss to balance new network costs and the constraints of business directives.

The maximum loss of IP packets or frames between endpoints must be:

- 1% or less for best quality.
- 3% or less for Business Communications quality. Business Communications quality is much better than cell phone quality.
- 3% and above is acceptable for voice but can negatively impact signaling, which can degrade voice quality due to increased traffic. For more information on signaling bandwidth requirements, see the white papers on the Avaya Support Web site at https://support.avaya.com.

Thìrd-party tools, such as Prognosis, can measure packet loss for ongoing calls.

Packet loss concealment

It is possible to reduce some amount of packet loss by generating voice samples to replace the missing samples. ITU standards G.711 Annex I and the G.729 standard define methods for packet loss concealment. For excessive packets, it is not possible to generate voice samples, therefore, packet loss concealment results in comfort noise generation (CNG).

PLC functions by slowly silencing the voice packets. PLC can be applied over the loss of a maximum of six consecutive packets.

Echo

The two main types of echo are acoustic echo and electrical echo caused by hybrid impedance mismatch. Usually, in a two-party call, only the speaker hears an echo but the listener does not. However, in a conference call, many parties might hear an echo.

Acoustic echo occurs when the voice of the speaker traverses through the airpath in the acoustic environment of the listener and reflects back to the microphone of the terminal of the listener. The severity of the echo effect depends on the acoustic properties of the room of the listener, such as, room size and wall reflection characteristics.

Electrical echo is also a reflection effect but is due to an impedance mismatch between four-wire and two-wire systems or in the interface between a headset and its adapter.

The perception of echo for the listener increases with delay. Usually, human ears ignore echo received within 30 ms. However, if the level of the received echo signal is extremely high, even 2 ms of delay causes a perception of echo. Echo received after 30 ms is usually perceived as annoyance. The perception of echo can be greater in the IP Telephony system because the end-to-end latency in some IP Telephony implementations exceeds the latency in some circuit-switched systems.

To reduce echo, customers must deploy echo cancellers at strategic places in telephones or network equipment. Echo cancellers, which have varying amounts of memory, store incoming voice streams in a digital form in a buffer and compare the received voice with the previously transmitted voice patterns stored in memory. If the patterns match, the echo canceller attempts to remove the newly received voice stream, but a residual level of echo is left even in optimal operating conditions.

Echo cancellers function properly only if the one-way delay between the echo canceller and the echo source, for example, the acoustic airpath at the telephone set or electrical hybrid, is not larger than the capacity of the echo canceller. Otherwise, the echo canceller does not find a pattern to cancel.

The Avaya G430 and G450 Branch Gateways, Avaya Aura® Media Server (MS), the Avaya IP SoftPhone, and all IP Telephones incorporate echo cancellation designed for IP Telephony to improve voice quality.

Signal levels

To provide better sound quality in telephone conversations, voice communication systems add an acoustic loss of 10 dB between the listener and the speaker. This 10 dB acoustic loss provides the level of sound quality that emulates a scenario where the speaker and listener are only one meter apart and having a face-to-face conversation. Any significant difference from this loss level is audible as too soft or too loud and can result in some degree of listener discomfort.

In IP Telephony networks, the voice communication system implements the 10 dB acoustic loss as follows:

- 8 dB in the telephone of the speaker
- 0 dB in the IP network
- 2 dB in the telephone of the receiver

To account for personal preferences or the presence of background noise, listeners can adjust the volume control of the telephone relative to the 10 dB loss value. The IP Telephony loss values are globally identical and specified in ITU-T Recommendations.

In traditional circuit-switched networks, the telephone that send, receive, and interport line or interport trunk losses are country-dependent. The end-to-end country-specified losses often differ somewhat from the 10 dB loss value. The country-dependency of loss values makes it more challenging to guarantee a proper listener signal level when the PSTN is involved or when signals traverse country borders.

IP Telephony gateways must provide proper signal level adjustments from the IP network to the circuit-switched network and in the reverse direction, and also between circuit-switched ports.

To configure Avaya endpoints across the globe, the devices must be programmed for loss values. To ensure that the signal levels are controlled properly within the scope of a voice network consisting of Avaya systems, customers must administer the appropriate country-dependent loss plan.

In addition to administering loss for two-party calls, Communication Manager provides country-dependent conference call loss administration. Loss is applied depending on the number of parties involved in the conference.

Echo and signal levels

In circuit-switched telephony, echo can be caused by acoustic reflection in the remote party environment or by electrical reflection from 2-wire to 4–wire analog-hybrid impedance mismatches. Impedance mismatch can occur in analog telephones and analog line/trunk cards, electrical cross-talk in circuitry, or in telephony wiring particularly in low-cost headsets. Due to this impedance mismatch that causes echo, the circuit-switched analog and digital telephones are implemented with a relatively large transmit loss. In principle, the transmit loss of telephones can be made very large followed by signal amplification in the receiving telephone. In practice, however, the transmit loss must be limited to prevent the electrical voice signal from dropping below electrical background noise. This has resulted in the adoption of transmit loss and receive loss values around 8 dB and 2 dB, respectively, although country-specific values can deviate from these values.

The loss plan administration that Communication Manager provides is primarily intended to control signal losses in telephones and gateways and not intended to control echo. However, in case of severe echo, the administered loss plan can be changed to a different plan. An increase in loss by a certain amount between two endpoints decreases the echo level by twice this amount. You must use this method of loss plan administration only after consulting Avaya Services personnel. To reduce echo, you must use echo cancellers with Avaya products.

Tone Levels

The level of call progress and DTMF tones played out through telephones must adhere to specified levels. Different countries follow different tone level standards which can be administered in Communication Manager. You can adjust the volume of received call progress tones using the telephone volume control.

Audio codecs

Codecs (Coder-Decoders) convert analog voice signals to digital signals and vice versa. Avaya supports several different codecs that offer varying bandwidth usage and voice quality. The following are some codecs that Avaya supports:

- G.711: This codec produces uncompressed audio at 64 kbps.
- G.729: This codec produces compressed audio at 8 kbps.
- G.723.1: This codec produces compressed audio at 5.3 or 6.3 kbps.
- G.722: This codec produces compressed audio at 64, 56, or 48 kbps.
- G.726: This codec produces compressed audio at 32 kbps.

Note:

The PolyCom-proprietary Siren codecs are audio only and support wide band. There are three Siren codecs:

- Siren 7 supports 7 KHz
- Siren 14 supports 14 KHz

- Siren 22 supports 22 KHz

The following table provides a comparison of voice quality considerations associated with some of the codecs supported by Avaya products.

Toll-quality voice must achieve a mean opinion score (MOS) of 4 or above. The MOS scoring is a long-standing, subjective method of measuring voice quality.

Table 2: Comparison of speech coding standards (without IP/UDP/RTP overhead)

Standard	Coding Type	Bit Rate (kbps)	MOS-LQO (Mean Opinion Score - Listening Quality Objective)
G.711	PCM	64	4.37
G.729	CS-ACELP	8	3.94
G.723.1	ACELPMP-MLQ	6.3 5.3	3.78 3.68
G.726	ADPCM	32	4.30

[1] As predicted. Measured according to ITU-IT Recommendation P.862 (PESQ). See draft Recommendation P.862.2, application guide for PESQ.

[2] Given MOS-LQO values for American English.

In a properly functioning IP network, the G.711 codec offers the highest level of voice quality as the codec does not use compression. Unfortunately, there is a trade-off with higher bandwidth usage. In situations where bandwidth is limited, such as across WAN links, G.729 provides good audio clarity and consumes less bandwidth.

Codecs with compression use twice as many signal processing resources than the G.711 codec. On the G430 media gateway, there are 120 DSP resources. Therefore, one media gateway supports:

- A maximum of 120 connections that use the G.711 codec
- A maximum of 60 connections that use the G.729 codec with compression

The G450 media gateway supports:

- 320 channels of G.711 (u/a-law)
- 320 channels of G.729A/G.729AB
- 320 channels of G.726 (32 kbps only)
- 320 channels of T.38
- 320 channels of V.32 SPRT

The above channel counts are the same if Advanced Encryption Standard (AES) encryption and SHA-1 authentication are enabled.

The Avaya One-X Deskphones (96xx) support the G.722 codec with 64 kbps and with 20 ms packets.

Usually, G.711 is used on LANs because bandwidth is abundant and inexpensive whereas G.729 is used across bandwidth-limited WAN links. G430 and G450 Branch Gateways can have varying amounts of DSP resources by adding more number of DAR daughter cards installed.

G.726 Codec and branch gateways

Media processing resources on branch gateways support the G.726 codec. For more information on the corresponding capacities, see Number of Simultaneous Bi-Directional Connections Supported on page 90. G430 supports 20 to 80 connections and G450 supports 80 to 320 connections.

Table 3: Number of simultaneous bidirectional connections supported

Codec	G430	G450
G.726A Unencrypted	10	16
G.726A with Avaya Encryption Algorithm (AEA) encryption	10	16
G.726A with Advanced Encryption Standard (AES) encryption	10	12

Video codecs

A video codec is a device or software that enables video compression or decompression or both. There are various kinds of video codecs available. Several companies have implemented these codecs by different algorithms, therefore, the codecs have different specifications and applications in various fields. These video codecs generally comply with Industry standards.

Avaya uses the following signaling and content codecs in video:

- Video codecs for transmitting content:
    - H.261: Known as MPEG-1. This codec is the first to support video over ISDN.
    - H.263: This is a well-known video-conferencing codec that is optimized for low data rates and low motion.
    - H.264: This codec supports high definition video and is used by Blu-Ray players, YouTube, iTunes, and Adobe Flash. You can use this codec for high definition video conferencing.
- Video codecs for multimedia signaling:
    - H.224: This codec is well-supported by Microsoft and is primarily used by soft clients, such as Avaya one-X® Communicator, that support video signaling.
    - H.224.1 (data, far-end camera control): This signaling codec is used by video conferencing companies like PolyCom and LifeSize.

Various video codecs are technically differentiated from each other based on several factors such as compression technology, compression algorithm, supported platform, sampling, and supported OS.

Silence suppression or voice activity detection

You can use Voice Activity Detection (VAD) or silence suppression to save bandwidth. During a conversation, because only one party is speaking at a time, more than 40% of the transmission is silence. VAD in Avaya IP telephones monitor the locally produced voice signal for voice activity. When there is no voice activity for a configured period of time, the network does not transmit any packets, resulting in bandwidth savings.

When you enable silence suppression, the network at the remote end is made to generate *comfort noise* that fills the artificial silence in a transmission when no voice is present during a conversation. The trade-off with silence suppression lies with the silence detection algorithm. If the algorithm is too aggressive, the beginnings and ends of words can be *clipped*. If not aggressive enough, no bandwidth is saved.

Silence suppression is built into G.729B and can be enabled for other codecs from within Communication Manager. Because of voice quality concerns with respect to clipping, silence suppression is disabled by default with the exception of G.729B.

The following Avaya products use silence suppression to preserve bandwidth:

- The Avaya Communication Manager software (for control)
- All Avaya IP Telephones
- Avaya IP SoftPhone
- Avaya Media Gateways

For procedures to administer QoS parameters, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.

Transcoding overview

Transcoding or tandeming occurs when a voice signal passes through multiple codecs, for example, when the call coverage is applied on a branch office system to a centralized voice mail system. These calls might experience multiple transcodings including, for example, G.729 across the WAN and G.711 into the voice mailbox. Each transcoding action results in degradation of voice quality. Avaya products minimize transcoding using methods such as shuffling and hairpinning.

IP Telephony network engineering overview

In the early days of local area networking, network designers used hubs to connect servers, workstations, and routers to split the network into manageable sub-networks. Because of the high cost of router interfaces and the inherent limitations of shared-media hubs, network design was fairly simple. In recent years, with the rise of switches to split networks, a network with minimal faults was still able to provide good performance. As a result, network design was often less than optimal. IP Telephony places new demands on the network. Suboptimal design cannot cope with these demands. With the installation of switches, a company must also follow industry best practices to have a properly functioning voice network. Therefore, for better voice quality, administrators must implement a well-designed network before beginning IP Telephony deployments.

Network engineering overview

Industry best practices dictate that a network be designed considering the following factors:

- Reliability and redundancy
- Scalability
- Manageability
- Bandwidth

Voice mandates consideration of the following additional factors when designing a network:

- Delay
- Jitter
- Loss
- Duplex

In general, these concerns dictate a hierarchical network that consists of at most three layers (Layers in a hierarchical network on page 92):

- Core
- Distribution
- Access

In some networks, a single device can perform the functions of several layers.

Table 4: Layers in a hierarchical network

Layer	Description
Core	The core layer is the heart of the network. The core layer forwards packets as quickly as possible. The core layer must be designed with high availability in mind. Usually, these high-availability features include redundant devices, redundant power supplies, redundant processors, and redundant links. Today, core interconnections increasingly use 10 Gigabit Ethernet or higher.
Distribution	The distribution layer links the access layer with the core. The distribution layer is where policy like the QoS feature and access lists are applied. Generally, Gigabit Ethernet connects to the core, and either Gigabit Ethernet or 100base-TX/FX links connect the access layer. Redundancy is important at this layer but not as important as in the core. This layer is combined with the core in smaller networks.
Access	The access layer connects servers and workstations. Switches at this layer are smaller, usually 24 to 48 ports. Desktop computers, workstations, access points, and servers are usually connected at 100 Mbps or 1 Gbps. Limited redundancy is used. Some QoS and security features can be implemented in the access layer. Mostly, Power over Ethernet (PoE) is included to power IP telephones and other access devices.

For IP Telephony to work well, WAN links must be properly sized with sufficient bandwidth for voice and data traffic. Each voice call uses 9.6 kbps to 120 kbps, depending on the desired codec, payload size, and header compression used. Additional bandwidth might be used if video or redundancy for fax, modem, and TTY is implemented. The addition of video can stress WAN links engineered for voice only. WAN links must be re-engineered when video is introduced to an existing network. The G.729 compression algorithm, which uses about 27 kbps of bandwidth, is one of the most used standards today. Traditional telephone metrics, such as average call volume, peak volume, and average call length, can be used to size interoffice bandwidth demands. For more information, see Traffic engineering on page 139.

Quality of Service (QoS) also becomes increasingly important with WAN circuits. In this case, QoS means the classification and the prioritization of real-time traffic such as voice, video, or FoIP. Real-time traffic must be given absolute priority through the WAN. If links are not properly sized or queuing strategies are not properly implemented, the quality and the timeliness of voice and data traffic will be less than optimal.

The following WAN technologies are commonly used with IP Telephony:

- Multiprotocol Label Switching (MPLS)
- Asynchronous Transfer Mode (ATM)
- Frame Relay
- Point-to-point (PPP) circuits
- Internet VPNs

MPLS, ATM, Frame Relay, and PPP circuits, all have good throughput, low latency, and low jitter. MPLS and ATM have the added benefit of enhanced QoS. MPLS is a relatively new service offering and can have issues with momentary outages of 1 to 50 sec duration.

Frame Relay WAN circuits can be difficult to use with IP Telephony. Congestion in Frame Relay networks can cause frame loss, which can significantly degrade the quality of IP Telephony conversations. With Frame Relay, proper sizing of the committed information rate (CIR) is critical. In a Frame Relay network any traffic that exceeds the CIR is marked as discard eligible, and is discarded at the option of the carrier if it experiences congestion in its network. Because voice packets and other real-time packets must not be dropped during periods of congestion, CIR must be sized to maximum traffic usage. Also, Service Level Agreements (SLAs) must be established with the carrier to define maximum levels of delay and frame loss and remediation if the agreed-to levels are not met.

Internet VPNs are economical but more prone to quality issues than the other four technologies because there is no control or SLA to modify the handling of voice packets over data packets.

Network Management is another important area to consider when implementing IP Telephony. Because of the requirements imposed by IP Telephony, it is critical to have an end-to-end view of the network and ways to implement QoS policies globally. Products such as HP OpenView Network Node Manager, Prognosis, Concord NetHealth, and MRTG help administrators maintain acceptable service. Outsource companies are also available to assist other companies that do not have the resources to implement and maintain Network Management.

Voice quality

Defining *good* voice quality varies with business needs, cultural differences, customer expectations, and the hardware and software used. The requirements set forth are based on the ITU-T and EIA/TIA guidelines and extensive testing. Avaya requirements meet or exceed most customer expectations. However, the final determination of acceptable voice quality lies with the customer definition of quality and the design, implementation, and monitoring of the end-to-end data network.

Quality is not a discrete value where the low side is good and the high side is bad. A trade-off exists between real-world limits and acceptable voice quality. Lower delay, jitter, and packet loss values can produce the best voice quality, but might also come with a cost to upgrade the network infrastructure to get to the low values. Another real-world limit is the inherent WAN delay. An IP trunk that links the west coast of the United States to India could add a fixed delay of 150 ms into the overall delay budget.

Perfectly acceptable voice quality is attainable but will not be toll quality. Therefore, Avaya presents a tiered choice of elements that make up the requirements.

The critical objective factors in assessing IP Telephony quality are delay, jitter, and packet loss. To ensure good and consistent levels of voice quality, Factors that affect voice quality on page 94 lists Avaya's suggested network requirements. These requirements are valid for both LAN only and for LAN and WAN connections. Note that all measurement values are between endpoints and therefore reflect the performance of the network without endpoint consideration.

Table 5: Factors that affect voice quality

Network factor	Measurement
Delay (one-way between endpoints)	• A delay of 80 ms or less can, but might not, yield the best quality. • A delay of 80 ms to 180 ms can yield business-communication quality. Business-communication quality is much better than cell phone quality, and is well-suited for a majority of businesses. Also, business-communication quality is defined as less than toll quality but much better than cell phone quality. • Delays that exceed 180 ms might still be acceptable depending on customer expectations, analog trunks used, and the codec type.
Jitter (variability of the delay between endpoints)	• 20 ms or less than half the sample size, for the best quality. **Note:** This value has some latitude, depending on the type of service that the jitter buffer has in relationship to other router buffers and the packet size used.
Packet loss (maximum packet/frame loss between endpoints)	• < 1% can yield the best quality, depending on several factors. • < 3% gives business communications quality, which is much better than cell phone quality. • > 3% might be acceptable for voice but might interfere with signaling.

For more information, see Voice quality network requirements on page 83.

Best practices

To consistently ensure the highest quality voice, you must follow industry best practices when implementing IP Telephony. Note that these suggestions are only options and might not fit individual business needs in all cases.

- QoS/CoS

  QoS for real-time packets is obtained only after a Class of Service (CoS) mechanism tags voice packets as having priority over data packets. Networks with periods of congestion can still provide excellent voice quality when using a QoS/CoS policy. The recommendation for switched networks is to use IEEE 802.1p/Q. The recommendation for routed networks is to use DiffServ Code Points (DSCP). The recommendation for mixed networks is to use both. You can also port priority to enhance DiffServ and IEEE 802.1p/Q. Even networks with sufficient bandwidth should implement CoS/QoS to protect voice communications from periods of unusual congestion that a computer virus might cause. For more information,

- Switched network

  A fully switched LAN network is a network that allows full duplex and full endpoint bandwidth for every endpoint that exists on that LAN. Although IP Telephony systems can work in a shared or hub-based LAN, a switched network provides consistently high results to IP Telephony.

- Network assessment

  A Basic Network Readiness Assessment Offer from Avaya is vital to a successful implementation of IP Telephony products and solutions. Go to the Avaya Support website at https://support.avaya.com for current documentation, product notices, knowledge articles related to the topic, or to open a service request.

- VLANs

  Placing voice packets on a separate VLAN or subnetwork from data packets is a generally accepted practice to reduce broadcast traffic and to reduce contention for the same bandwidth as voice. Note that Avaya IP Telephones provide excellent broadcast storm protection. Other benefits become available when using VLANs, but there can be a substantial cost with initial administration and maintenance.

Common issues

Some common negative practices that can severely impact network performance, especially when using IP Telephony, include:

- A flat, non-hierarchical network

  For example, cascading small workgroup switches together in a flat non-hierarchical network. This technique quickly results in bottlenecks, because all traffic must flow across the uplinks at a maximum of 10 Gbps, versus traversing switch fabric at speeds of 256 Gbps or greater. The greater the number of small switches or layers, the greater the number of uplinks, and the lower the bandwidth for an individual connection. Under a network of this type, voice performance can quickly degrade to an unacceptable level.

Avaya recommends that the network segments connected to the Session Manager network interfaces have a netmask of at least 23 bits or more. Issues can arise when the Session Manager is connected to large network segments where ARP traffic on causes kernel buffer issues and continual garbage collection of the ARP cache. For network segments with a netmask of 23 bits or more, you can restrict the number of network devices on that segment to 512, and the kernel ARP cache can handle that with no negative impact on Session Manager.

For example:

a netmask of 255.255.255.0 is 24 bit that will allow up to 256 devices in the subnet, and

a netmask of 255.255.254.0 is 23 bit that will allow up to 512 devices in the subnet.

- Multiple subnets on a VLAN

  A network of this type can have issues with broadcasts, multicasts, and routing protocol updates. This practice can have a significant negative impact on voice performance and complicate troubleshooting.

- A hub-based network

  All hubs must be replaced with switches if they will lie in the path of IP telephony. Hubs are half-duplex by definition and can degrade the performance of real-time communications over IP.

- Too many access lists

  Access lists slow down a router. While access lists are appropriate for voice networks, you must not apply them to unnecessary interfaces. Traffic should be modeled beforehand and access lists applied only to the appropriate interface in the appropriate direction, not to all interfaces in all directions.

Customers must exercise caution when using the following:

- Network Address Translation (NAT)

  IP Telephony cannot work across NAT because if private IP addresses are exchanged in signaling messages, these addresses are not reachable from the public side of the NAT and cannot be used for the media sessions.

- Analog dial-up

  Be careful in using analog dial-up (56 kbps) to connect two locations. Upstream bandwidth can be limited to a maximum of 33.6 kbps and is lesser usually, resulting in insufficient bandwidth to provide quality voice. Some codecs and network parameters provide connections that are acceptable, but consider each connection individually.

- Virtual Private Network (VPN)

  Large delays are inherent in some VPN software products due to encryption, decryption, and additional encapsulation. Some hardware-based products that encrypt at near wire speed can be used. In addition, if the VPN is run over the Internet, sufficient quality for voice cannot be guaranteed unless delay, jitter, and packet loss are contained within the listed parameters.

LAN issues

This section covers Local Area Network (LAN) issues, including speed and duplex, inline power, and hubs versus switches.

General guidelines

Because of the time-sensitive nature of IP telephony applications, IP telephony should be implemented on an entirely switched network. Ethernet collisions, which are a major contributor to delay and jitter, are virtually eliminated on switched networks. Additionally, the procr, media server, and IP telephones should be placed on a separate subnetwork or VLAN (that is, separated from other non-IP telephony hosts). This separation provides for a cleaner design where IP telephony hosts are not subjected to broadcasts from other hosts and where troubleshooting is simplified. This separation also provides a routed boundary between the IP telephony segments and the rest of the enterprise network, where restrictions can be placed to prevent unwanted traffic from crossing the boundary. When personal computers are attached to IP telephones, the uplink to the Ethernet switch should be a 100 Mbps link or greater, so that there is more bandwidth to be shared between the telephone and the computer.

Avaya solutions for large flat subnets with thousands of devices on them is not a supported configuration. If IP telephones and Avaya servers will share a subnetwork with other hosts, the IP telephones and Avaya servers should be placed on a subnetwork of manageable size (24-bit subnet mask or larger, with 254 hosts or less), with as low a rate of broadcasts as possible. With this situation, a worst-case example is the scenario where IP telephones and Avaya servers are deployed on a large subnetwork that is running IPX or other broadcast-intensive protocol, with broadcasts approaching 500 per second. There is an arp cache limit of 1024. When the arp cache is full, it will be unable to communicate with any new hosts until the arp cache times out on other hosts. So, network segregation into smaller subnets like /24 or the creation of VLANs, or doing both is strongly recommended.

Ethernet switches

The following recommendations apply to Ethernet switches to optimize operation with Avaya endpoints. These recommendations are meant to provide the simplest configuration by removing unnecessary features.

- Enable spanning tree fast start feature or disable spanning tree at the port level. The Spanning Tree Protocol (STP) is a Layer 2 loop-avoidance protocol. When a device is first connected or reconnected to a port that is running spanning tree, the port takes 31 to 50 s to cycle through the Blocking, Listening, and Learning states. This delay is neither necessary nor desired on ports that are connected to IP endpoints. Instead, enable a fast start feature on these ports to put them into the Forwarding state almost immediately. If this feature is not available, you can consider the option of disabling the spanning tree on the port. Do not disable spanning tree on an entire switch or VLAN. Also, Rapid Spanning Tree Protocol (802.1w) is always preferred over STP (802.1D). When using RSTP, the Ethernet switch ports connected to IP phones must be in the *Edge-Type* mode. This places the port in a fast-start mode. Bridge Protocol Data Unit (BPDU) guard is also desirable if it is available on the Ethernet switch to protect against a loop created through the IP phone.

- Disable the vendor features that are not required. Some vendor features that are not required by Avaya endpoints include EtherChannel/LAG, cdp, and proprietary (not 802.3af) inline power. These features are nonstandard mechanisms that are relevant only to vendor-specific devices and can sometimes interfere with Avaya devices.
- Properly configure 802.1Q trunking on Cisco switches. When trunking is required on a Cisco CatOS switch that is connected to an Avaya IP telephone, enable it for 802.1Q encapsulation in the no-negotiate mode. This causes the port to become a plain 802.1Q trunk port with no Cisco autonegotiation features. When trunking is not required, explicitly disable it.

Speed and duplex

One major issue with Ethernet connectivity is proper configuration of the speed and duplex settings. The speed and duplex settings must be configured properly and must match.

A duplex mismatch condition results in a state where one side perceives a high number of collisions, while the other side does not. This results in packet loss. Although it degrades performance in all cases, this level of packet loss might go unnoticed in a data network because protocols such as TCP retransmit lost packets. In voice networks, however, this level of packet loss is unacceptable. Voice quality rapidly degrades in one direction. When voice quality problems are experienced, you must first check the duplex mismatches.

The best practice is to use autonegotiation on both sides of an IP connection. You can also lock down interfaces on both sides of a link. However, many a times, this practice requires a coordination between the Ethernet switch data team and the voice team. Gigabit links should *always* use Auto-Negotiation. For details of all aspects of Auto-Negotiation and lockdown, see the *Ethernet Link Guidelines for Avaya Aura Unified Communications Products* whitepaper at http://support.avaya.com/.

Whether you choose the autonegotiation mode or the lock down mode, make sure that both the ends of the link use the same mode which results in 100 Mbps and full duplex for 10/100 Mbps links. Also, ensure that Gigabit links result in 1 Gbps and full duplex in autonegotiation mode.

⚠ **Caution:**

Do not use the autonegotiation mode on one side of the IP connection and the lock down mode on the other side as this can result in a duplex mismatch and cause voice quality and signaling problems.

Virtual LANs

Virtual Local Area Networks (VLANs) are an often-misunderstood concept. This section defines VLANs and addresses configurations that require the Avaya IP telephone to connect to an Ethernet switch port that is configured for multiple VLANs. The IP telephone is on one VLAN, and a personal computer that is connected to the telephone is on a separate VLAN. Two sets of configurations are given: Cisco CatOS, and Cisco IOS.

VLAN defined

With simple Ethernet switches, the entire switch is one Layer 2 broadcast domain that usually equates to one IP subnetwork (Layer 3 broadcast domain). Consider a single VLAN on a VLAN capable Ethernet switch as being equivalent to a simple Ethernet switch. A VLAN is a logical

Layer 2 broadcast domain that typically equates to one IP subnetwork. Therefore, multiple VLANs are same as logically separated subnetworks. This arrangement is analogous to multiple switches being physically separated subnetworks. A Layer 3 routing process is required to route between VLANs. This routing process can take place on a connected router or a router module within a Layer 2/Layer 3 Ethernet switch. If no routing process is associated with a VLAN, devices on that VLAN can only communicate with other devices on the same VLAN.

Port or native VLAN

Port VLAN and native VLAN are synonymous terms. The IEEE 802.1Q standard and most vendor switches use the term *port VLAN*, but Cisco switches use the term *native VLAN*.

Every port has a port VLAN or a native VLAN. Unless otherwise configured, VLAN 1 is the default VLAN. It can be configured on a per-port basis or over a range of ports.

All untagged Ethernet frames (with no 802.1Q tag, for example, from a personal computer) are forwarded on the port VLAN or the native VLAN. This is true even if the Ethernet switch port is configured as an 802.1Q trunk or otherwise configured for multiple VLANs.

Trunk configuration

A trunk port on an Ethernet switch is one that is capable of forwarding Ethernet frames on multiple VLANs through the mechanism of VLAN tagging. IEEE 802.1Q specifies the standard method for VLAN tagging.

A trunk link is a connection between two devices across trunk ports. This connection can be between a router and a switch, between two switches, or between a switch and an IP telephone. Some form of trunking or forwarding multiple VLANs must be enabled to permit the IP telephone and the attached personal computer to appear on separate VLANs. The following commands enable VLAN trunking.

Table 6: Commands for VLAN trunking

Cisco IOS	Cisco CatOS
`switchport mode trunk` By default, all VLANs (1 to 4094) are enabled on the trunk port. Switches supporting ISL trunking have different commands for trunk setup. For more information, see the IOS manual.	`set trunk` *`<mod/port>`* `nonegotiate dot1q` By default, all VLANs (1 to1005) are enabled on the trunk port. VLANs can be selectively removed with the command `clear trunk` *`<mod/port> <vid>`*

Note that Cisco and other vendor switches can remove VLANs from a trunk port. This feature is highly desirable because only a maximum of two VLANs should appear on a trunk port that is connected to an IP telephone. That is, broadcasts from nonessential VLANs should not be permitted to bog down the link to the IP telephone. Cisco IOS switches can have an implicit trunk that contains only two VLANs, one for data and one for voice. You can configure an implicit trunk using the following commands:

- `switchport access vlan` *`<vlan-id>`*

- `switchport voice vlan <vlan-id>`

Trunking for one-X Communicator and other softphones

You can set the Layer 2 priority on a softphone (or physical phone) using IEEE-802.1p bits in the IEEE-802.1Q VLAN tag. This is useful if the telephone and the attached personal computer are on the same VLAN (same IP subnetwork), but the telephone traffic requires higher priority (Trunking for softphones or physical phones on page 100). Enable 802.1Q tagging on the IP phone, set the priorities as desired, and set the VID to zero. As per the IEEE standard, a VID of zero assigns the Ethernet frame to the port VLAN or the native VLAN.

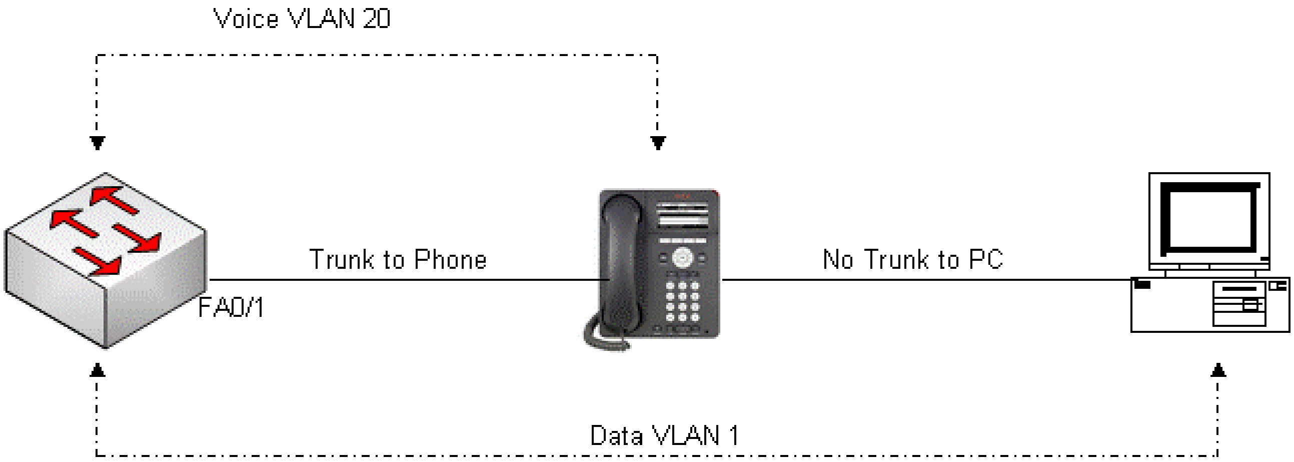


Figure 12: Trunking for softphones or physical phones

Cisco switches function differently in this scenario, depending on the hardware platforms and OS versions.

Note:

Setting a Layer 2 priority is useful only if QoS is enabled on the Ethernet switch. Otherwise, the priority-tagged frames are treated the same as clear frames.

WAN

Because of the high costs and lower bandwidths available, there are some fundamental differences in running IP telephony over a Wide Area Network (WAN) versus a LAN. As more problems occur in WAN environment, you must consider network optimizations and proper network design.

WAN QoS

In particular, Quality of Service (QoS) becomes more important in a WAN environment than in a LAN. In many cases, transitioning from the LAN to the WAN reduces bandwidth by approximately 99%. Because of this severe bandwidth crunch, strong queuing, buffering, and packet loss management techniques have been developed. Severe bandwidth crunch, strong queuing, buffering, and packet loss management techniques are covered in more detail in Quality of Service guidelines on page 114.

Recommendations for QoS

For both small and medium customers, a simple configuration is more effective than a complex configuration when implementing QoS for voice, data, signaling and video. If traffic engineering is done properly and sufficient bandwidth is available, especially for WAN links, voice and voice signaling traffic can both be tagged as DSCP 46. This Class of Service (CoS) tagging places both types of packets into the same High Priority queue with minimum of effort. The key is to have enough bandwidth to prevent any packets from dropping.

Large enterprises and multinational companies might find a stratified approach to CoS more beneficial. This approach allows maximum control for many data and voice services. For this environment, customers must use DSCP 46 (Expedited Forwarding) for voice (bearer), but voice signaling could have its own DSCP values and dedicated bandwidth. This would prevent traffic from contending with signaling. Although the configuration can be more complex to manage and administer, the granularity will give the best results and is regarded as a best practice.

For the routers, customers must use strict priority queuing for voice packets and weighted-fair queuing for data packets. Voice packets should always get priority over non-network-control data packets. This type of queuing is called Class-Based Queuing (CBQ) on Avaya data networking products or Low-Latency Queuing (LLQ) on Cisco routers.

Codec selection and compression

Because of the limited bandwidth available on the WAN, using a compression codec allows efficient use of resources without a significant decrease in voice quality. IP telephony implementations across a WAN must use the G.729 codec with 20 ms packets. This configuration uses 24 kbps (excluding Layer 2 overhead), 30% of the bandwidth of the G.711 uncompressed codec (80 kbps).

To conserve bandwidth, RTP header compression (cRTP) can be used on point-to-point links. cRTP reduces the IP/UDP/RTP overhead from 40 bytes to 4 bytes. With 20 ms packets, this translates to a savings of 14.4 kbps, making the total bandwidth required for G.729 approximately 9.6 kbps. The trade-off for cRTP is a higher CPU utilization on the router. The processing power of the router determines the amount of compressed RTP traffic that the router can handle. Avaya testing indicates that a typical small branch-office router can handle 768 kbps of compressed traffic. Larger routers can handle greater amounts. cRTP is available on several Avaya secure routers (1000–series, 2330, 3120, and 4134) and on the Extreme, Juniper, Cisco, and other vendor routers.

Serialization delay

Serialization delay refers to the delay that is associated with sending bits across a physical medium. Serialization delay is important to IP telephony because this delay can add significant jitter to voice packets, and impair voice quality.

Network design

Routing protocols and convergence

While designing an IP telephony network across a WAN, care should be taken when selecting a routing protocol or a dial-backup solution. Different routing protocols have different convergence times, which is the time that it takes to detect a failure and route around it. While a network is in the process of converging, all voice traffic is lost.

The selection of a routing protocol depends on several factors:

- If a network has a single path to other networks, static routes are sufficient.
- If multiple paths exist, is convergence time an issue? If yes, Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) are appropriate.
- Are open standards-based protocols required? If yes, OSPF and RIP are appropriate, but not EIGRP or IGRP, which are Cisco proprietary.

In general, you must use OSPF when routing protocols. OSPF allows relatively fast convergence and does not rely on proprietary networking equipment.

In many organizations, because of the expense of dedicated WAN circuits, dial-on-demand circuits are provisioned as backup if the primary link fails. The two principal technologies are ISDN (BRI) and analog modem. ISDN dial-up takes approximately 2 s to connect and offers 64 kbps to 128 kbps of bandwidth. Analog modems take approximately 60 s to connect and offer up to 56 kbps of bandwidth. If G.729 is used as the codec, either technology can support IP telephony traffic. If G.711 is used as the codec, only ISDN is appropriate. Also, because of the difference in connection time, ISDN is the preferred dial-on-demand technology for implementing IP telephony.

Multipath routing

Many routing protocols, such as OSPF, install multiple routes for a particular destination into a routing table. Many routers attempt to load-balance across the two paths. There are two methods for load balancing across multiple paths. The first method is per-packet load balancing, where each packet is serviced in a round-robin fashion across the two links. The second method is per-flow load balancing, where all packets in an identified flow (source and destination addresses and ports) take the same path. IP telephony does not operate well over per-packet load-balanced paths. This type of setup often leads to *choppy* quality voice. In situations with multiple active paths, you must use per-flow load balancing instead of per-packet load balancing.

Balancing loads per-flow

About this task

In the presence of multiple links, data can be balanced across them by a round-robin fashion for either packets or a stream (flow) of data. Real-time media like voice and video should use flow balancing only.

Frame relay

The nature of Frame Relay poses a challenge for IP telephony, as described in this section.

Overview of frame relay

Frame Relay service is composed of three elements: the physical access circuit, the Frame, Relay port, and the virtual circuit. The physical access circuit is usually a T1 or fractional T1 and is provided by the local exchange carrier (LEC) between the customer premise and the nearest central office (CO). The Frame Relay port is the physical access into the Frame Relay network, a port on the Frame Relay switch itself.

The access circuit rate and the Frame Relay port rate must match to eliminate the possibility of discarded packets during periods of congestion. The virtual circuit is a logical connection between Frame Relay ports that can be provided by the LEC for intra-lata Frame Relay or by the inter-exchange carrier (IXC) for inter-lata Frame Relay. The most common virtual circuit is a permanent virtual circuit (PVC), which is associated with a committed information rate (CIR). The PVC is identified at each end by a separate data-link connection identifier (DLCI) in Data-link connection identifiers over an interexchange carrier Frame Relay network on page 103.

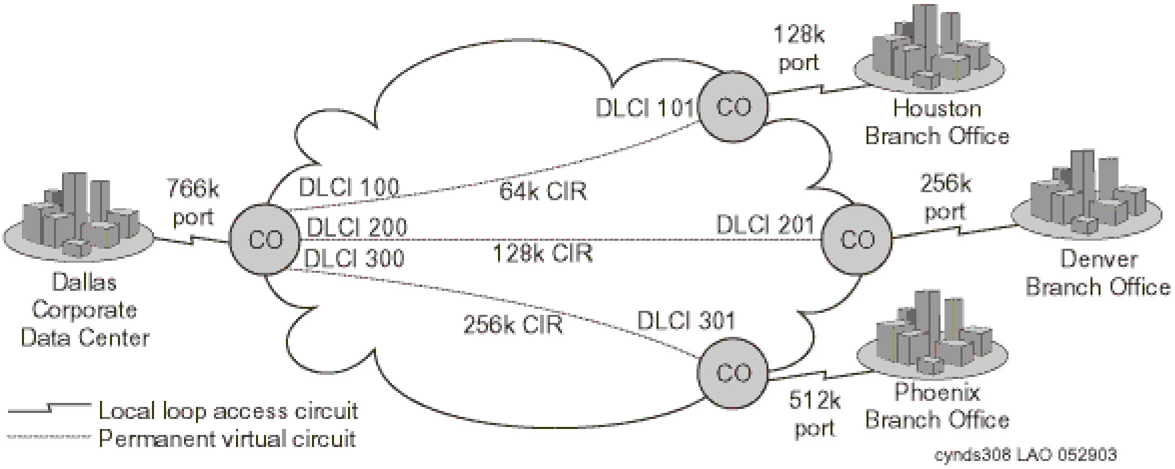


Figure 13: Data-link connection identifiers over an interexchange carrier Frame Relay network

This hypothetical implementation shows the Dallas corporate office connected to three branch offices in a common star topology (or hub and spoke). Each office connects to a LEC CO over a fractional T1 circuit, which terminates onto a Frame Relay port at the CO, and on to a Frame Relay capable router at the customer premise. The port rates and the access circuit rates match. PVCs are provisioned within the Frame Relay network between Dallas and each branch office. The CIR of each PVC is sized so that it is half the respective port rate, which is a common implementation. Each branch office is guaranteed its respective CIR, but it is also allowed to burst up to the port rate without any guarantees.

The port rate at Dallas is not quite double the aggregate CIR, but it does not need to be, because the expectation is that not all three branch offices will burst up to the maximum at the same time. In an implementation like this, the service is probably negotiated through a single vendor. But it is likely that Dallas and Houston are serviced by the same LEC, and that the Frame Relay is intra-lata, even if the service was negotiated through an IXC, such as AT&T or Sprint. The service between Dallas and the other two branch offices, however, is most likely inter-lata.

A frame relay issue and alternatives

The obstacle in running IP telephony over Frame Relay involves the treatment of traffic within and outside the CIR, commonly termed the burst range.

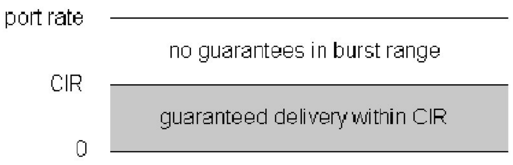


Figure 14: Committed information rate (burst range)

As Committed information rate (burst range) on page 103 shows, traffic up to the CIR is guaranteed, whereas traffic beyond the CIR usually is not. This is how Frame Relay is intended to work. CIR is a committed and reliable rate, whereas burst is a bonus when network conditions permit it without infringing upon the CIR of any user. For this reason, burst frames are marked as discard eligible (DE) and are queued or discarded when network congestion exists. Although customers can achieve significant burst throughput, burst throughput is unreliable, unpredictable, and not suitable for real-time applications like IP telephony.

Therefore, the objective is to prevent voice traffic from entering the burst range and being marked DE. One way to accomplish this is to prohibit bursting by shaping the traffic to the CIR and setting the excess burst size (B_e – determines the burst range) to zero. However, this also prevents data traffic from using the burst range.

Additional frame relay information

Most IXCs convert the long-haul delivery of Frame Relay into ATM, that is, the Frame Relay PVC is converted to an ATM PVC at the first Frame Relay switch after leaving the customer premises. It is not converted back to Frame Relay until the last Frame Relay switch before entering the customer premise. This is significant because ATM has built-in Class of Service (CoS). A customer can enter a contract with a carrier to convert the Frame Relay PVC into a constant bit rate (CBR) ATM PVC. ATM CBR cells are delivered with lower latency and higher reliability.

Finally, under the best circumstances, Frame Relay is still inherently more susceptible to delay than ATM or TDM. Therefore, after applying the best possible queuing mechanism, you can still expect a longer delay over Frame Relay than over ATM or TDM.

Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) VPN service from service providers is commonly used by enterprises for WAN connectivity. The service is often available over different types of access links and usually offers multiple classes of service. The MPLS service generally provides good QoS and therefore, satisfies VoIP requirements. However, this service often depends on the Service Layer Agreement (SLA) and the actual quality delivered by the service provider.

With MPLS service, unlike private WAN, the enterprise controls QoS explicitly only on the access link, that is, on the connection from each enterprise site to the MPLS network. In the MPLS network, QoS is controlled by the service provider. The enterprise affects the service given to its traffic by assigning the traffic to appropriate classes of service in the service provider’s network. This is done with DiffServ Code Point (DSCP) marking in the packet’s IP header. DSCP remarking by the enterprise edge routers might be required. DSCP remarking includes mapping the DSCPs of enterprise traffic to the DSCP values designated by the MPLS service provider for the different classes of service in their service offering.

VPN overview

VPNs refer to encrypted tunnels that carry packetized data between remote sites. VPNs can use private lines or use the Internet through one or more Internet Service Providers (ISPs). VPNs are implemented in both dedicated hardware and software but can also be integrated as an application to existing hardware and software packages. A common example of an integrated package is a firewall product that can provide a barrier against unauthorized intrusion as well as perform the security features that are needed for a VPN session.

The encryption process can take from less than 1 ms to 1 s or more, at each end. VPNs can represent a significant source of delay and therefore, have a negative impact on voice performance. Also, because most VPN traffic runs over the Internet and there is little control over QoS parameters for traffic crossing the Internet, voice quality might suffer due to excessive packet loss, delay, and jitter. You can negotiate a service-level agreement with the VPN provider to guarantee an acceptable level of service. Before implementing IP telephony with a VPN, you should test their VPN network over time to ensure that it consistently meets the Avaya requirements.

Convergence advantages

For an increasing numbers of enterprises, VPN carries both data and voice communications. Though voice communication over IP networks (IP telephony) creates new quality of service (QoS) and other challenges for network managers, there are compelling reasons for moving forward with convergence over maintaining a traditional voice and data infrastructure:

- A converged infrastructure makes it easier to deploy eBusiness applications such as customer care applications that integrate voice, data, and video.
- Enterprises can reduce network costs by combining disparate network infrastructures and eliminating duplicate facilities.
- A converged infrastructure can increase the efficiencies of the IT organization.
- Long distance charges can be reduced by sending voice over IP networks.

Voice over IP VPN is emerging as a viable way to achieve these advantages. The emergence of public and virtual private IP services promises to make it easier for customers, suppliers, and businesses to use data networks to carry voice services. As with any powerful new technology, however, VPNs require skilled management to achieve top performance. The highest network performance becomes imperative when the VPN network must deliver high-quality voice communication. Not all IP networks can meet these quality requirements today. For instance, the public Internet is a transport option for voice communication only when reduced voice performance is acceptable and global reach has the highest priority. When high voice quality is a requirement, ISPs and Network Service Providers (NSPs) can provide other VPN connections that meet the required Service Level Agreements (SLAs).

Managing IP telephony VPN issues

This section provides information on communications security, firewall technologies, and Network Management as related to VPN issues.

Communication security

The public nature of the Internet, its reach, and its shared infrastructure provide cost savings when compared to leased lines and private network solutions. However, those factors also contribute to make Internet access a security risk. To reduce these risks, network administrators must use the appropriate security measures.

A managed service can be implemented either as a premises-based solution or a network-based VPN service. A premises-based solution includes customer premises equipment (CPE) that allows end-to-end security and Service Level Agreements (SLAs) that include the local loop. These end-to-end guarantees of quality are key differentiators. A network-based VPN, on the other hand, is provisioned mainly by equipment at the service provider's point-of-presence (PoP), so it does not provide equivalent guarantees over the last mile. For a secure VPN that delivers robust, end-to-end SLAs, an enterprise must demand a premises-based solution that is built on an integrated family of secure VPN platforms.

The *private* in virtual private networking is also a matter of separating and insulating the traffic of each customer so that other parties cannot compromise the confidentiality or the integrity of data. IPSec tunneling and data encryption achieves this insulation by essentially carving private end-to-end pipes or *tunnels* out of the public bandwidth of the Internet and then encrypting the information within those tunnels to protect against wrongful access. In addition to IPSec, there are two standards for establishing tunnels at Layer 2: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP). Neither PPTP nor L2TP include the encryption capabilities of IPSec. The value of IPSec beyond these solutions is that IPSec operates at IP Layer 3. IPSec at IP Layer 3 allows for native, end-to-end secure tunneling. As an IP-layer service, IPSec is also more scalable than the connection-oriented Layer 2 mechanisms.

Also, note that IPSec can be used with either L2TP or PPTP, since IPSec encrypts the payload that contains the L2TP/PPTP data. IPSec provides a highly robust architecture for secure wide-area VPN and remote dial-in services. IPSec is complementary to any underlying Layer 2 network architecture. With its addition of security services that can protect the VPN of a company, IPSec marks the clear transition from early tunneling to full-fledged Internet VPN services.

However, different implementations of IPSec confer varying degrees of security services. Products must be compliant with the latest IPSec drafts, must support high-performance encryption, and must scale to VPNs of industrial size.

A VPN platform should support a robust system for authentication of the identity of end users based on industry standard approaches and protocols.

Firewall technologies

To reduce security risks, appropriate network access policies should be defined as part of business strategy. Firewalls can be used to enforce such policies. A firewall is a network interconnection element that polices traffic flows between internal or protected networks and external or public networks such as the Internet. Firewalls can also be used to segment internal networks.

The application of firewall technologies only represents a portion of an overall security strategy. Firewall solutions do not guarantee 100% security by themselves. These technologies must be complemented with other security measures, such as user authentication and encryption, to achieve a complete solution.

The three technologies that are most commonly used in firewall products are packet filtering, proxy servers, and hybrid. These technologies operate at different levels of detail and provide varying degrees of network access protection. Therefore, these technologies are not mutually exclusive. A firewall product might implement several such technologies simultaneously.

Network Management and outsourcing models

While enterprises acknowledge the critical role that the Internet and IP VPNs can play in their strategic eBusiness initiatives, they face a range of choices for implementing their VPNs. The options range from enterprise-based or do-it-yourself VPNs that are fully built, owned, and operated by the enterprise to VPNs that are fully outsourced to a carrier or other partner. In the near term, enterprise-operated and managed VPN services are expected to hover around a 50/50 split, including hybrid approaches.

Increasingly, enterprises are assessing their VPN implementation options across a spectrum of enterprise-based, carrier-based/outsourced, or hybrid models. Each approach offers a unique business advantage.

- Enterprise based

  This option operates over a public network facility, most commonly, the Internet, using equipment that is owned and operated by the enterprise. The benefit of the enterprise-based option is the degree of flexibility and control this option offers over VPN deployment, administration, and adaptability or change.

- Fully outsourced

  This managed service can be implemented by a collection of partners, including an ISP and a security integration partner. The advantages of the fully outsourced option include quick deployment, easy global scalability, and freedom from overhead Network Management.

- Shared management

  With this hybrid approach, a partner can take responsibility for major elements of infrastructure deployment and management, but the enterprise retains control over key aspects of policy definition and security management.

Conclusion

Moving to a multipurpose packet-based VPN that transports both voice and data with high quality poses a number of significant management challenges. Managers must determine whether to operate the network using an enterprise-based model, an outsourced or carrier-based model, or a hybrid model. They must settle security issues that involve several layers of the network. And they must ensure that they and their vendors can achieve the required QoS levels across these complex networks. Yet, the advantages of converged, multipurpose VPNs remain a strong attraction. The opportunity to eliminate separate, duplicate networks and costly dedicated facilities, minimize costly public network long distance charges, and reduce administrative overhead provides a powerful incentive. Most important, by helping integrate voice and data communication, multimedia Messaging, supplier and customer relationship management, corporate data stores, and other technologies and resources, converged networks promise to become a key enabler for eBusiness initiatives.

NAT overview

IP telephony cannot work across Network Address Translation (NAT) because if private IP addresses (RFC-1918) are exchanged in signaling messages, these addresses are not reachable from the public side of the NAT and cannot be used for the media sessions.

The problem is not encountered in all VoIP scenarios. It is not used for VPN-based remote access, and NATs are usually not needed internally within the enterprise network. VoIP has to traverse NAT usually at the border between the enterprise and a VoIP trunk to a service provider as well as in hosted VoIP service.

If the network design includes a firewall within the enterprise network to protect certain servers or some part of the network so that IP telephony traffic has to traverse the internal firewall, then the firewall should not perform a NAT function. IP telephony will then work across the firewall once the appropriate ports are open on the firewall. For information on the list of needed ports for any Avaya product, go to the Avaya Support website at https://support.avaya.com to refer current documentation and knowledge articles related to opening a service request.

When you connect the enterprise to an IPT SP through a VoIP trunk, either SIP or H.323, a NAT is done at the enterprise border. The solution for this scenario is to deploy a Session Border Controller (SBC) near the NAT, for example, in the enterprise DMZ. SBCs from multiple vendors have been tested for interoperability with Avaya's IP telephony solutions.

Alternatively, in certain cases, you can use an Application Layer Gateway (ALG).

Solutions based on standards such as ICE and STUN are expected to be supported in some NAT traversal scenarios.

Converged network design

Converged networks require the application of good management and control practices to support and sustain the deployment of IP telephony. The first step in implementing an IP telephony system is making the commitment to provide a network capable of supporting a real time application such as voice.

Design and management

Highly available networks have to be planned and maintained. The probability of success for these activities is improved by the application of three fundamental principles: Simplicity, Manageability and Scalability.

To deploy a business-critical IP-based service, the network upon which the IP runs must be:

- Easy to configure
- Easy to monitor and troubleshoot
- Extensible with minimum reconfiguration, that is, designed with enough resources to grow with the business the IP supports

Design for simplicity

IT staff must interact with the network and therefore, if the system is difficult to understand, the probability of error increases. You must reduce the number of protocols and services on any network segment and reduce the number of decisions the network must make. Simple, documentable, reproducible, and verifiable configurations are a must for IP telephony deployment. The IT staff responsible for the network must understand how the network works. New staff is easy to train on a simple network. A conscious choice to favor simplicity in design might be the single biggest factor in improving uptime due to its cascading effect on process, documentation and verification.

Design for manageability

Studies of operator errors have identified several classes of errors typical of network service administrators. Most of these are the result of misconfiguration of new components and unintended actions such as restarts or disabling of hardware while diagnosing problems. Significantly, operators of all experience levels were found to introduce almost all classes of errors with roughly equal frequency.

Research conducted at Rutgers University [6] found that operator action-verification techniques allowed detection and prevention of over half of the errors typically introduced by operators. This data strongly argues for the implementation of reliable change control procedures and change verification as requisites for highly available networks. To support these activities, management tools must be in place to aid in detecting and reporting errors, both for validation of operator actions and diagnosing problems. Network documentation is typically inaccurate and outdated [7] (due in part to lack of change control) so management capabilities to verify configurations are essential.

Design for scalability

Other researchers have proposed mechanisms for reducing or eliminating the need for operator interaction by automating common tasks. The success of these approaches argues that reducing the scope of changes required to manage and expand network services will pay dividends in network uptime. Excess bandwidth, unused ports and available addresses are required to verify changes and to simplify network expansion. Expansion should begin well before these resources are exhausted.

Using designs that limit the impact of changes reduces the potential for errors. For example, if the administrator needs to change both an aggregation switch and a router configuration to accommodate new media gateway interfaces, the design doubles the opportunity for a configuration error. If a new subnet needs to be added to Access Control Lists throughout the network core, the potential for outage is expanded further.

The same principles used to reduce software complexity and improve software reliability are applicable to the network complexity problem. Modularity, design reuse, and testability are all attributes of highly reliable networks.

Topologies

The network topology recommended consists of a redundant core with building blocks of layered routers and switches as shown in Figure 15: Typical network topology design on page 110. This is the defacto standard for network design supporting both modularity and reuse.

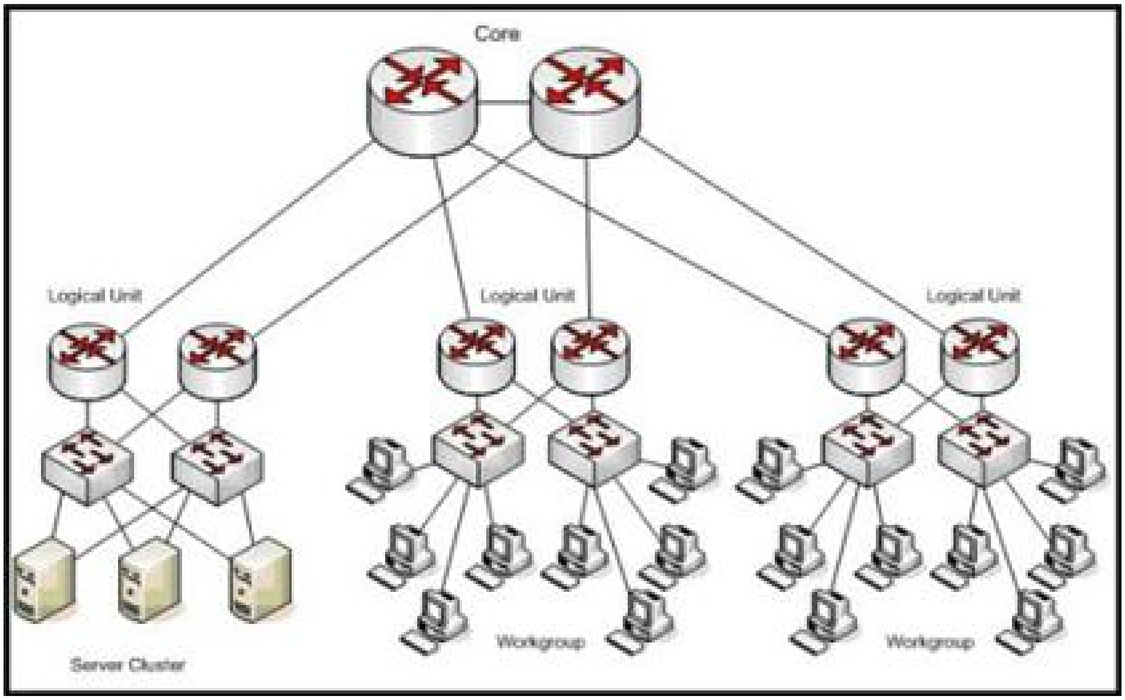


Figure 15: Typical network topology design

Real networks are far more complex with many more nodes and services. In addition, real deployments typically have legacy constraints, multiple sites, and heterogeneous equipment. It is beyond the scope of this document to detail solutions for the potential configurations of entire networks. To address those issues, Avaya provides a full range of service offers from assessment to outsourced management. For more information regarding these services, see the Avaya Web site at https://support.avaya.com.

Layers

There is a separate Layer 2 access level when the devices at the Layer 3 distribution layer are capable of Layer 2 switching. The access layer reduces the complexity of the network block by separating the functions of the devices and provides scalability when more ports are required as the network grows. To ensure network modularity, the routers serving this cluster should be dedicated to the cluster and sized to the task. Simplification argues for the reduction of subnets and routed interfaces in the cluster since the service is common. If multiple server clusters are implemented across the network, using a single subnet within the cluster simplifies the configuration of the entire network. The addition of static subnets in the direction of the cluster increases the configuration complexity with little benefit in terms of availability unless the subnets terminate on different routers, which in turn implies separate modular clusters. A separate management subnet is created but is unrelated to the service address configuration. Separate subnets simplify diagnostic activities, but this benefit is achievable with address partitioning within the subnet. Port densities for smaller full featured routers can be inadequate to scale to the connectivity requirements of even this small cluster when the extra ports for management, troubleshooting, and testing are considered.

An alternative design uses the smaller high density integrated switching and routing platforms that are becoming popular as routing functions have moved into commodity Application-Specific Integrated Circuits (ASIC).

When selecting this type of configuration, bandwidth and inter-switch traffic capacity must be considered. In a load balanced configuration under fault conditions, approximately half the call load can travel on the inter-switch link. The inter-switch link must be redundant to prevent a single failure from causing a bifurcated network, and if a Link Aggregation Group (LAG) is used to eliminate potential spanning tree loops, the individual link bandwidth must still be capable of supporting the required traffic.

Redundancy

Hardware redundancy is a proven and well defined tool for increasing the availability of a system. Avaya Critical Availability solutions has employed the symmetric (active-active) technique to achieve 99.999% availability. Consider the symmetric (active-active) configuration for deployment of redundant hardware.

Because two G450 media gateways do not share the same TDM bus, redundancy is achieved only for the media server features and not for the media gateway features. The configuration of redundancy for media server is symmetric (active/active).

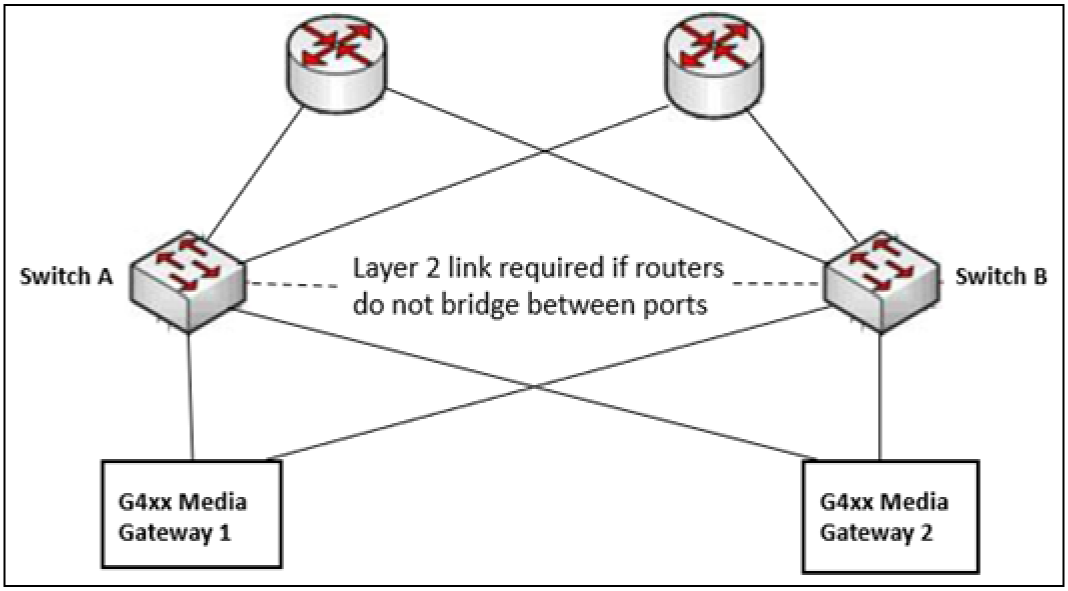

Switch A
Layer 2 link required if routers do not bridge between ports
Switch B
G4xx Media Gateway 1
G4xx Media Gateway 2

Figure 16: Redundant connections

It is a good practice to connect each media gateway to redundant Layer 2 switches as shown in the figure to protect each media gateway from failure of the Layer 2 switch itself.

Layer 2

Layer 2 configuration of the switches supporting the cluster should use IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) to prevent loops and for selection between redundant links. Most modern switches implement this protocol. The G4xx media gateway supports RSTP. Selecting a device for Layer 2 access that does not support RSTP should be very carefully considered since those devices are likely to be obsolete and lacking in other highly desirable features in areas such as Quality of Service, security, and manageability. RSTP is also preferred over most alternative solutions that are typically not standards based and can cause problems with interoperability, scalability and configuration complexity. The selected redundancy protocol must be well understood by the IT staff responsible for maintaining the network.

It is good policy to enable RSTP on all ports of the Layer 2 switches, including the ports directly connected to hosts. Misconfiguration and human error are more likely to occur than link failure and the added protection of loop avoidance is worth the minimal overhead. This possibility is an additional argument in favor of using RSTP as a redundancy protocol since other solutions cannot be uniformly applicable to the subnet.

With modular configuration, the spanning tree is kept simple and deterministic. Consider the sample spanning tree configuration in Figure 17: Sample spanning tree on page 112. The topology has been redrawn and the host connections have been removed to simplify the explanation. Assume the bridge priorities are assigned such that the VRRP primary router has the highest priority, the secondary router is next, Switch 1 is third, and Switch 2 is last. It is also important that the bandwidth of all links be equivalent and adequate to handle the aggregated traffic.

In Figure 17: Sample spanning tree on page 112, links A and B are directly attached to the root bridge so links A and B will be in forwarding mode. Link C connects to a higher priority bridge than link D, so link D will be disabled and Switch 1 will be the designated root for the secondary router. In this configuration, traffic from the attached devices flows directly to the primary router on links A and B.

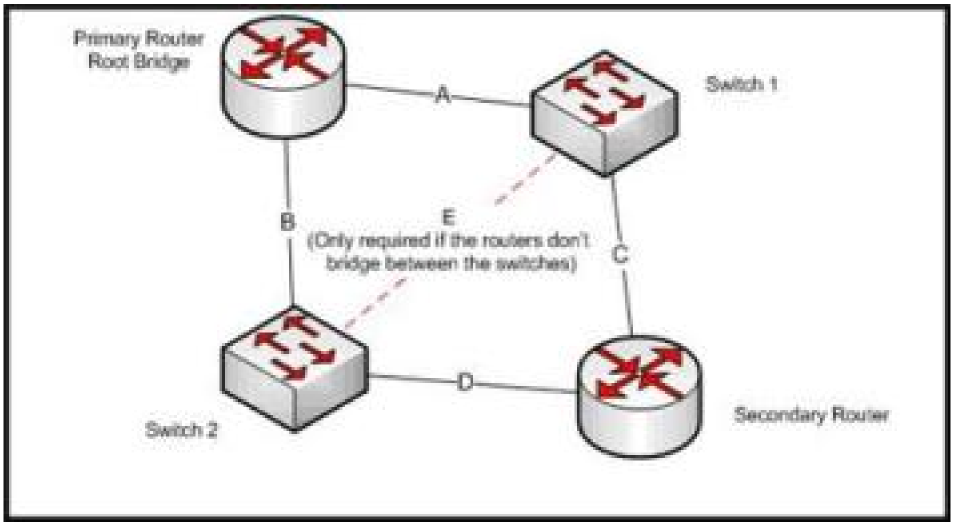

Primary Router
Root Bridge
A
Switch 1
B
E
(Only required if the routers don't bridge between the switches)
C
D
Switch 2
Secondary Router

Figure 17: Sample spanning tree

If the primary router fails, the secondary router becomes both the active router and the root bridge, and traffic from the switches flows on the reconfigured spanning tree along links C and D. If bridge priorities are not managed, traffic from one switch can be directed through the secondary router and the other switch as normal operation.

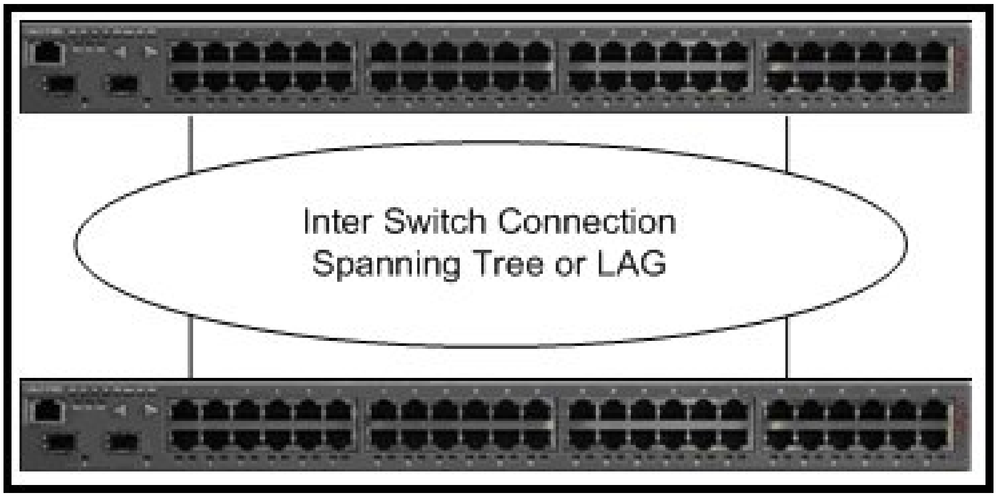


Figure 18: Alternate configuration - Layer 2

In the alternate integrated device configuration, bridge priority is less significant but other factors such as link sizing becomes an issue if there are not enough Gigabit Ethernet aggregation ports. If a link aggregation group (LAG) is used, flow distributions must be understood to ensure correct behavior.

Layer 3

The symmetric or asymmetric question is linked to the configuration of redundancy for the routers serving this cluster. If the single subnet model is used, the router configuration in the direction of the cluster also follows the asymmetric model. Virtual Router Redundancy (VRRP) is configured with one router as the primary and the other router as the secondary. If multiple subnets are configured, it is common practice to make one router the primary for some of the subnets and the other router as the primary for the rest. Note that VRRP should be configured with a failover latency greater than the latency required for the Layer 2 loop avoidance protocol to prevent LAN failures from disturbing the wider network. Typical defaults are between two and three seconds, which should be enough to prevent LAN failures in a simple well configured spanning tree.

The cluster subnet is exported to OSPF through the interfaces to the core so that the devices are reachable, but OSPF needs to know which router interface to use for the packets directed to the cluster. For proper operation, the link to the primary router must be the preferred OSPF path. If the primary router fails but the link to the core is still operational, packets do not reach the cluster until the neighbor adjacency times out. Making these timeouts too small makes the protocol overly sensitive and may still provide inadequate results.

The probability of a VRRP interchange that occurs asymmetrically is arguably lower than a router failure that leaves the physical link state unchanged. Some implementations address this by allowing the link state of different interfaces to be coupled. These techniques are also applicable to the OSPF solution but are typically proprietary. Combining the link state of different interfaces with the decoupling route core disruption from local failure are arguments for this configuration.

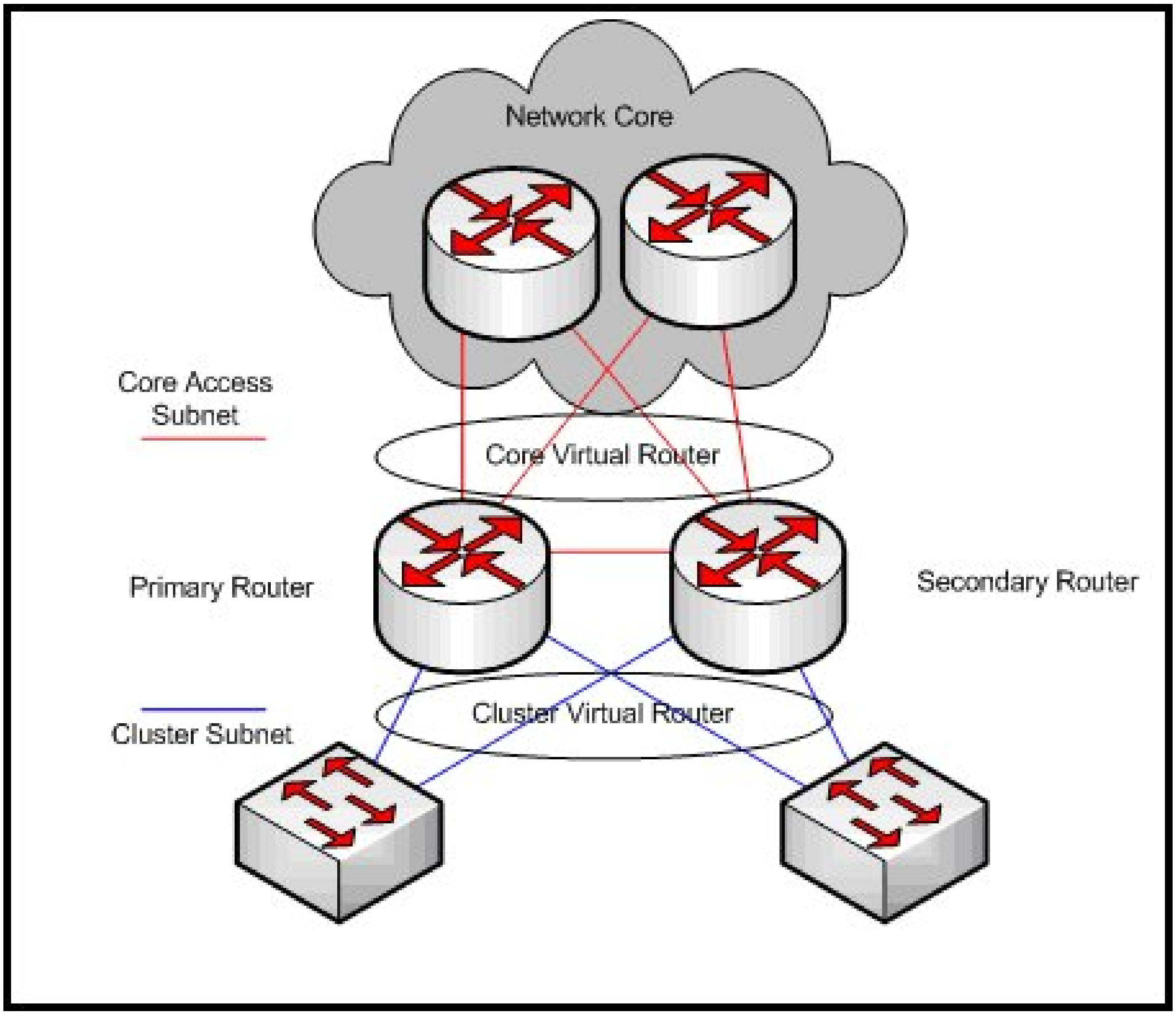


Figure 19: VRRP configured for Core Access

QoS guidelines

This section contains guidelines for deploying Quality of Service (QoS) for an IP Telephony network.

Class of Service refers to mechanisms that tags traffic in such a way that the traffic can be differentiated and segregated into various classes. *Quality of Service* refers to what the network does to the tagged traffic to give higher priority to specific classes. If an endpoint tags its traffic with Layer 2 802.1p priority 6 and Layer 3 Differentiated Services Code Point (DSCP) 46, for example, the Ethernet switch must be configured to give priority to value 6, and the router must be configured to give priority to DSCP 46. The fact that certain traffic is tagged with the intent to give it higher priority does not necessarily mean it will receive higher priority. CoS tagging is ineffective without the supporting QoS mechanisms in the network devices.

CoS overview

IEEE 802.1p/Q at the Ethernet layer (Layer 2) and DSCP at the IP layer (Layer 3) are two standards-based CoS mechanisms that are used by Avaya products. These mechanisms are supported by the IP telephone, procr, G4xx media gateways, and Avaya Aura® Media Server. Although TCP/UDP source and destination ports are not CoS mechanisms, they can be used to identify specific traffic and can be used much like CoS tags. Another non-CoS methods to identify specific traffic is to key in on source and destination IP addresses and specific protocols, such as RTP. The Media Processor circuit pack and IP telephones use RTP to encapsulate audio.

Because of this format change, older switches had to be explicitly configured to accept 802.1Q tagged frames. Otherwise, the switches reject the tagged frames. However, this problem has not been significant during the last few years.

The two fields to be concerned with are the Priority and Vlan ID (VID) fields. The Priority field is the *p* in 802.1p/Q, and ranges from 0 to 7. *802.1p/Q* is a common term used to indicate that the Priority field in the 802.1Q tag has significance. Prior to real-time applications, 802.1Q was used primarily for VLAN trunking, and the Priority field was not important. The VID field is used to indicate the VLAN to which the Ethernet frame belongs.

The IP header with its 8-bit Type of Service (ToS) field was originally used and is still used in some cases. This original scheme was not widely used, and the IETF developed a new Layer 3 CoS tagging method for IP called Differentiated Services (DiffServ, RFC 2474/2475). DiffServ uses the first 6 bits of the ToS field and ranges in value from 0 to 63. Comparison of DSCP with original ToS on page 115 shows the original ToS scheme and DSCP in relation to the 8 bits of the ToS field.

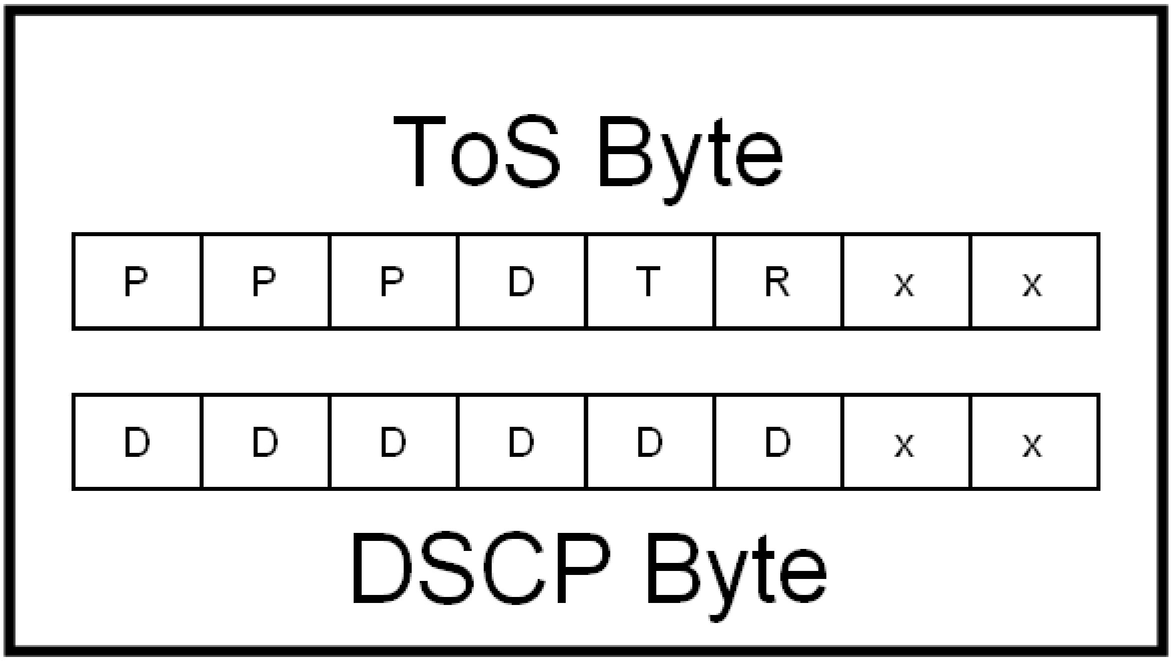


Figure 20: Comparison of DSCP with original ToS

Ideally, any DSCP value should map directly to a precedence and traffic parameter combination of the original scheme. However, this mapping does not exist in all cases and might cause problems on some older devices.

On any device, new or old, a nonzero value in the ToS field has no effect if the device is not configured to examine the ToS field. Problems arise on some legacy devices when the ToS field is examined, either by default or by enabling QoS. These legacy devices (network and endpoint) might contain code that implemented only the precedence portion of the original ToS scheme, with the remaining bits defaulted to zeros. This means that only DSCP values that are divisible by 8 (XXX000) can map to the original ToS scheme. For example, if an endpoint is tagging with DSCP 40, a legacy network device can be configured to look for precedence 5, because both values show up as 10100000 in the ToS field. However, a DSCP of 46 (101110) cannot be mapped to any precedence value alone. Another problem arises if the existing code implemented precedence with only one traffic parameter permitted to be set high. In this case, a DSCP of 46 still does not work, because it requires 2 traffic parameter bits to be set high. When these mismatches occur, an older device, about 10 years older, might reject the DSCP tagged IP packet or exhibit some other abnormal behavior. Most newer devices support both DSCP and the original ToS scheme.

Layer 2 quality of service

On Cisco and other vendor switches, IP telephony traffic can be assigned to higher priority queues. The number, sizes, and functioning of the queues is device dependent and beyond the scope of this document.

However, a fixed number of queues exist, and the queues are usually not configurable. Older or lower end switches have only two queues or none. Newer or higher-end switches commonly have four or eight queues, with eight being the maximum because there are only eight Layer 2 priority levels. When configured, the Ethernet switch can identify the high-priority traffic by the 802.1p/Q tag and assign that traffic to a high-priority queue. On some switches, a specific port can be designated as a high-priority port, which causes all traffic that originates from that port to be assigned to a high-priority queue.

Layer 3 quality of service

Implementing QoS on a router is more complicated than on an Ethernet switch. Unlike Ethernet switches, routers do not just have a fixed number of queues. Instead, routers have various queuing mechanisms. For example, Cisco routers have standard first-in first-out queuing (FIFO), weighted fair queuing (WFQ), custom queuing (CQ), priority queuing (PQ), and low-latency queuing (LLQ). LLQ is a combination of priority queuing and class-based weighted fair queuing (CBWFQ), and it is the preferred queuing mechanism of Cisco for real-time applications such as IP telephony. Each queuing mechanism behaves differently, is configured differently, and has its own set of queues.

First, the desired traffic must be identified using IEEE-802.1p/Q, DSCP, IP address, TCP/UDP port, or protocol. Then the traffic must be assigned to a queue in one of the queuing mechanisms. Then the queuing mechanism must be applied to an interface.

The interface itself might also require additional modifications, independent of the queuing mechanism, to make QoS work properly. For example, Cisco requires traffic shaping on Frame

Relay and ATM links to help ensure that voice traffic is allotted the committed or guaranteed bandwidth. Cisco also prefers link fragmentation and interleaving (LFI) on WAN links below 768 kbps to reduce serialization delay. Serialization delay is the delay that is incurred in encapsulating a packet and transmitting the packet out of the serial interface. Serialization delay increases with packet size but decreases with WAN link size. The concern is that large low-priority packets induce additional delay and jitter, even with QoS enabled. This is overcome by fragmenting the large low-priority packets and interleaving them with the small high-priority packets, reducing the wait time for the high-priority packets. Serialization delay matrix on page 117 lists serialization delay for a variety of packet sizes and line speeds. The formula for determining serialization delay is:

serialization delay = Packet size in bits/Line speed

Table 7: Serialization delay matrix

WAN line speed	Packet size					
	64 bytes	**128 bytes**	**256 bytes**	**512 bytes**	**1024 bytes**	**1500 bytes**
56 kbps	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbps	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 kbps	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 kbps	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
512 kbps	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 kbps	640 µs	1.28 ms	2.56 ms	5.12 ms	10.24 ms	15 ms

Because of all these configuration variables, proper implementation of QoS on a router is an important task. However, QoS is needed most on the router because most WAN circuits terminate on routers.

QoS guidelines

There is no all-inclusive rule regarding the implementation of QoS because all networks and their traffic characteristics are unique. A good practice is to baseline the IP telephony response on a network without QoS and then apply QoS as necessary. Avaya Professional Services (APS) can help with baselining services. Conversely, enabling multiple QoS features simultaneously without knowing the effects of respective features is a bad practice.

For newer network equipment, best practices involve enabling Layer 3 (DiffServ) QoS on WAN links traversed by voice. Tag voice and data with DiffServ Code Point 46 (Expedited Forwarding), and set up a strict priority queue for voice. If voice quality is still not acceptable, or if QoS is desired for contingencies such as unexpected traffic storms, QoS can then be implemented on the LAN segments as necessary.

⚠ **Caution:**

> There is one caution to keep in mind about QoS with regard to the processor load on network devices.

Simple routing and switching technologies have been around for many years and have advanced significantly. Packet forwarding at Layer 2 and Layer 3 is commonly done in hardware. Cisco calls this fast switching, with switching being used as a generic term here, without heavy processor intervention. When selection criteria such as QoS and other policies are added to the routing and switching process, it inherently requires more processing resources from the network device. Many new devices can handle this additional processing in hardware and maintain speed without a significant processor burden. However, to implement QoS, some devices must move a hardware process to software. Cisco calls this *process switching*. Process switching not only reduces the speed of packet forwarding, but it also adds a processor penalty that can be significant. Processor penalty can result in an overall performance degradation from the network device and even device failure. You must examine each network device individually to determine if enabling QoS will reduce its overall effectiveness by moving a hardware function to software or for any other reason. Since most QoS policies are implemented on WAN links, the following points increase the effectiveness of QoS remains:

- Hardware platforms such as the 2600, 3600, 7200, 7500 series, or later are required. Newer platforms such as the 1800, 2800 and 3800 series can handle QoS well because of powerful processors.
- Newer interface modules such as WIC, and VIP are required.

  Note:

  If you are using Cisco devices with the interfaces such as WIC, and VIP, you must consult Cisco to determine which hardware revision is required for any given module.
- Sufficient memory is required: device dependent.
- Recommended IOS 12.0 or later.

Examine the following when you enable QoS on a network device.

- First, the network administrator should examine the processor load on the device and compare the load to the levels before QoS was enabled. The levels are likely to have gone up but the increase might not be significant. If it is, then it is likely that the QoS process is being done by software.
- Also, the processor load must remain at a manageable level (50% average, 80% peak). If the processor load is manageable, then the IP telephony response, for example, voice quality should be checked to verify that it has improved under stressed conditions, for example, high congestion. If the IP telephony response has improved, the other applications should be checked to verify that their performances have not degraded to unacceptable levels.

IEEE 802.1Q standard

Surprisingly, many data network engineers are still not familiar with CoS/QoS. Data networks were not designed for real-time protocols and this section helps the engineers to understand the protocols.

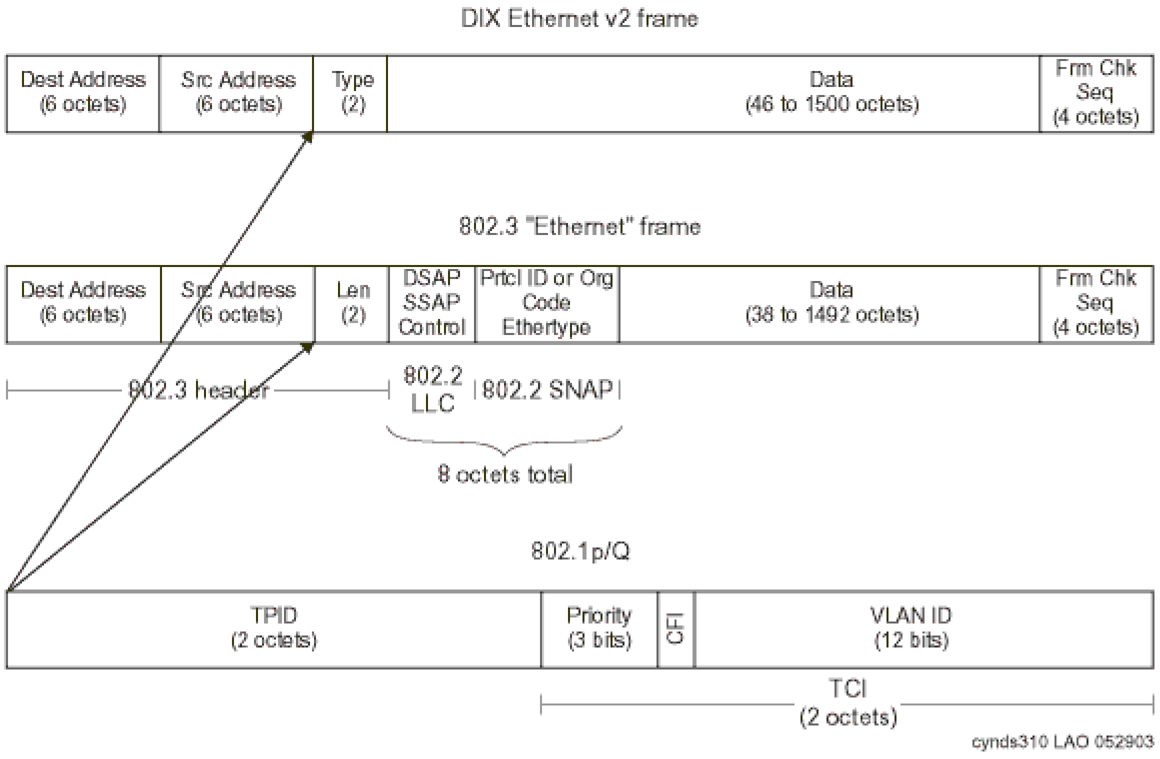


Figure 21: 802.1Q tag

The IEEE 802.1Q standard is a Layer 2 tagging method that adds four bytes to the Layer 2 Ethernet header. IEEE 802.1Q defines the open standard for VLAN tagging. Two bytes house 12 bits that are used to tag each frame with a VLAN identification number. The IEEE 802.1p standard uses three of the remaining bits in the 802.1Q header to assign one of eight different classes of service. Communication Manager users can add the 802.1Q bytes and set the priority bits as desired. *Avaya suggests that a priority of 6 be used for both voice and signaling* for simplicity. However, the default values are: 5-Video, 6-Voice, and 7-Control. IEEE 802.1p and IEEE 802.1Q are OSI layer 2 solutions and work on frames.

Because 802.1Q is a Layer 2 (Ethernet) standard, it only applies to the Ethernet header. At every Layer 3 boundary (router hop), the Layer 2 header, including CoS parameters, is stripped and replaced with a new header for the next link. Therefore, 802.1Q does not enable end-to-end QoS.

Recommendations for end-to-end QoS

You can use DiffServ on page 120 when end-to-end QoS is desired.. Modern routers can map DiffServ Code Points (DSCP) to 802.1p priority values, so 802.1p tags can be recreated on each Ethernet link.

IEEE 802.1p states a standard according to which these bits are used for CoS. The precedence is listed in IEEE 802.1 precedence and service mapping on page 120.

Table 8: IEEE 802.1 precedence and service mapping

User priority	Service mapping
000	Default, assumed to be best effort
001	Reserved, less than best effort
010	Reserved
011	Reserved
100	Delay sensitive, no bound
101	Delay sensitive, 100 ms bound
110	Delay sensitive, 10 ms bound
111	Network control

Differentiated services

The Differentiated Services (DiffServ) prioritization scheme redefines the existing ToS byte in the IP header (Differentiated Services (DiffServ) ToS byte on page 120) by combining the first 6 bits into 64 possible combinations. The ToS byte can be used by Communication Manager, IP telephones, and other network elements such as routers and switches in the LAN and WAN.

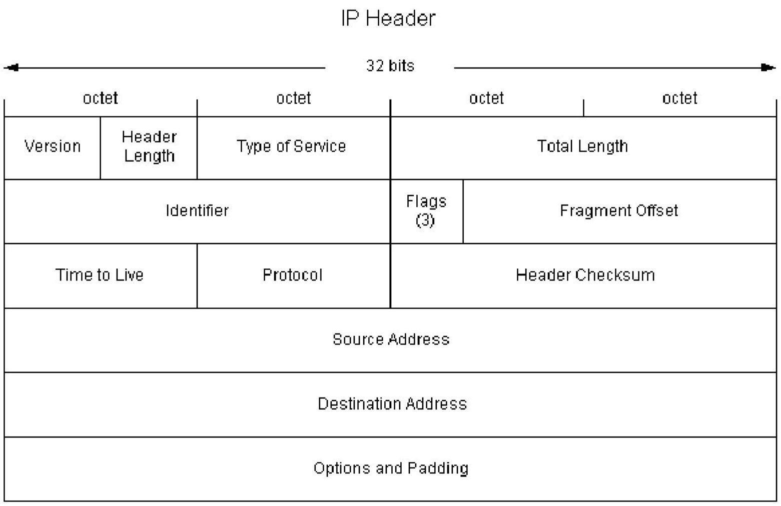


Figure 22: Differentiated Services (DiffServ) ToS byte

A DiffServ Code Point (DSCP) of 46 (101110), referred to as expedited forwarding (EF), is used for the proper treatment of voice packets. Signaling packets can also be marked with DSCP 46 if there is sufficient bandwidth to prevent dropped packets. To assure that voice and signaling packets are not in contention, mark signaling packets with a different DSCP value. With Communication Manager, you can set any DSCP value needed to work with a company's QoS scheme.

Some common DiffServ Code Points are defined in RFCs 2474 and 2475. Although DSCPs are specified in IETF RFCs, the treatment of packets that are tagged with DiffServ depends on implementation.

Note that older routers might require a DSCP setting of 40 (101000), which is backward compatible with the original ToS byte definition of critical. But again, Avaya products and software allows you to set any of the 64 possible DSCP values to work with your voice quality policy. You must use DSCP-46 for both bearer and control for simplicity. The default values are: Bearer-46, Control-34, Video-26. The ToS byte is an OSI model Layer 3 solution and works on IP packets on the LAN and WAN, depending upon the service provider.

Table 9: Original ToS specification

Bit description	Value	Use
Bits 0-2 IP precedence	000	Routine
	001	Priority
	010	Immediate
	011	Flash
	100	Flash Override
	101	CRITIC/ECP
	110	Internetwork control
	111	Network control
Bit 3 delay	0	Normal
	1	Low
Bit 4 Throughput	0	Normal
	1	High
Bit 5 reliability	0	Normal
	1	High
Bit 6 monetary cost	0	Normal
	1	Low
Bit 7 reserved		Always set to 0

Resource reservation protocol

Resource Reservation Protocol (RSVP) is a protocol that hosts can use to request specific QoS parameters through the network for a particular application data stream. A host can request guaranteed service through a network. If all routers have RSVP support enabled and there is sufficient unreserved bandwidth, a reservation is established throughout the network. In case of insufficient bandwidth, the reservation fails and notifies the hosts. At that point, hosts can send traffic without a reservation, or drop the connection.

RSVP can be enabled per network region on the network region form. If RSVP is enabled, endpoints including IP telephones and media processors attempt to establish a reservation for each call. If the reservation fails, Avaya endpoints still try to place a call but lower the DiffServ priority of the call to the better-than-best-effort (BBE) DSCP that is defined on the network region form. By default, this value is 43.

If RSVP is enabled on a network region, it is very important that it also be enabled on associated routers. If not, all RSVP reservations fail, and all voice traffic in that region is marked with the BBE DSCP, which generally receives degraded service versus the EF (DSCP 46) DiffServ Code Point.

Queuing methods

This section discusses common queuing methods and their appropriateness for voice.

Weighted fair queuing

Weighted fair queuing (WFQ) is similar to FIFO queuing, except that WFQ grants a higher weight to small flows and flows that are marked with higher DiffServ or IP TOS priorities. This queuing strategy does allow smaller (such as telnet) and higher-priority (such as IP telephony) protocols to squeeze in before high-flow, for example, ftp packets but does not starve off any traffic. By itself, it is not appropriate for IP telephony traffic because high-flow traffic can still delay IP telephony traffic and cause unacceptable latency and jitter.

Priority queuing

Strict priority queuing (PQ) divides traffic into different queues. These queues are usually high, medium, normal, and low, based on traffic type. This form of queuing services the queues in order of priority, from high to low. If there is a packet in the high-priority queue, it will always be serviced before the queue manager services the lower-priority queues. With priority queuing, however, it is possible to starve out lower-priority flows if sufficient traffic enters the high-priority queue. This mechanism works very well for IP telephony traffic where IP telephony bearer and signaling are inserted in the high-priority queue but does not work as well for routine data traffic that is starved out in case of sufficient high-priority traffic.

Round-robin

Round-robin queuing, also called *custom* queuing, sorts data into queues and services each queue in order. An administrator manually configures which type of traffic enters each queue, the queue depth, and the amount of bandwidth to allocate to each queue.

Round-robin queuing is not particularly suited to IP telephony. It does not ensure strict priority to voice packets, so they may still wait behind other traffic flows in other queues. Latency and jitter can be at unacceptable levels.

Class-Based weighted fair queuing

Class-Based Weighted Fair Queuing (CB-WFQ) with Low-Latency Queuing (LLQ), which is sometimes called Class-Based Queuing (CBQ), combines the above-mentioned queuing mechanisms. Generally, there is one strict-priority queue, several round-robin queues, and weighted fair queuing for the remainder. This queuing mechanism works very well for converged networks. IP telephony bearer and signaling packets receive the priority they need, while there remains an equitable mechanism for distributing remaining bandwidth. In addition, limits can be set on the high-priority queue to prevent it from using more than a specified amount of bandwidth. Bandwidth reserved for the high-priority queue is given to other queues in case of insufficient traffic in the high-priority queue.

Random early detection and weighted random early detection

Although they are not queuing methods *per se*, Random Early Detection (RED) and Weighted Random Early Detection (WRED) are important queue management techniques. RED and WRED work by randomly discarding packets from a queue. RED takes advantage of the congestion control mechanism of TCP. By randomly dropping packets prior to periods of high congestion, RED causes the packet source to decrease its transmission rate. Assuming that the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, which indicates that the congestion is cleared. Some implementations of RED, called Weighted Random Early Detection (WRED), combines the capabilities of the RED algorithm with IP Precedence. This combination provides for preferential traffic handling for higher-priority packets. RED/WRED can selectively discard lower-priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service.

RED and WRED are useful tools for managing data traffic but should not be used for voice. Because IP telephony traffic runs over UDP, IP telephony protocols do not retransmit lost packets, and IP telephony transmits at a constant rate. The IP telephony queue should never be configured for WRED. WRED only adds unnecessary packet loss and reduces voice quality.

Traffic shaping and policing

Traffic shaping is a mechanism to reduce the rate at which data is transmitted over an interface. Traffic shaping refers to the related technology of traffic policing. Policing works by either adjusting the priority of excess traffic to a lower queue or discarding the excess traffic. As with RED, discarding TCP traffic has the effect of throttling the stream by forcing the window size to shrink and decreasing its transmission rate. Because RTP is a fixed-bandwidth application, discarding RTP packets reduces voice quality without altering the transmission rate. Adjusting the priority of voice traffic removes the strict priority protection that reduces latency and jitter and offers the highest voice quality. Therefore, in most cases, it is beneficial to use QoS mechanisms rather than traffic shaping and policing to offer the highest quality for voice.

Frame Relay traffic shaping

Traffic shaping is important in technologies that implement virtual circuits (VCs), such as Frame Relay or ATM, where the Committed Information Rate (CIR) might be less than the physical speed of the interface, the port speed. In such scenarios, it is possible for traffic to burst above the CIR. Depending on the Service Level Agreement (SLA), a carrier might mark excess traffic as Discard Eligible (DE). The carrier might delay or discard excess traffic if congestion is detected within the network of the carrier. This behavior is unacceptable for voice traffic, which must minimize delay and jitter to achieve optimal voice quality. To solve this issue, Frame Relay traffic shaping gives an administrator tools to limit the transmission rate on a Frame Relay virtual circuit to the CIR.

A popular misconception is that voice traffic can be confined to the CIR while data traffic can be allowed to burst. But this does not know how Frame Relay works. No QoS mechanism for Frame Relay is negotiated between service providers and customers. Service providers view all traffic equally and mark any packet that exceeds the CIR as DE, even if the packet is high-priority voice. Therefore, the only way to guarantee optimal performance for voice traffic is to restrict the traffic rate to the CIR.

Configuring the Cisco router

Procedure

1. Disable Frame Relay adaptive shaping.

   This technique reduces the CIR in response to backwards explicit congestion notification (BECN) messages from the service provider. Because traffic is being transmitted at the CIR in the first place, it does not need to be throttled.

2. Set *`cir`* and *`mincir`* to the negotiated CIR.

   If FRF.12 fragmentation is implemented, reduce the *`cir`* and *`mincir`* values to account for the fragment headers.

3. Set *`be`*, the excess burst rate, to 0.
4. Set *`bc`*, the committed burst rate, to cir/100.

   This accounts for a serialization delay of maximum 10 ms .

5. Apply this map class to an interface, subinterface, or VC.

Example

The complete configuration for Frame Relay traffic shaping looks like the following:

```
map-class frame-relay
    NoBurst no frame-relay adaptive shaping
    frame-relay cir 384000! (for a 384K CIR)
    frame-relay mincir 384000
    frame-relay be 0
    frame-relay bc 3840

    interface serial 0
    frame-relay class NoBurst
```

Fragmentation

A big cause of delay and jitter across WAN links is serialization delay or the time that it takes to put a packet on a wire. For example, a 1500 byte FTP packet takes approximately 214 ms to be fed onto a 56 Kbps circuit. For optimal voice performance, the maximum serialization delay should be close to 10 ms. Therefore, a voice packet to wait for a large data packet over a slow circuit. The solution to this problem is to fragment the large data packet into smaller pieces for propagation. If a smaller voice packet comes in, it can be squeezed between the data packet fragments and be transmitted within a short period of time.

The following sections discuss some of the common fragmentation techniques:

Maximum transmission unit

The maximum transmission unit (MTU) is the longest packet (in bytes) that can be transmitted by an interface without fragmentation. Reducing the MTU on an interface forces a router to fragment the large packet at the IP level. This allows smaller voice packets to squeeze through in a timely manner.

The drawback to this method is that it increases overhead and processor occupancy. For every fragment, a new IP header must be generated, which adds 20 bytes of data. If the MTU is 1500 bytes, the overhead is approximately 1.3%. If the MTU is shortened to 200 bytes, however, the overhead increases to 10%. In addition, shortening the MTU to force fragmentation increases processor utilization on both the router and the end host that needs to reassemble the packet.

For these reasons, you must decrease the MTU only as a last resort. The techniques described later in this section are more efficient and should be used before changing the values of the MTU. When changing the MTU, size it such that the serialization delay is less than or equal to 10 ms. Thus, for a 384 kbps circuit, the MTU should be sized as follows: 384 kbps *0.01 second (10 ms)/8 bits/byte = 480 bytes. As the circuit size diminishes, however, care should be taken to not reduce the MTU below 200 bytes. Below that size, telephony signaling and bearer (voice) packets can also be fragmented, which reduces the link efficiency and degrades voice performance.

Link fragmentation and interleaving

Link Fragmentation and Interleaving (LFI) is an enhancement to Multilink PPP (MLP) that fragments packets at the Layer 2 (PPP) level. Fragmenting at the IP layer, as with MTU reduction, forces the addition of a new 20 byte IP header and an 8 byte PPP header. However, fragmenting at the data link (PPP) layer only forces generation of an 8 byte PPP header, which greatly increases the efficiency of the link.

You must use the LFI functionality instead of MTU manipulation when transmitting IP telephony packets over PPP links. As with MTU, you must size the packets so that the serialization delay is approximately 10 ms or less.

FRF.12

FRF.12 is a Frame Relay standard for fragmentation. It works for Frame Relay in the same way that LFI works for PPP, with similar increases in efficiency over MTU manipulation. When implementing a Frame Relay network, you must use FRF.12 for fragmentation and size the fragments such that the serialization delay is no more than 10 ms.

Real-time transport protocol

RTP header compression is a mechanism that reduces the protocol overhead associated with IP telephony audio packets. This mechanism is a function of the network and not a function of the IP telephony application. Along with the advantages of using RTP header compression, there are also some disadvantages as well.

Application perspective

Anatomy of 20 ms G.729 audio packet on page 126 shows the anatomy of a 20 ms G.729 audio packet, which is preferably used across limited bandwidth WAN links. Notice that two-thirds of the packet is consumed by overhead such as IP, UDP, and RTP and only one-thirds is used by the actual audio.

Table 10: Anatomy of 20 ms G.729 audio packet

IP header	UDP header	RTP header	20 ms of G.729 audio
20 B	8 B	12 B	20 B

All 20-ms G.729 audio packets, regardless of the vendor, are constructed like this. Not only is the structure of the packet the same, but the method of encoding and decoding the audio itself is also the same. This similarity allows an Avaya IP telephone to communicate directly with a Cisco IP telephone or any other IP telephone when using matching codecs. The packets from the application perspective are identical.

Network perspective

RTP header compression is a mechanism that routers use to reduce 40 bytes of protocol overhead to approximately 2 to 4 bytes. Cisco routers uses this RTP header compression. The RTP header compression can drastically reduce the IP telephony bandwidth consumption on a WAN link when using 20 ms G.729 audio. When the combined 40 byte header is reduced to 4 bytes, the total IP packet size is reduced by 60% (from 60 bytes to 24 bytes). This equates to reducing the total IP telephony WAN bandwidth consumption by roughly half, and it applies to all 20 ms G.729 audio packets, regardless of the vendor.

Recommendations for RTP header compression

Enterprises that deploy routers capable of this feature can benefit from the feature. However, Cisco suggests caution in using RTP header compression on its routers because it can significantly tax the processor if the compression is done in software. Depending on the processor load before compression, enabling RTP header compression can significantly slow down the router or cause the router to stop completely. For best results, use a hardware/IOS/interface module combination that permits the compression to be done in hardware.

RTP header compression has to function with precision or audio will be disrupted. If, for any reason, the compression at one end of the WAN link and decompression at the other end do not function properly, the result can be intermittent loss of audio or one-way audio. RTP header compression has been very difficult to quantify, but there is evidence that cRTP sometimes leads to voice-quality issues. One production site in particular experienced intermittent one-way audio, the cause of which was garbled RTP audio samples inserted by the cRTP device. When, for experimentation purposes, RTP header compression was disabled, the audio problems disappeared.

Cisco configuration example

The following example shows the Cisco IOS Ethernet switch commands that demonstrate and optimize an environment needed for IP Telephony and video.

Connecting to the Ethernet switch

Ports 1 through 10 are assigned to the voice VLAN and this configuration is suitable for stand-alone IP phones and video devices that connect to the Ethernet switch.

```
Switch> enable                                      change from user to privilege mode
Switch # configure terminal                     change to global config mode
Switch(config)# vlan 20 name v20               create vlan 20 for voice traffic
Switch(config)# int range fa 0/1 - 10            context for ports 1 through 10
Switch(config)# des “IP phones with no
PCs attached”                                Description of ports’ use
Switch(config)# switchport access vlan 20 change native/port vlan from data (vlan-1) to
voice (vlan-20)
Switch(config)# no cdp enable                  disable CDP for ports 11-20 (remove
proprietary protocols)
Switch(config)# spanning-tree portfast        place ports in forwarding mode immediately
Switch(config)# spanning-tree bpduguard
enable                                      enable bpdu guard in case of a layer-2 loop
```

Attaching a PC

Ports 12 through 20 are assigned to the voice vlan and this config is suitable for IP phones and video devices that have a PC attached to them..

```
Switch(config)# int range fa 0/11 - 20           context for ports 11 through 20
Switch(config)# des “IP phones with PCs
attached”                                       description of ports’ use
Switch(config)# speed 100                             lock port speed to 100-Mbps
(optional setting to Auto-Neg)
Switch(config)# duplex Full                         lock port duplex to Full (optional
setting to Auto-Neg)
Switch(config)# switchport voice vlan 20         config implicit trunk for IP phones or
video endpoints
Switch(config)# no cdp enable                       disable CDP for ports 11 through 20
Switch(config)# spanning-tree portfast            place ports in forwarding mode
immediately
Switch(config)# spanning-tree bpduguard enable enable bpdu guard in case of a layer-2
loop
```

Taking traffic to a router

These commands create a trunk (more than one vlan) to take voice and data traffic to a router.

```
Switch(config)# int fa 0/48                         context for port 48
Switch(config-if)# des “Uplink trunk to
router R1”                                       description of port usage
Switch(config-if)# switchport trunk encap
dot1q                                             define port 48 as a data trunk using
802.1Q
Switch(config-if)# switchport mode trunk        enable trunking mode
Switch(config-if)# switchport nonegotiate        trunk port 48 will not negotiate a
trunk status with the
                                               other end of the link
Switch(config-if)# switchport trunk allowed
vlan remove 2-19,21-4094                           remove unneeded vlans
```

Chapter 8: Avaya solution elements

Avaya SBC overview

Avaya SBC provides security to SIP-based Unified Communications (UC) networks. Avaya SBC is available in two versions: Standard Services and Advanced Services. Either version can reside on supported servers. For information about supported servers, see Supported device configurations on page 130.

Avaya SBC has two main components: the management system named Element Management System (EMS), and the call processing system named SBC. Depending on the network size and service requirement, you can deploy Avaya SBC in one of the following configurations:

- Standalone configuration

  In the standalone configuration, the EMS and SBC co-reside in the same server.
- Multiple server configuration

  In the multiple server configuration, the EMS and SBC are deployed on separate servers.
- High Availability (HA) configuration

  In an HA configuration, SBC servers are deployed in pairs. Each pair has one SBC acting as the primary while the other SBC is the secondary. Both servers are controlled by a single EMS or a replicated EMS pair.

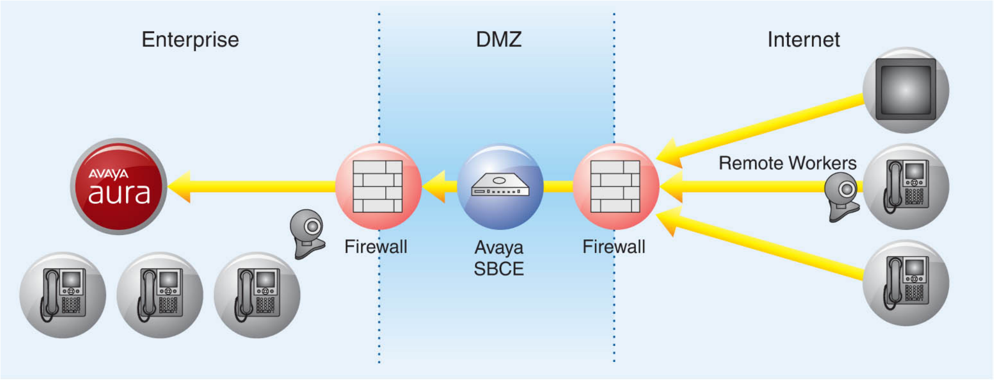
Advanced Services

Avaya SBC Advanced Services is a specialized Unified Communications (UC) security product. Advanced Services protects all IP-based real-time multimedia applications, endpoints, and network infrastructure from potentially catastrophic attacks and misuse. This product provides the real-time flexibility to harmonize and normalize enterprise communications traffic to maintain the highest levels of network efficiency and security.

Advanced Services provides the security functions required by the ever changing and expanding UC market. Advanced Services protects any wire-line or wireless enterprise or service provider that has deployed UC from malicious attacks such as denial of service, teardrop, and IP sweep attacks. These attacks can originate from anywhere in the world anytime. Advanced Services is the only UC-specific security solution that effectively and seamlessly incorporates all approaches into a single, comprehensive system.

Avaya SBC Advanced Services incorporates the best practices of all phases of data security to ensure that new UC threats are immediately recognized, detected, and eliminated. Advanced Services incorporates security techniques that include UC protocol anomaly detection and filtering, and behavior learning-based anomaly detection. Together, these techniques monitor, detect, and protect any UC network from known security vulnerabilities by:

- Validating and supporting remote users for extension of Avaya Aura® UC services.
- Using encryption services such as SRTP.



cysbavsd 061313

Figure 23: Advanced Services Solution

Standard services

Avaya SBC Standard Services provides a subset of the functionality of the Advanced Services offer. Standard services has the functionality required for an enterprise to terminate SIP trunks without the complexity and higher price associated with a typical Session Border Controller (SBC).

Avaya SBC Standard Services is a true enterprise SBC, not a repackaged carrier SBC. This product provides a lower-cost alternative to the more expensive Carrier SBCs. Standard Services also provide an Enterprise SBC that is affordable, highly scalable, and easy to install and manage. Standard Services is a Plug and Play solution for Enterprises and Small to Medium Businesses.

With this product, customers can benefit from Avaya's extensive experience in SIP trunk deployments and supporting large numbers of enterprise users. Avaya SBC Standard Services features the unique Signaling Manipulation module (SigMa module), which dramatically simplifies the deployment of SIP trunks. The SigMa module streamlines integration of SIP trunks into thousands of variations of enterprise SIP telephony environments, greatly reducing implementation time. As a result, SIP trunk deployment in many standard configurations can occur in 2 hours or less.

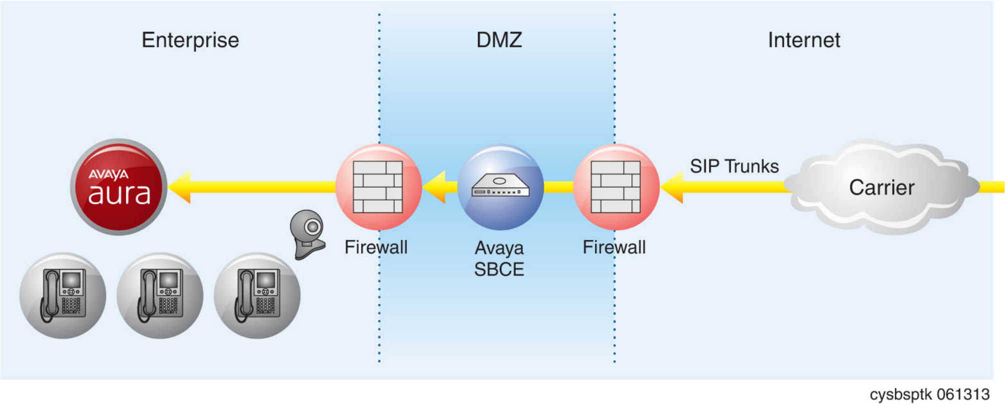


Figure 24: SIP trunking

Supported device configurations

Hardware server device configurations supported with this release

The following table lists the Avaya SBC or EMS device configurations supported by each hardware server. The table also contains information about the number of NIC ports available and the hardware category for each server.

Server	NIC Ports	DVD drive	Hardware category	Supported device configuration		
				EMS	SBC	EMS+SBC
Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3	6	Yes	310	Supported	Supported	Supported
Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5	6	Yes	310	Supported	Supported	Supported
Dell™ PowerEdge™ R340 Avaya Solutions Platform 110 Appliance server	6	No	310	Supported	Supported	Supported
Dell 3240	5	No	310	Not Supported	Not Supported	Supported
Dell VEP1425N	8 ports available , but only 4 ports are supporte d	Yes	310	Not supported	Not Supported	Supported

Table continues…

Server	NIC Ports	DVD drive	Hardware category	Supported device configuration		
				EMS	SBC	EMS+SBC
Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A2	6	Yes	310	Supported	Supported	Supported
Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A3	8 ports available , but only 6 ports are supporte d	Yes	310	Supported	Supported	Supported
Dell R360	6	Yes	310	Supported	Supported	Supported

Hardware servers that support new installations for this release

- Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3
- Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5
- Dell™ PowerEdge™ R340 Avaya Solutions Platform 110 Appliance server
- Dell 3240
- Dell VEP1425N
- Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A2
- Dell R660 Avaya Solutions Platform 110 Appliance server - Profile A3
- Dell R360

Avaya Communication Server 1000 E overview

Avaya Communication Server 1000 E is a robust and highly scalable IP Private Branch eXchange (PBX) that supports traditional Meridian features as well as new IP telephony features, including SIP.

With the CS 1000E, customers can evolve from a traditional Time Division Multiplexing (TDM) network to a converged IP network. Deployment is seamless because the CS 1000E integrates with existing PBX systems from Avaya and third parties. This deployment enables customers to expand the size and functionality of their networks while preserving their investment in legacy equipment, such as Meridian 1, Option 11C, and Communication Server 1000 systems.

Being IP-based, CS 1000E supports distributed architecture. With the distributed architecture, the customer can place the systems and components where they can be fit best. For example, using the Branch Office feature, customers can set up Branch Office Media Gateways (MG 1000B) in remote sites to extend the complete feature set across various geographic locations across the globe. Customers can also configure the CS 1000E to support Campus Redundancy and Geographic Redundancy to increase system availability.

The CS 1000E provides the same business-grade availability, security, reliability, and scalability as the other Enterprise solutions of Avaya.

Related links

Key attributes of Avaya Communication Server 1000 E on page 132

Key attributes of Avaya Communication Server 1000 E

Avaya Communication Server 1000E has the following key attributes:

- Adaptable to meet current and future needs: CS 1000E provides an evolutionary path to next-generation multimedia communications.
- Superior IP Telephony experience: CS 1000E has an open platform that takes advantage of innovative applications and feature-rich, next generation clients.
- Improved reliability and security: CS 1000E offers better business continuity improvement from a reliable and secure environment.
- Simplified convergence solution: CS 1000E offers a product portfolio that is simplified for easier deployment, configuration, and management.

Related links

Avaya Communication Server 1000 E overview on page 131

Other applications

Communication applications

Communication Manager supports a large variety of communication capabilities and applications, including:

- CallCenter on page 132
- Unified Communication Center on page 133
- Avaya overview on page 133
- Computer Telephony Integration (CTI) on page 133
- Application Programming Interfaces (APIs) on page 134
- BSR polling on page 134

Call Center

Avaya Call Center provides a total solution for the sales and service needs of a customer. Avaya Call Center connects callers with the appropriate agents. When a caller places call to a contact center, Communication Manager captures the information about the caller and, depending on this information, routes the call to the appropriate caller in the contact center.

The Call Center solution consists of new and existing versions of Avaya servers, Communication Manager, and Call Center peripherals. This solution supports:

- Extensions of up to 13 digits
- LAN backup of Call Management System for high availability
- Customer-requested enhancements

Some of the Call Center applications that integrate with Communication Manager are:

- Avaya Call Management System for real-time reporting and performance statistics
- Avaya Business Advocate for expert, predictive routing based on historical data and incoming calls

Unified Communication Center

Using Unified Communication Center, mobile, remote and office workers can easily gain access to important communications tools and information through any telephone by using simple and intuitive speech commands.

Avaya Call Management System overview

Avaya Call Management System (CMS) is a software product for businesses and organizations that have Communication Manager and receive a large volume of telephone calls that are processed through the Automatic Call Distribution (ACD) feature. CMS collects call-traffic data, improves the readability of management reports, and provides an administrative interface to the ACD feature on Communication Manager.

Administrators can access the CMS database, generate reports, modify ACD parameters, and monitor call activities to improve call processing efficiency.

CMS uses dual TCP/IP links for duplicated data collection and high availability. To prevent data loss from ACD link failures, CMS hardware or software failures, and maintenance or upgrades, the ACD data is sent to both servers over different network routes. You can administer the ACD data from either server.

Computer Telephony Integration

Using Computer Telephony Integration (CTI), you can control Communication Manager using enables external applications. With CTI you can integrate customer databases with call control features. CTI is a LAN-based solution that consists of server software that runs in a client/server configuration.

CTI opens up Application Programmer Interfaces like ASAI, Telephony Services Application Programming Interface (TSAPI), and Java Telephony Application Programming Interface (JTAPI). An external application can use these APIs to control the server.

Application Programming Interfaces

Communication Manager supports the following APIs to interface with other applications:

- Adjunct Switch Application Interface (ASAI): With this API, adjunct applications can use Communication Manager features and services. Integration with adjuncts occurs through APIs. ASAI is part of Avaya Computer Telephony.
- DEFINITY Application Programming Interface (DAPI) for accessing control and data paths within Communication Manager.
- Java Telephony Application Programming Interface (JTAPI): This is an open API supported by Avaya Computer Telephony and enables integration to Communication Manager ASAI.
- Telephony Application Programming Interface (TAPI): This API is used to provide telephony services to computers running the Microsoft Windows operating system.
- Telephony Services Application Programming Interface (TSAPI): This open API is supported by Avaya Computer Telephony and enables integration to Communication Manager ASAI.

Best Service Routing polling

Best Service Routing (BSR) polling over QSIG Call Independent Signaling Connections (CISCs) and Temporary Signaling Connections (TSCs) provides the ability to do BSR polling between multiple sites over H.323 IP trunks without requiring an ISDN PRI B-channel. BSR polling software uses QSIG CISC/TSCs to reduce the need for IP Media Processor circuit packs resulting in a solution that is cost-effective for a multisite Contact Center.

Soft clients

Avaya Workplace Client overview

Avaya Workplace Client is a soft phone application that provides access to Unified Communications (UC) and Over the Top (OTT) services. You can access Avaya Workplace Client on the following platforms:

- Mobile:
  - Android: From a mobile phone, tablet, or an Avaya Vantage™ device
  - iOS: From an iPad or iPhone.
- Desktop:
  - Mac
  - Windows
  - Chrome: From a Google Chromebook

Based on your feature requirement, you can deploy Avaya Workplace Client in several ways. In the basic deployment type, you can have only voice calling. You can then include additional features such as directory search, contact management, presence, instant messaging, and conferencing.

With Avaya Workplace Client, you can use the following functionalities:

- Make point-to-point audio and video calls.
- Answer calls, send all calls to voice mail, and forward calls
- Extend calls to your mobile phone if EC500 is configured
- Log in to your extension and join calls with multiple devices if Multiple Device Access (MDA) is configured.
- Listen to your voice mail messages.
- View your call history.
- Access your Avaya Aura® and local contacts.
- Perform an enterprise-wide search using Avaya Aura® Device Services, Client Enablement Services, Avaya Cloud Services, ActiveSync on mobile platforms and Avaya Aura® Device Services, LDAP, or Avaya Cloud Services on desktop platforms.
- Manage your presence status and presence status message.
- Send instant messages.
- Capture photo, audio, and video files, and send generic file attachments in an IM conversation.
- Join and host conference calls with moderator controls.
- Use point-to-point and conference call control functionality. You can also add participants to a conference.
- Share a screen portion, the entire display screen, an application, or a whiteboard while on a conference call on desktop platforms.
- View a portion of the screen, the entire display screen, an application, or a whiteboard shared by another conference participant on mobile and desktop platforms.

Note:

Some Avaya Workplace Client features must be configured for your enterprise before you can use them.

Features

Avaya Workplace Client provides the following features:

- Enterprise capabilities with ease of use in a single experience.
    - Enterprise voice: Supports mission critical voice services, which ensure people can talk when and how they need to.
    - Video everywhere: Enriches the quality of communication interactions.
    - Persistent multimedia messaging: Provides a social style conversation hub with rich multimedia and multiparty capabilities.

  - Rich presence: Makes it easy to determine availability and reachability of your contacts.
  - Integrated video collaboration with interactive content sharing: Makes remote team meetings just as effective as face-to-face meetings.
- Available across a full range of platforms, such as Android, iOS, Mac, and Windows.
- Remote worker support with Avaya Session Border Controller. Enables secure VPN-less access to services when working outside of the private network.
- Simplified provisioning. Avaya Workplace Client is designed to import administrator-defined settings and remove virtually all end-user configuration tasks short of entering user name and password.
- Solution resiliency. Includes automated Avaya Aura® Session Manager failover support with primary, secondary, and branch simultaneous registration.
- Secure communication channels. Protects end-user privacy. Enhancements in this release also include client identity certificate support to enable trusted connections and to reliably authenticate both servers and connecting clients.

For a detailed list of features, see *Using Avaya Workplace Client for Android, iOS, Mac, and Windows*.

IP/SIP telephones and softphones

Using IP and SIP telephones, you can gain access to the features of Communication Manager from multiple locations. Mobility is a major benefit of IP and SIP telephones. For example, you can move the telephones by plugging the telephones anywhere in the network. Similarly, another benefit of mobility in IP softphones is that after you install the softphones on a laptop computer, you can connect these softphones to Communication Manager from any remote location. Users can place calls and handle multiple calls on their computers.

IP telephones support the following features: Time-To-Service (TTS) capability, gratuitous ARP reply, and acceptance of incoming TCP connection from an active server.

See Telephones, endpoints, video devices, and software client on page 34 for the list of supported endpoints.

For more information on the supported features, refer to Communication Manager feature description guide and the respective endpoints overview guide.

Extension to Cellular overview

The Avaya Extension to Cellular feature provides users with the capability to have one administered telephone that supports Communication Manager features for both an office telephone and up to four outside telephones. An office telephone is a telephone that is directly under the control of Communication Manager, such as a desk telephone in an office. The outside telephone is a cellular or wireless telephone and is referred to in this text as a *cell phone.* Extension to Cellular works with any type of wireless or cellular service.

With Extension to Cellular, users can receive and place official calls anywhere, at any time, even if the users are not in the office. In addition, users can also access Communication Manager features through the cell phone. Users can enable and disable Extension to Cellular so that the cell phone does not always receive office telephone calls. Users can also switch between the cell phone and office telephone during an ongoing Extension to Cellular telephone call.

When Extension to Cellular is administered and active, a call to the office telephone extension alerts both the office telephone and the cell phone simultaneously. In addition, Extension to Cellular maintains consistency in contact information. The cell phone takes on the identity of the office telephone when calls are made from the cell phone to another number on the same switch as the cell phone sends the caller ID information of the office telephone of the caller. Therefore, calls from the cell phone appear to be from the office telephone number.

A user operates a cell phone as if it were a standard, caller ID-enabled telephone extension connected directly to an Avaya server running Communication Manager. The cell phone acts as an extension because the cell phone is mapped to the main office telephone. All other types of cell phone calls, such as direct calls to and from the published cell phone number, are not affected by Extension to Cellular. The cell phone performs exactly as it did before enabling Extension to Cellular. If your Cellular Service Provider (CSP) provides this service, Extension to Cellular is always enabled. You can also enable or disable Extension to Cellular by using a Feature Name Extension (FNE), as described in Setting up Feature Name Extensions set.

Note:

> EC500 and CSP work only with ISDN-PRI, ISDN-BRI, H.323, Multi Frequency Compelled (MFC), and SIP trunks.

Cellular service providers who resell the Extension to Cellular service use the CSP or SPFMC (Service Provider Fixed-Mobile Convergence for dual mode phones) application type. CSP/SPFMC support ISDN, H.323, and SIP trunks. CSP/SPFMC is essentially the same as the Extension to Cellular application. Unlike Extension to Cellular, CSP/SPFMC is always enabled. With CSP or SPFMC, users cannot disable Extension to Cellular.

The Extension to Cellular feature also supports Fixed Mobile Applications (FMC), Public Fixed Mobility (PBFMC), and Private Fixed Mobility (PVFMC). The FMC applications are used for wireless endpoints that support a one-X Mobile Client application that has two modes called SMode (Single Mode) and DMode (Dual Mode). The FMC applications (PBFMC, PVFMC, and SPFMC) are the only OPTIM applications that support the CTI Mobility Integration feature.

When both the PBFMC and the PVFMC applications are administered for a station, incoming calls to that station are forked to both the public and private destinations specified in the station-mapping administration list. If the private FMC application receives a message indicating that the far-end has answered the call, Communication Manager cancels the call on the public FMC application. Reception of an alerting indication means that the wireless endpoint must be present in the private wireless network and therefore cannot be in the cellular network.

See also Application RTUs for Fixed Mobile Convergence.

Unified communications for business users

Conferencing using Avaya Equinox® Conferencing

Avaya Equinox® Conferencing continues the evolution of Conferencing with the following features:

- Meeting participation extended to include the WebRTC participant. You do not need any plug-in to participate.
- An integrated portal that detects the browser or device you are on and connects you to the meeting. This is possible using WebRTC or the native application.
- Audio participation extended to thousands.
- Automatic cloud provisioning for room systems.

Advanced conferencing features are supported only if your deployment includes Avaya Equinox® Conferencing.

Download and installation of Avaya Equinox® Conferencing client

The Avaya Equinox® Conferencing portal detects whether you have installed Avaya Workplace Client.

- If Avaya Workplace Client is installed, Avaya Workplace Client is used to join a conference.
- If Avaya Workplace Client is not installed, the portal prompts you to use the WebRTC browser client only on desktops. Otherwise, you must install Avaya Workplace Client to join the conference.
- If Avaya Workplace Client is installed but not logged-in, you can join the conference without configuring your account.

The portal provides a mechanism to detect the version of the installed client and install any required update, linking to the app store as appropriate for mobile clients.

Chapter 9: Traffic Engineering

Introduction to traffic engineering

In its most general sense, an Avaya Aura® enterprise solution consists of a network of various applications. Currently, the most prominent application is Communication Manager. Other applications include

- Experience Portal (Voice Portal)
- Expanded Meet-Me Conferencing
- Avaya Aura® Conferencing
- Avaya Aura® Messaging
- Voice Recording

The various applications supported by an enterprise can be interconnected in various ways. Circuit-switched trunking (TDM trunking) and H.323 trunking (IP trunking) are still widely used in the field today.

The interconnection of enterprise elements via SIP uses Avaya Aura® Session Manager, which controls the call routing between all SIP-enabled elements in an enterprise. Session Manager can also function as a registrar for SIP stations.

The primary purpose of this section is to provide methodologies by which the traffic-sensitive components in an Avaya communication enterprise can be properly engineered. Special emphasis is placed on elements associated with the most recent Session Manager and Communication Manager releases.

Design inputs

This section discusses the essential design elements to be specified by the customer. Those elements pertain to the configuration topology, the various endpoints involved, and the nature of the traffic flow between those endpoints.

Topology

An Avaya Aura® enterprise solution consists of a network of various applications, including Session Manager, Communication Manager, Experience Portal (Voice Portal), Messaging, and Voice Recording. Communication Manager, which is currently the most prominent application, consists of a server and all of the components under that server's control. The various components can be placed into logical and/or physical groups.

A single Communication Manager system comprises one or more network regions. Each network region is a logical grouping of components such as endpoints, gateways, and certain circuit packs. The components of a Communication Manager system could also span various physical placements including gateways and geographical locations (sites).

Knowledge of the details of the configuration topology, from both logical and physical standpoints, is essential to properly conduct a traffic analysis. In particular, the topology often plays a role in determining the routes that are traversed by various call types.

Related links

Erlang and ccs definitions on page 141
Endpoint usages on page 143
Erlang B and C models on page 142
Required number of branch gateways on page 159
Determining G450 Branch Gateway media resources on page 161
Determining G430 Branch Gateway media resources on page 160

Calls and endpoints

A call is normally thought of as a communication between two or more parties, across a set of communication facilities, and it is natural to think of those parties as the endpoints involved in the call. In fact, such parties are sometimes referred to as terminals, and they can include telephones, fax machines, voice recorders, IVRs (Interactive Voice Response units), and video devices. However, the term endpoint can also be used in certain circumstances to include facilities that do not represent the true points of termination of a call (most notably, trunks).

We use the term station to refer to a device being used by human beings in real-time to originate and receive calls (including voice calls, faxes, and text messaging). Such devices include circuit-switched telephones, H.323 hardphones and softphones, SIP hardphones and softphones, and fax machines. The people using them are referred to as users.

When referring to a domain such as an Avaya Aura® enterprise solution or a particular Communication Manager system, the term station is only used to refer to stations within that domain. For example, when performing traffic analysis on a particular Avaya Aura® enterprise, telephones in the PSTN are not considered to be stations in that enterprise. This represents a circumstance in which trunks are referred to as endpoints from the perspective of the enterprise of interest, even though they are not true points of call termination.

Normally, the set of enterprise configuration inputs includes a specification of the quantity, physical location, and logical association (for example, network region) of each type of station to be used in a particular enterprise. In some cases, the number of trunks is also specified, while in others, the number of trunks must be calculated as an output of the traffic-engineering process.

Traffic usages

Erlang and ccs definitions

Consider a stream of calls flowing across a group of trunks from one population of endpoints to another. The number of simultaneous calls traversing the trunks generally varies over time (that is, it increments by one every time a new call arrives on an available trunk, and it decrements by one every time an existing call terminates). The corresponding *carried load* (or *usage*), expressed in Erlangs, is defined as the *average number of simultaneous calls* that are traversing the trunks during a given time period (for example, during the busy hour). Note that in this example, the number of active calls always equals the number of busy trunks (since each active call requires exactly one trunk). Therefore, the *call usage* (that is, the average number of simultaneous active calls) equals the *trunk usage* (that is, the average number of simultaneous busy trunks) in this example.

If a call arrives while all trunks are busy, it is said to be blocked at the trunk group. In other words, not all calls that are offered to the trunks are actually carried by the trunks. Accordingly, the corresponding offered load, expressed in Erlangs, is defined as the average number of simultaneous calls that would have been traversing the trunks during a given time period (for example, during the busy hour), had there been enough trunks to prevent blocking. Note that in this example, the offered call load (that is, the average number of simultaneous active calls had there been enough trunks to carry all call attempts) equals the offered trunk load (that is, the average number of simultaneous busy trunks had there been enough trunks to carry all call attempts) in this example.

To summarize so far, the traffic load, expressed in Erlangs, represents the average number of simultaneous active calls or busy resources, during a given time period (for example, the busy hour).

Also note that the usage of a single station, when expressed in Erlangs, represents the fraction of time the station is in use. For example, a station that carries 0.1 Erlang of usage is busy 10% of the time (during the time interval of interest; for example, the busy hour).

Two fundamental characteristics of a stream of call traffic are the call rate (usually expressed in calls per hour) and the average call duration (usually expressed in seconds). The corresponding call usage can be defined as follows:

Usage (in Erlangs) = [(calls per hour)(seconds per call)]/3600

Note that in some traffic reports, the call rates are termed as call counts. If a particular report is associated with a period of time other than one hour, care must be taken not to mistakenly apply the call count as the calls per hour in the preceding formula. Be careful to convert call counts to calls per hour before applying the formula.

The term ccs stands for centum call seconds, which is a period of time 100 s in duration. To minimize confusion, although ccs is technically a unit of time and could be used as such, in this case it is only used to designate traffic loads.

Recall that a traffic load expressed in Erlangs is tacitly associated with a given time period (typically one hour). If that is the case, the relationship between a traffic load expressed in Erlangs and that same load expressed in ccs is:

Usage (in Erlangs) = Usage (in ccs)/36

However, consider a case in which a particular load, expressed in Erlangs, represents the average number of simultaneous active calls or busy resources, during a given time period other than one hour. In such a case, the denominator in the preceding expression should be set to equal the number of 100 s intervals in the time period of interest.

Finally, since a single station carrying one ccs of traffic is busy for 100 s during the busy hour, the maximum traffic that can be carried by a single station or trunk is 36 ccs.

Related links

Topology on page 139
Endpoint usages on page 143
Erlang B and C models on page 142
Required number of branch gateways on page 159
Determining G450 Branch Gateway media resources on page 161
Determining G430 Branch Gateway media resources on page 160

Erlang B and C models

The Erlang B model is used to represent a situation in which calls that arrive when all resources (for example, trunk channels) are busy, are blocked and subsequently denied service. The model further assumes that the calls follow Poisson arrival and departure processes (which is typical for actual calls in real configurations), and that blocked calls never retry.

There are four parameters associated with the Erlang B model:

- Offered load (Erlangs)
- Carried load, which is sometimes referred to as usage (Erlangs)
- Number of resources
- GoS (grade of service, which is the probability of blocking at the resources)

Normally, when working with anticipated traffic loads (for example, for a new configuration), we work with the offered load, the number of resources, and the GoS. On the other hand, when working with measured traffic loads (for example, found on traffic reports run on existing configurations), we work with the carried load (usage), the number of resources, and the GoS. In either case, given any two of the three relevant values, the Erlang B model produces the third value.

The Erlang C model is used to represent a situation in which calls that arrive when all resources (for example, trunk channels) are busy, are blocked and subsequently queued. Like the Erlang B model, the Erlang C model is predicated on the assumption that the calls follow Poisson arrival and departure processes. Furthermore, the Erlang C model assumes an infinite amount of space in the queue.

There are three parameters associated with the Erlang C model:

- Offered load, which equals the carried load in this model (Erlangs)
- Number of resources

- GoS (grade of service, which is the probability of blocking at the resources)

Given the values of any two of those three parameters, the Erlang C model produces the third value.

Note that the GoS is often expressed as P01 or P001. P01 represents at most 1 call out of every 100 being blocked at the resource of interest (that is, 1% blocking), and P001 represents at most 1 call out of every 1000 being blocked at the resource of interest (that is, 0.1% blocking).

Consider a situation in which a call that is blocked is constantly retried until it receives service, meaning that as soon as a busy signal is heard, the caller hangs up and immediately redials. This is the most extreme form of retrial, and it is almost as if each blocked call is simply placed in queue and receives service as soon as a resource frees up for it. In other words, the Erlang C model is a reasonable approximation for constant retrials.

So, since Erlang B represents no retrials and Erlang C approximates constant retrials, the average of the two models is a reasonable approximation for moderate retrials. In this document, the pure Erlang B model is used when ignoring the effect of retrials, and the average of the Erlang B and C models (that is, a mixed Erlang B/C model) is used when the effect of retrials is deemed to be relevant.

Although the Erlang C model deals with queueing effects, it is not a particularly reasonable model for inbound Call Centers unless the number of trunks is significantly higher than (for example, several orders of magnitude greater than) the number of agents. The M/M/c/k Finite Queue model, which is beyond the scope of this discussion, should be used instead. A pure Erlang C model is never used in this discussion.

Related links

Topology on page 139
Erlang and ccs definitions on page 141
Endpoint usages on page 143
Required number of branch gateways on page 159
Determining G450 Branch Gateway media resources on page 161
Determining G430 Branch Gateway media resources on page 160

Endpoint usages

The three fundamental components of general business call traffic are intercom (that is, calls between two enterprise stations), outbound (that is, enterprise station to PSTN trunk), and inbound (that is, PSTN trunk to enterprise station). There are two possible approaches for determining default values for the corresponding per-station call usages; one approach typically applies if the number of PSTN trunks is unknown and needs to be sized, and the other can only be applied if the number of PSTN trunks is known (or assumed to be a specific value) a priori.

Endpoint usages in a 1/3-1/3-1/3 call mix

In a general business environment, the intercom, outbound, and inbound call usages are often assumed to be equal. In other words, each of those three components represents 1/3 of the traffic.

The average duration of a general business call is typically assumed to be 200 s (20 s for call set-up, and 180 s of talk time) as a default. Furthermore, the average station is assumed to induce the following call rates during the busy hour.

Light General Business Traffic:

- originate 0.25 intercom call per hour
- originate 0.25 outbound call per hour
- receive 0.25 inbound call per hour

Moderate General Business Traffic:

- originate 0.50 intercom call per hour
- originate 0.50 outbound call per hour
- receive 0.50 inbound call per hour

Heavy General Business Traffic:

- originate 0.75 intercom call per hour
- originate 0.75 outbound call per hour
- receive 0.75 inbound call per hour

The corresponding default per-station busy-hour usages can be calculated using the preceding call rates, a 200-s average hold time, and the formulas in the Erlang and ccs definitions section.

Light General Business Traffic:

- originate 0.5 ccs = 0.014 Erlang of intercom call usage
- originate 0.5 ccs = 0.014 Erlang of outbound call usage
- receive 0.5 ccs = 0.014 Erlang of inbound call usage

Moderate General Business Traffic:

- originate 1.0 ccs = 0.028 Erlang of intercom call usage
- originate 1.0 ccs = 0.028 Erlang of outbound call usage
- receive 1.0 ccs = 0.028 Erlang of inbound call usage

Heavy General Business Traffic:

- originate 1.5 ccs = 0.042 Erlang of intercom call usage
- originate 1.5 ccs = 0.042 Erlang of outbound call usage
- receive 1.5 ccs = 0.042 Erlang of inbound call usage

Endpoint usages driven by the number of trunks

If the number of PSTN trunks is known (or is assigned some assumed value as part of the given information), then an alternate approach to the one provided in Endpoint Usages in a 1/3-1/3-1/3 Call Mix can be used. Actually, the procedure for determining the per-station intercom usage is identical to the procedure used in the 1/3-1/3-1/3 model. The difference appears in the outbound and inbound usages; specifically, the outbound and inbound components of the traffic are derived by assuming the trunks have been engineered to a P01 GOS. The results are as follows:

- The default per-station intercom usage either 0.5 ccs = 0.014 Erlang (light general business traffic), 1.0 ccs = 0.028 Erlang (moderate general business traffic), or 1.5 ccs = 0.042 Erlang (heavy general business traffic)
- The default per-station outbound usage is determined by calculating the carried load associated with the given number of outbound trunks, an assumed grade of service (P01 is standard for PSTN trunks), and the mixed Erlang B/C model
- The default per-station inbound usage is determined by calculating the carried load associated with the given number of inbound trunks, an assumed grade of service (P01 is standard for PSTN trunks), and the mixed Erlang B/C model

One drawback to using this method is that it assumes the trunks have been engineered to a P01 GOS. If the trunks are not being heavily used (for example, if a lot of extra trunks have been added solely for redundancy purposes), this model produces estimates for the outbound and inbound usages that are far greater than the actual usages.

Related links

Topology on page 139
Erlang and ccs definitions on page 141
Erlang B and C models on page 142
Required number of branch gateways on page 159
Determining G450 Branch Gateway media resources on page 161
Determining G430 Branch Gateway media resources on page 160

Non-SIP Communication Manager

In this document, the term non-SIP Communication Manager refers to a Communication Manager supporting no SIP signaling groups. A non-SIP Communication Manager supports TDM stations (for example, DCP, analog, BRI) and H.323 stations. TDM stations can be administered to port networks and branch (H.248) gateways. H.323 stations can register to Communication Manager through Processor Ethernet. Since no SIP signaling groups are supported on non-SIP-enabled Communication Manager (by definition), such systems do not support SIP stations.

Note that the only way endpoints administered to a non-SIP-enabled Communication Manager can talk to endpoints elsewhere in the enterprise is through non-SIP trunks to a Communication Manager administered as either a feature server or evolution server.

Additional non-IMS elements

Communication Manager administered as an evolution server and embedded in a branch gateway connects to Session Manager via non-IMS SIP trunks. Other SIP elements connected to Session Manager via non-IMS trunks include:

- SIP stations
- SIP service providers (optionally via session border controllers)
- SIP voice portals

- Avaya Aura® Conferencing Standard Edition
- Avaya Aura® Messaging
- Non-Avaya SIP gateways

Call types encountered in a Session Manager enterprise

For the purposes of identifying call flows and the corresponding Session Manager and Communication Manager SIP resources involved, the endpoints are consolidated into the following four categories:

- SIP stations

  SIP stations registered to Session Manager, using Communication Manager administered as either a feature server or an evolution server as feature source.
- Non-IMS SIP elements

  Non-SIP endpoints on a Communication Manager administered as an evolution server, endpoints on non-Avaya SIP gateways, SIP service providers, SIP voice portals, and Messaging
- Non-SIP Communication Manager

  Endpoints on non-SIP-enabled Communication Manager
- Non-SIP PSTN trunks

  Endpoints in the PSTN that are connected to Session Manager via non-SIP trunking (the case of SIP trunking is covered in non-IMS SIP elements)

The call flows associated with the various combinations of the preceding endpoint types are described in more detail in the examples.

Session Manager call types: Example 1

Example 1 describes calls between two SIP stations within the same Session Manager instance with the same Communication Manager administered as either a feature server or evolution server.

Call between two SIP stations with same Session Manager instance and same Communication Manager on page 147 shows the signaling flow associated with a call between two SIP stations registered to the same Session Manager instance, and using the same Communication Manager as a feature source.

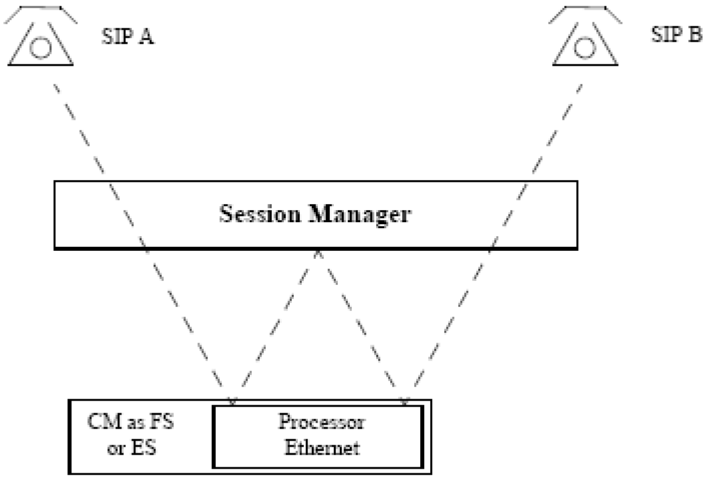


Figure 25: Call between two SIP stations with same Session Manager instance and same Communication Manager

The Session Manager resources associated with the call depicted in Figure 25: Call between two SIP stations with same Session Manager instance and same Communication Manager on page 147 include:

- 3 SIP sessions
  - SIP A - Session Manager - Communication Manager
  - Communication Manager - Session Manager - Communication Manager
  - Communication Manager - Session Manager - SIP B

Communication Manager resources associated with the call depicted in Figure 25: Call between two SIP stations with same Session Manager instance and same Communication Manager on page 147 include:

- 2 SIP trunk channels if evolution server; 4 SIP trunk channels if feature server
- CPU for 2 SIP trunk call legs if evolution server; CPU for 4 SIP trunk call legs if feature server

Session Manager call types: Example 2

Example 2 describes calls between two SIP stations within the same Session Manager instance with different Communication Managers administered as either a feature server or evolution server.

Call between two SIP stations with same Session Manager instance and different Communication Managers on page 148 shows the signaling flow associated with a call between two SIP stations registered to the same Session Manager instance and using different feature servers, different evolution servers, or one of each.

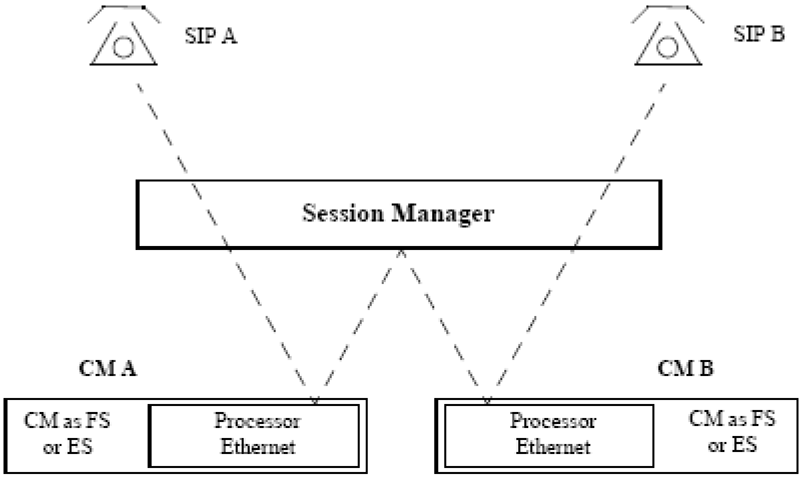


Figure 26: Call between two SIP stations with same Session Manager instance and different Communication Managers

Session Manager resources associated with the call depicted in Figure 26: Call between two SIP stations with same Session Manager instance and different Communication Managers on page 148 include:

- 3 SIP sessions
    - SIP A - Session Manager - Communication Manager
    - Communication Manager - Session Manager - Communication Manager
    - Communication Manager - Session Manager - SIP B

Communication Manager resources associated with each Communication Manager for the call depicted in Figure 26: Call between two SIP stations with same Session Manager instance and different Communication Managers on page 148 include:

- 2 SIP trunk channels (for either feature server or evolution server)
- CPU for 2 SIP trunk call legs (for either feature server or evolution server)

Session Manager call types: Example 3

Example 3 describes calls between two SIP stations within different Session Manager instances with the same Communication Manager administered as either a feature server or evolution server.

Call between two SIP stations with different Session Manager instances and same Communication Manager on page 149 shows the signaling flow associated with a call between two SIP stations registered to different Session Manager instances and using the same Communication Manager as a feature server.

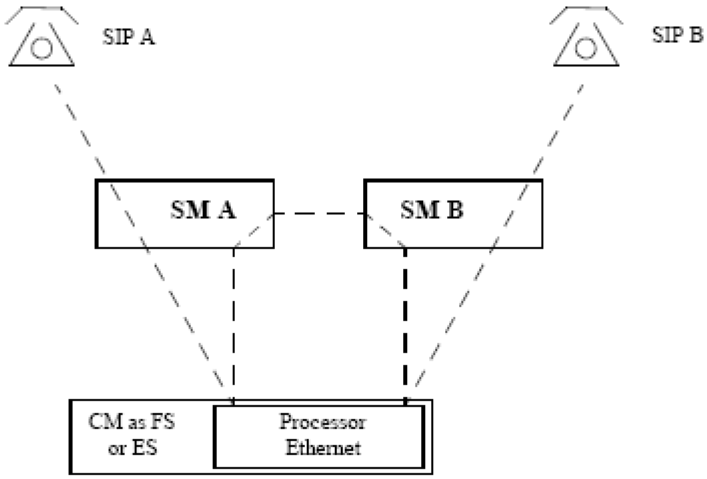


Figure 27: Call between two SIP stations with different Session Manager instances and same Communication Manager

Resources associated with each Session Manager instance for the call depicted in Figure 27: Call between two SIP stations with different Session Manager instances and same Communication Manager on page 149 include:

- 2 SIP sessions
  - SIP A or SIP B - Session Manager - Communication Manager
  - Communication Manager - one Session Manager - other Session Manager

Communication Manager resources associated with the call depicted in Figure 27: Call between two SIP stations with different Session Manager instances and same Communication Manager on page 149 include:

- 2 SIP trunk channels if evolution server; 4 SIP trunk channels if feature server
- CPU for 2 SIP trunk call legs if evolution server; CPU for 4 SIP trunk call legs if feature server

Session Manager call types: Example 4

Example 4 describes calls between two SIP stations within different Session Manager instances with different Communication Managers administered as either feature servers or evolution servers.

Call between two SIP stations with different Session Manager instances and same Communication Manager on page 148 shows the signaling flow associated with a call between two SIP stations registered to different Session Manager instances and using a different feature servers, different evolution servers, or one of each.

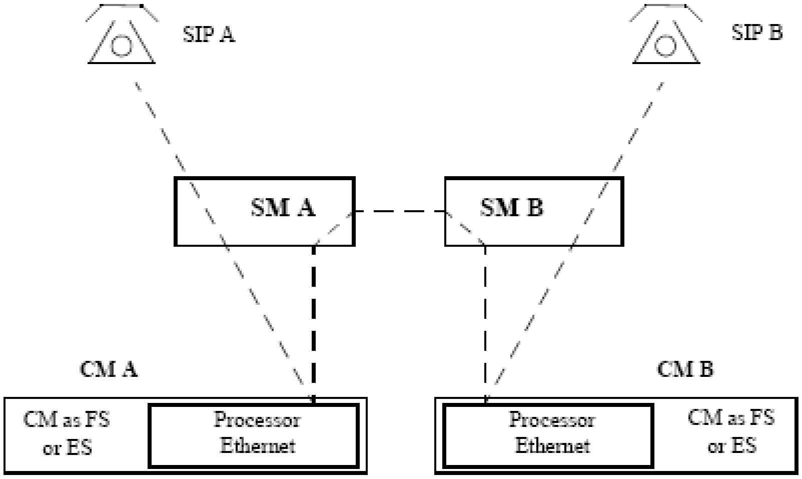


Figure 28: Call between two SIP stations with different Session Manager instances and different Communication Managers

Resources associated with each Session Manager instance for the call depicted in Session Manager call types: Example 3 on page 148 include:

- 2 SIP sessions
  - SIP A or SIP B - Session Manager - Communication Manager
  - Communication Manager - one Session Manager - other Session Manager

Communication Manager resources associated with each Communication Manager for the call depicted in Session Manager call types: Example 3 on page 148 include:

- 2 SIP trunk channels (for either feature server or evolution server)
- CPU for 2 SIP trunk call legs (for either feature server or evolution server)

Session Manager call types: Example 5

Example 5 describes calls between a SIP station and a non-IMS SIP element.

Call between a SIP station and a non-IMS SIP element on page 151 shows the signaling flow associated with a call between a SIP station and a non-IMS SIP element. Communication Manager is administered as either feature server or evolution server.

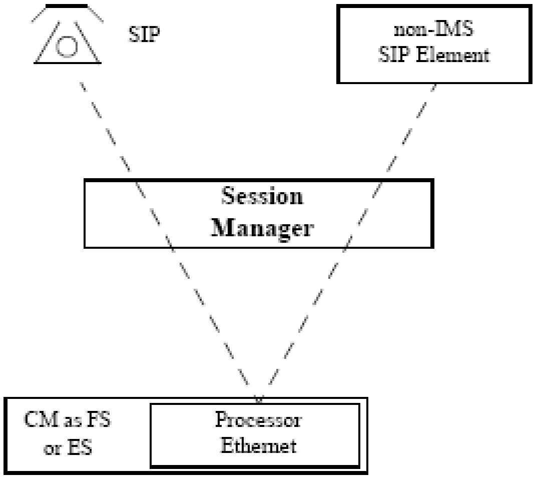


Figure 29: Call between a SIP station and a non-IMS SIP element

Session Manager resources associated with the call depicted in Figure 29: Call between a SIP station and a non-IMS SIP element on page 151 include:

- 2 SIP sessions
  - SIP - Session Manager - Communication Manager
  - Communication Manager - Session Manager - non-IMS SIP element

Communication Manager resources associated with the call depicted in Figure 29: Call between a SIP station and a non-IMS SIP element on page 151 include:

- Case 1

  Non-IMS SIP Element is a non-SIP endpoint on the same evolution server that's associated with the SIP station

  - 3 SIP trunk channels
  - CPU for 3 SIP trunk call legs and for 1 non-SIP call leg
- Case 2

  non-IMS SIP Element is a non-SIP endpoint on a different Communication Manager than the one that's associated with the SIP station or is any other type of non-IMS SIP element as defined at the beginning of the Call Types Encountered in an Session Manager Enterprise section.

  - 2 SIP trunk channels
  - CPU for 2 SIP trunk call legs

Session Manager call types: Example 6

Example 6 describes calls between a SIP station and a non-SIP Communication Manager or the PSTN. Communication Manager is administered as either feature server or evolution server.

Call between a SIP station and a non-SIP Communication Manager or The PSTN on page 152 shows the signaling flow associated with a call between a SIP station and a non-SIP Communication Manager or the PSTN.

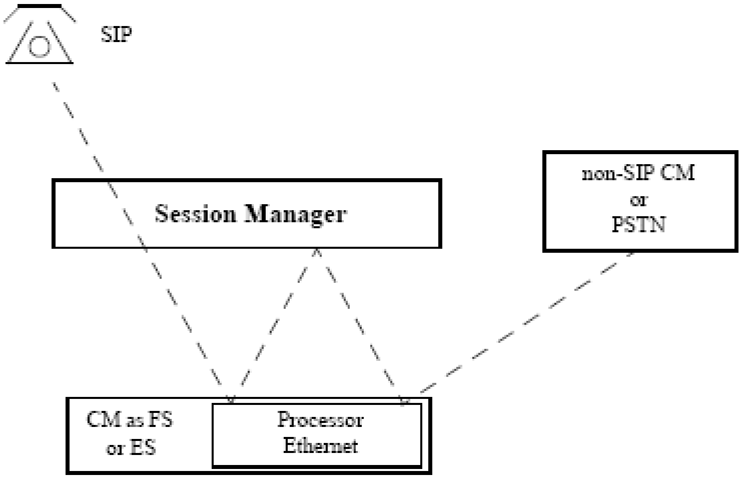


Figure 30: Call between a SIP station and a non-SIP Communication Manager or the PSTN

Session Manager resources associated with the call depicted in Figure 30: Call between a SIP station and a non-SIP Communication Manager or the PSTN on page 152 include:

- 2 SIP sessions
  - SIP - Session Manager - Communication Manager
  - Communication Manager - Session Manager - Communication Manager

Communication Manager resources associated with the call depicted in Figure 30: Call between a SIP station and a non-SIP Communication Manager or the PSTN on page 152 include:

- 3 SIP trunk channels
- 1 non-SIP trunk channel
- CPU for 3 SIP trunk call legs and for 1 non-SIP trunk call leg

> **Note:**
>
> Session Manager skips origination processing and application sequencing for emergency calling.

Session Manager call types: Example 7

Example 7 describes calls between two non-IMS SIP elements.

Call between two non-IMS SIP elements on page 153 shows the signaling flow associated with a call between two non-IMS SIP elements.

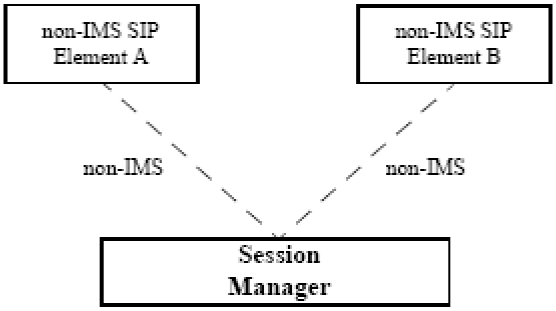


Figure 31: Call between two non-IMS SIP elements

Session Manager resources associated with the call depicted in Figure 31: Call between two non-IMS SIP elements on page 153 include

- 1 non-IMS - non-IMS SIP session
  - non-IMS SIP A - Session Manager - non-IMS SIP B

Session Manager call types: Example 8

Example 8 describes calls between a non-IMS SIP element and a non-SIP Communication Manager administered as either a feature server or evolution server.

Call between a non-IMS SIP element and a non-SIP Communication Manager on page 153 shows the signaling flow associated with a call between a non-IMS SIP Element and a non-SIP Communication Manager.

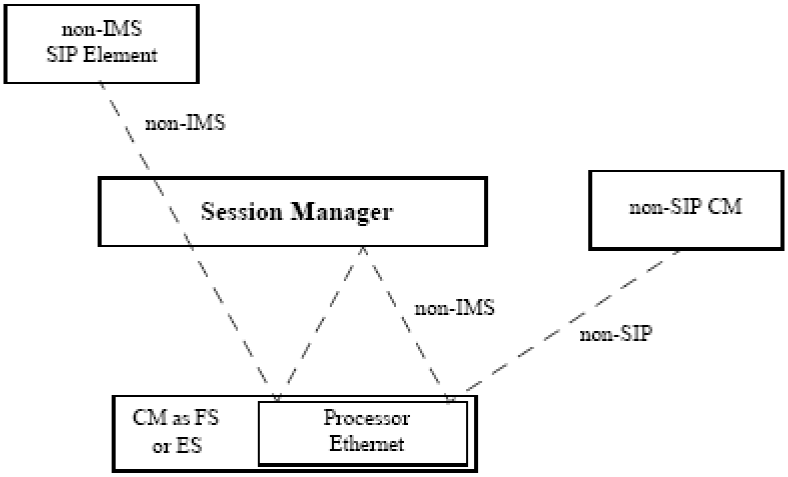


Figure 32: Call between a non-IMS SIP element and a non-SIP Communication Manager

Session Manager resources associated with the call depicted in Figure 32: Call between a non-IMS SIP element and a non-SIP Communication Manager on page 153 include:

- 2 SIP sessions
  - non-IMS SIP Element - Session Manager - Communication Manager
  - Communication Manager - Session Manager - Communication Manager

Note:

The signaling path from Session Manager to Communication Manager to Session Manager consists of two IMS SIP legs if Communication Manager is a feature server or two non-IMS legs if Communication Manager is an evolution server.

Communication Manager resources associated with the call depicted in Figure 32: Call between a non-IMS SIP element and a non-SIP Communication Manager on page 153 include:

- 3 SIP trunk channels
- 1 non-SIP trunk channel
- CPU for 3 SIP trunk call legs and for 1 SIP non-SIP trunk call leg

Session Manager call types: Example 9

Example 9 describes calls between two non-SIP Communication Managers administered as either feature servers or evolution servers.

Call between two non-SIP Communication Managers on page 154 shows the signaling flow associated with a call between two non-SIP Communication Manager.

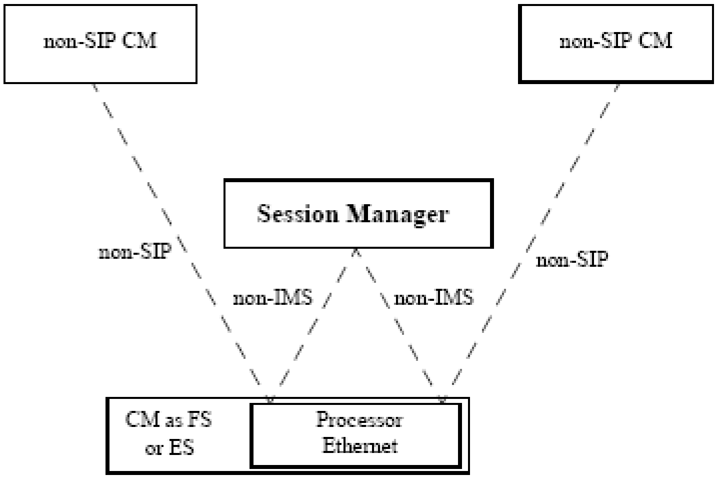


Figure 33: Call between two non-SIP Communication Managers

Session Manager resources associated with the call depicted in Figure 33: Call between two non-SIP Communication Managers on page 154 include:

- 1 non-IMS - non-IMS SIP session
    - Communication Manager - Session Manager - Communication Manager

Communication Manager resources associated with the call depicted in Figure 33: Call between two non-SIP Communication Managers on page 154 include:

- 2 SIP trunk channels
- 2 non-SIP trunk channels
- CPU for 2 SIP trunk call legs and for 2 non-SIP trunk call legs

Session Manager call types: Example 10

Example 10 describes calls between Communication Manager administered as an evolution server or a non-SIP Communication Manager and the PSTN.

We assume that the Communication Managers and non-SIP Communication Managers in a Session Manager enterprise supports their own non-SIP trunks directly to the PSTN.

Session Manager SIP sessions required per call for various call types on page 155 summarizes the number of SIP sessions involved per Session Manager instance for each of the calls described in the Call Types Encountered in an Session Manager Enterprise section.

Table 11: Session Manager SIP sessions required per call for various call types

Endpoints involved in the call	SIP sessions per SM
Two Avaya SIP stations registered to the same Session Manager instance, using the same Communication Manager administered as either a feature server or evolution server.	3
Two Avaya SIP stations registered to the same Session Manager instance, using different Communication Managers administered as either feature servers or evolution servers	3
Two Avaya SIP stations registered to different Session Manager instances, using the same Communication Manager administered as either a feature server or evolution server.	2
Two Avaya SIP stations registered to different Session Manager instances, using different Communication Managers administered as either feature servers or evolution servers	2
An Avaya SIP station and a non-IMS SIP element	2
An Avaya SIP station and a non-SIP Communication Manager or the PSTN	2
Two non-IMS SIP elements	1
A non-IMS SIP element and a non-SIP Communication Manager	2

Table continues…

Endpoints involved in the call	SIP sessions per SM
Two non-SIP Communication Managers	1
A Communication Manager as an access element or non-SIP Communication Managerand the PSTN via non-SIP trunks	—

Communication Manager core resources required per call for various call types on page 156 summarizes the number of SIP trunk channels per Communication Manager administered as either a feature server or evolution server, the number of SIP trunk call legs per Communication Manager administered as either a feature server or evolution server, and the number of non-SIP trunk call legs per Communication Manager administered as either a feature server or evolution server for each of the calls described in the Call Types Encountered in an Session Manager Enterprise section.

Table 12: Communication Manager core resources required per call for various call types

Endpoints involved in the call	SIP trunk call legs per FS or ES	Non-SIP trunk call legs per FS or ES
Two Avaya SIP stations registered to the same Session Manager instance, using the same core Communication Manager as a feature server	2 or 4[1]	NA
Two Avaya SIP stations registered to the same Session Manager instance, using different core Communication Managers as feature servers	2	NA
Two Avaya SIP stations registered to different Session Manager instances, using the same core Communication Manager as a feature server	2 or 4 [1]	NA
Two Avaya SIP stations registered to different Session Manager instances, using different core Communication Managers as feature servers	2	NA
An Avaya SIP station and a non-IMS SIP element	2 or 3[2]	0 or 1 [2]
An Avaya SIP station and a non-SIP Communication Manager or the PSTN	3	1
Two non-IMS SIP elements	NA	NA
A non-IMS SIP element and a non-SIP Communication Manager	3	1
Two non-SIP Communication Managers	2	2
A Communication Manager as access element or non-SIP Communication Manager and the PSTN via non-SIP trunks	NA	1

[1] SIP trunk channels per call if evolution server; 4 SIP trunk channels per call if feature server

[2] For a call between an Avaya SIP station and a non-IMS SIP element, the only time the larger numbers apply are when the non-IMS SIP element is a non-SIP endpoint on the same evolution server that is associated with the SIP station.

Each non-SIP Communication Manager involved in a call with another element in the Session Manager enterprise requires one non-SIP trunk channel for that call.

Engineering Session Manager instances

The two prominent performance-limiting factors associated with an Session Manager server are Session Manager server processing occupancy and memory constraints.

Session Manager processor occupancy is theoretically directly proportional to the rate at which Session Manager initiates and tears down SIP sessions. A SIP session consists of the signaling associated with a connection between two SIP trunks, communicating via a Session Manager instance. Session Manager SIP sessions required per call for various call types indicates that there is not generally a one-to-one correspondence between call and SIP session.

As a design criterion, the total occupancy (including the static occupancy) of the Session Manager server complex should not exceed 80%. That number is analogous to the 65% static + call-processing occupancy used in designing Communication Manager systems. The reason the design threshold is higher for Session Manager than Communication Manager is that Session Manager requires no processing cycles to be reserved for hardware maintenance activity.

Memory constraints establish a second, independent constraint, pertaining to the maximum number of simultaneous SIP sessions and the maximum number of TLS sockets supported by a single Session Manager instance.

Communication Manager traffic-engineering rules

This section discusses traffic-engineering rules associated with sizing various Communication Manager resources, including Communication Manager processor occupancy (which is directly related to BHCC capacities), Processor Ethernet interfaces, number of required gateways (for example, from a TDM timeslot perspective), trunk groups, media-processing resources, and TTR resources.

For detailed information about DSP usage and requirements, see *Avaya Aura® Communication Manager Reports*.

Processor occupancy and BHCC

The Busy Hour Call Attempt (BHCA) rate is the total number of calls attempted within that system during the busiest hour. This is distinct from the Busy Hour Call Completion (BHCC) rate, which counts only those calls that were actually completed. The BHCC rate determines the call capacity of a system.

In Communication Manager, processor occupancy, also known as server occupancy, consists of three main categories: static occupancy (ST), call processing occupancy (CP), and system management occupancy (SM).

Static occupancy: The processing required for keep-alive operations. Despite the nomenclature, the value of static occupancy in a List Measurements report can slightly vary.

Call processing occupancy: The processing required for setting up, maintaining, and tearing down calls, and for executing vectoring operations in call centers. The processor occupancy of Communication Release 6.3.6 and later for H323 RAS registration limit is 65% .

System management occupancy: The processing required for maintaining the sanity of the system, including periodic maintenance and audits. Due to the bursty nature of system management functions, a fixed portion of the overall processing capacity is allocated to system management for design purposes. For all Communication Manager servers, 27% of the total system processing capacity is assigned for system management. The 27% occupancy is not dedicated to system management but only used for traffic configuration calculations.

If the overall processor occupancy, ST + CP + SM, exceeds approximately 92%, all system management operations are temporarily delayed and subsequent call attempts are disallowed.

Therefore, the recommended total system processing occupancy is not more than 65%. That is, 100% - 27% for system management - 8% for the call throttling region.

Processing occupancy budgets for Communication Manager on page 158 shows the various occupancy budgets involved. To illustrate, the relationship between Communication Manager processor occupancy and the call rate is depicted as linear, although that is not always the case.

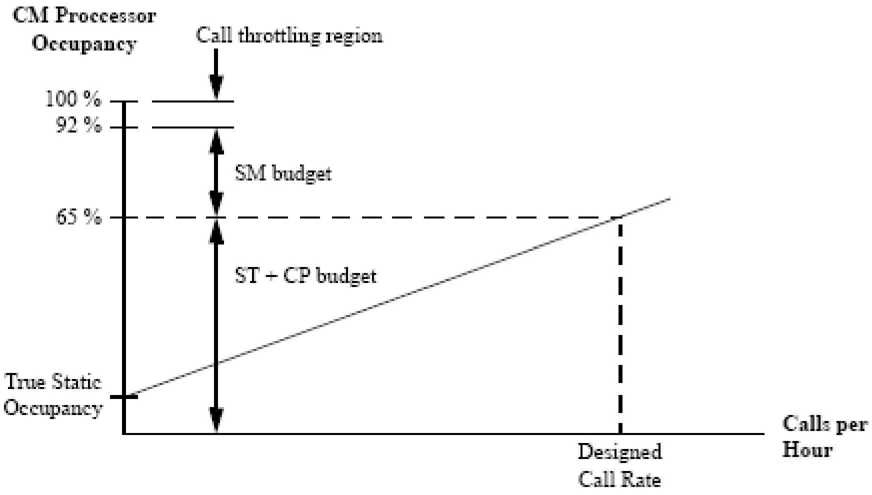


Figure 34: Processing occupancy budgets for Communication Manager

If the value of ST + CP occupancy is between 65% and 92%, some system management functions will be postponed to a quieter traffic period to allow static occupancy and call processing processes to use processor cycles from the system management budget. If the value of ST + CP occupancy exceeds 92%, all system management functions are suppressed and call throttling is initiated.

For more information, see *Avaya Aura® Call Center Elite Performance Report*.

Processor Ethernet

Processor Ethernet represents the interface by which IP endpoints, branch gateways, and adjuncts can register to Communication Manager.

The two primary considerations when engineering the required number of Processor Ethernet interfaces are registration and packet throughput. Registration considerations pertain to the maximum number of entities that can simultaneously reregister upon system failure. Packet throughput refers to the maximum number of simultaneous signaling connections supported by Processor Ethernet. For practical purposes, these two concepts can be considered independent of one another.

Registration considerations for adjuncts

Processor Ethernet can be used to support adjuncts and services such as Call Management System (CMS), Avaya Aura® Messaging, Call Detail Recording (CDR), DMCC-based recording, and Application Enablement Services (AES). The following adjuncts and services merit special allocation of the Processor Ethernet resources.

- A single Processor Ethernet interface can support up to two CMS applications.
- A single Processor Ethernet interface can support up to two CDR applications.
- A single Processor Ethernet interface can support up to 16 AES applications.

Required number of branch gateways

To size a given group of branch gateways, three pieces of information are needed:

- Total call usage (expressed in Erlangs) involving circuit-switched endpoints within the particular group of branch gateways. Designate this usage by u_{total} for the purposes of this discussion.
- Call usage (expressed in Erlangs) associated with calls between two circuit-switched endpoints within the particular group of branch gateways. Designate this usage by u_{tdm} for the purposes of this discussion.
- Maximum call usage (expressed in Erlangs) supported by a single branch gateway at the specified grade of service (GOS). Designate this usage by u_{GOS} for the purposes of this discussion. The value of u_{GOS} is determined by applying the Erlang B model to the number of time slot pairs available for bearer traffic and announcements and a specified GOS.
    - For a GOS of P001, use a value of u_{GOS} = 200.8 for G450 and a value of 193.3 for G430 Branch Gateway.
    - For a GOS of P000001 (essentially non-blocking), use a value of u_{GOS} = 175.1 for G450 and a value of 168.2 for G430 Branch Gateway.
    - The term u_{GOS} represents the maximum *port* usage (expressed in Erlangs) supported by a single branch gateway.

The number of port networks required for the given group of branch gateways is the smallest integer that is greater than or equal to the following formula:

$$\frac{(\mathrm{u}_{\mathrm{total}} + \mathrm{u}_{\mathrm{tdm}}) + \sqrt{(\mathrm{u}_{\mathrm{total}} + \mathrm{u}_{\mathrm{tdm}})^2 - 4\mathrm{u}_{\mathrm{tdm}}\mathrm{u}_{\mathrm{GOS}}}}{2\mathrm{u}_{\mathrm{GOS}}}$$

Related links

Topology on page 139
Erlang and ccs definitions on page 141
Endpoint usages on page 143
Erlang B and C models on page 142
Determining G450 Branch Gateway media resources on page 161
Determining G430 Branch Gateway media resources on page 160

Sizing of PSTN trunks

To size the PSTN trunks in a general business configuration, apply the Erlang B model to the PSTN call usage (expressed in Erlangs) and a P01 grade of service. For a call center, a reasonable rule of thumb is to multiply the number of agents by 1.4 to derive the number of trunks. However, a more rigorous approach is to apply the M/M/c/k Finite Queue model.

Sizing of media processing resources

For simplicity, the following default assumptions regarding media-processing usage is applied throughout this section:

- SIP–SIP two-party calls always use SIP direct media (that is, no media-processing resources are required)
- SIP–H.323 and H.323–H.323 two-party calls always shuffle (that is, one media-processing channel is required for the first 20 s of the call for each party)
- SIP–TDM and H.323–TDM two-party calls always require one media-processing channel on the gateway to which the TDM endpoint is administered for the entire call duration
- Intergateway TDM–TDM calls always require one media-processing channel on each gateway involved in the call for the entire call duration
- Intragateway TDM–TDM calls require no media-processing resources
- Multiparty (that is, 3-party or greater) calls cannot shuffle and, therefore, require media resources regardless of the types of endpoints involved. Call recorders and service-observing devices count as parties.

A system's media-processing resources can reside on any port network or branch gateway, and the rules for sizing those resources are contained in subsequent topics.

Determining G430 Branch Gateway media resources

About this task

A single G430 Branch Gateway can be configured to support up to 105 media-processing channels. You can use the following algorithm to determine the required number of G430 Branch Gateways to support the specified call usage.

Procedure

1. Determine the total call usage for media processing as follows:

   total usage = G.711 unencrypted CUR + G.711 encrypted CUR + G.729 unencrypted CUR + G.729 encrypted CUR + G.726 CUR + unencrypted T.38 fax and modem over IP CUR

2. Determine the required number of media processing channels:

   Apply an Erlang formula (mixed Erlang B / C is ideal, but pure Erlang B would also work) to the total usage and a suitable Grade of Service (for example, P001) to obtain the total number of media processing channels required.

3. Determine the required number of media processing channels.
4. Divide that number by 105 and round up to get the required number of G430 Branch Gateways.

Related links

Determining G450 Branch Gateway media resources on page 161

Topology on page 139

Erlang and ccs definitions on page 141

Endpoint usages on page 143

Erlang B and C models on page 142

Required number of branch gateways on page 159

Determining G450 Branch Gateway media resources

About this task

A single G450 Branch Gateway can be configured to support up to 320 media-processing channels. You can use the following algorithm to determine the required number of G450 Branch Gateways to support the specified call usage.

Procedure

1. Determine the total call usage for media processing as follows:

   total usage = G.711 unencrypted CUR + G.711 encrypted CUR + G.729 unencrypted CUR + G.729 encrypted CUR + G.726 CUR + unencrypted T.38 fax and modem over IP CUR

2. Determine the required number of media processing channels:

   Apply an Erlang formula (mixed Erlang B / C is ideal, but pure Erlang B would also work) to the total usage and a suitable Grade of Service (for example, P001) to obtain the total number of media processing channels required.

3. Determine the required number of media processing channels.
4. Divide that number by 320 and round up to get the required number of G450 Branch Gateways.

Related links

Determining G430 Branch Gateway media resources on page 160
Topology on page 139
Erlang and ccs definitions on page 141
Endpoint usages on page 143
Erlang B and C models on page 142
Required number of branch gateways on page 159

Touch tone receivers

When a station user goes off-hook, Communication Manager assigns an available time slot and a touch tone receiver (TTR) that listens to that time slot. The TTR collects the digits, formats a message, and sends the message uplink to the Communication Manager server. Communication Manager sends a downlink message to disconnect the TTR after all the digits have been collected.

For all intercom and auto route selection (ARS) trunk calls, the port on the Tone Detector circuit pack is released immediately when the last digit is dialed. In the case of non-ARS calls (operator-assisted calls, international calls, credit card calls) where the number of digits in a call may be unknown, there is a 10-s time-out period after each digit. If no new digit is generated during this time-out period, the port on the Tone Detector circuit pack is disconnected from the calling station.

If all TTRs in the system are busy, the request is put in a queue. The event of a full queue is treated as an error and results in intercept treatment; that is, a reorder tone is returned to the caller.

TTRs are used to collect digits from the following originating endpoints:

- analog sets
- DCP sets
- DS1 OPS (line-side T1)
- DS1 OPS (line-side E1)
- BRI sets
- analog trunks
- RBS digital trunks (T1)
- CAS digital trunks (E1)

TTRs are *not* used to collect digits from the following originating endpoints:

- IP telephones and trunks
- SIP telephones and trunks
- PRI T1 trunks
- PRI E1 trunks

TTR resources are determined by the originating station or trunk. For an outbound PSTN call, its TTR resource must reside in the same port network or branch gateway as the originating station, which is not necessarily the same port network or branch gateway as the trunk. IP or SIP endpoints do not need the use of a TTR. Incoming DID calls that do not use touch-tone dialing do not require TTRs. Incoming PRI calls that use authorization codes *do* require TTRs.

TTRs are engineered to 0.001 blocking using the blocked calls cleared model. This is conservative in that there is a small (4 entries) buffer for calls who find all TTRs busy.

Default holding time values for the different calls can be obtained by multiplying the number of digits in the call by 0.65 s and adding 3 s, which represents the period from off-hook to the first digit. The TTR usage, expressed in Erlangs, is calculated by multiplying the TTR holding time by the calls per hour, then dividing by 3600. The Erlang B formula with a P001 grade of service is then used to determine the required number of TTR resources. Each G430 branch gateway supports 32 TTR resources, and each G450 branch gateway supports 64 TTR resources. The TTR resources on a port network are scalable through the use of various circuit packs supporting TTR.

IP network bandwidth requirements

There are two general categories of bandwidth requirements: the bandwidth to support the media, and the bandwidth to support the signaling.

Media bandwidth

An IP packet consists of a payload and some amount of overhead, where the payload consists of actual sampled voice, and the overhead represents headers and trailers, which serve to navigate the packet to its proper destination. The overhead due to IP, UDP, and RTP is 40 bytes, while the Ethernet overhead is between 18 and 22 bytes (18 is assumed in this discussion). This represents a total overhead of 58 bytes (464 bits), regardless of the nature of the payload. For this example, Layer 2 (Ethernet) overhead has been included in that total. At every router boundary, because we have included Ethernet overhead in this example, our calculations are for bandwidth on a LAN. As WAN protocol (for example, ppp) Layer 2 headers are generally smaller than Ethernet headers, WAN bandwidth is typically less than LAN bandwidth.

The size of the payload depends upon certain parameters relating to the codec being used. The two most common codecs used with Communication Manager products are (uncompressed) G.711 and (compressed) G.729. The transmission rates associated with those codecs are 64 kbps for G.711 (this is the Nyquist sampling rate for human voice) and 8 kbps for G.729.

The packet size is sometimes expressed in units of time (specifically, in milliseconds). The following formula yields the packet size, expressed in bits:

number of bits of payload per packet = transmission rate (kbps) x milliseconds per packet

Payload size per packet on page 164, which has been populated using this formula, provides the payload size per packet (expressed in bits), as a function of packet size (milliseconds per packet) and codec:

Table 13: Payload size per packet

Packet Size	G.711	G.729
10 ms	640 bits	80 bits
20 ms	1280 bits	160 bits
30 ms	1920 bits	240 bits
60 ms	3840 bits	480 bits

Note that the number of bits of payload per packet depends on the packet size, but it is independent of the sizes of the individual frames contained in that packet. For example, a packet size of 60 ms could be referring to six 10-ms frames per packet, or three 20-ms frames per packet, or two 30-ms frames per packet. Presently, the most commonly-used packet sizes are 20 ms. Both G.711 and G.729 codecs typically utilize two 10-ms frames per packet.

As stated earlier, there is typically an overhead of 464 bits per packet in a LAN scenario. So, the bandwidth (expressed in kbps) associated with a unidirectional media stream (assuming no Silence Suppression is used) is augmented from 64 kbps and 8 kbps (for G.711 and G.729, respectively) to account for this overhead. The results of this exercise are provided in the Typical LAN bandwidth requirements for media streams on page 164:

Table 14: Typical LAN bandwidth requirements for media streams

Packet Size	G.711	G.729
10 ms	110.4 kbps	54.4 kbps
20 ms	87.2 kbps	31.2 kbps
30 ms	79.5 kbps	23.5 kbps
60 ms	71.7 kbps	15.7 kbps

The kilobits per second values in Typical LAN bandwidth requirements for media streams on page 164 were calculated by multiplying the transmission rate by the ratio of the total bits per packet (payload plus overhead) to the payload bits per packet. For example, for the G.711 codec, 20–ms packets, and 58 bytes of overhead per packet, the bandwidth per call is

(64 kbps)[(1280 + 464) / 1280] = 87.2 kbps

Note that the entries in Typical LAN bandwidth requirements for media streams on page 164 correspond with *unidirectional* media streams. A *full-duplex* connection with a kilobits per second capacity at least as large as the number in one of the table cells would be sufficient for carrying a two-way voice stream using the corresponding codec, packet size, and packet overhead. In other words, a full-duplex connection with a particular capacity rating would support enough bandwidth to carry that capacity in both directions. Alternatively, two half-duplex connections of the same capacity rating could be used.

99.9th percentile traffic

The call usage (expressed in Erlangs) between two facilities represents the *average* number of simultaneous bidirectional media streams between those facilities. For example, if the call usage between two facilities is 100 Erlangs, then the average number of simultaneous calls is 100. However, since this is only an average, roughly 50% of the time there are more than 100 simultaneous active calls. So, it would be a mistake to simply multiply 100 media streams by the appropriate value for kbps per stream.

The goal is to supply enough bandwidth to adequately support the media streams at least 99.9% of the time. Given a call usage, the Erlang B model is used to estimate the 99.9th percentile value for the number of simultaneous streams. For example, if the call usage rate is 100 Erlangs, the Erlang B model implies that there are at least 128 simultaneous media streams less than 0.1% of the time. So, in that example, it is sufficient to engineer the bandwidth to support 128 simultaneous media streams.

Once you determine the 99.9th percentile for the number of simultaneous media streams, it can be converted to kilobits per second by using the numbers in Typical LAN bandwidth requirements for media streams on page 164. For example, for a typical LAN configuration, the G.711 codec, and a packet size of 20 ms, Typical LAN bandwidth requirements for media streams on page 164 implies that 87.2 kbps are required per call. In that case, the required bandwidth would be 87.2 kbps x 128 = 11.2 Mbps in each direction.

Call Admission Control

A Call Admission Control (CAC) limit can be administered to any pair of Communication Manager network regions, and it can be specified as either the maximum number of simultaneous calls between the two network regions or the maximum bandwidth usage between the two network regions. Numbers such as 128 maximum simultaneous calls or 11.2 Mbps derived in the example in the previous section could serve as effective lower bounds for CAC limits.

Provisioning Session Manager and Communication Manager CAC together

For simultaneous use of Session Manager and Communication Manager CAC, following configurations should be done:

1. Create 1-to-1 mapping of Session Manager Locations to Communication Manager Network Regions, because Communication Manager uses Network Regions for CAC. This is limited by the fact that Communication Manager supports no more than 250 Network Regions for small and medium platforms and 2000 Network Regions for large platforms, while Session Manager supports thousands of Locations.
2. As Session Manager maps IP addresses to Locations, Communication Manager maps IP addresses to Network Regions. These mappings must be synchronized manually.
3. As part of Communication Manager administration, the SIP trunk from Communication Manager must be placed within a dummy Network Region for which no CAC limits are set.

This enables the following changes:

- Calls terminated to non-SIP destinations (H.323 phones, non-SIP trunks) are counted by Communication Manager CAC for the appropriate Network Regions.

- All calls terminated to SIP destinations (SIP phones, SIP trunks on Session Manager) are counted by Session Manager CAC for the appropriate Locations.
- SIP trunks on Communication Manager that do not route to Session Manager (not a recommended configuration) are counted by Communication Manager.

Note:

Communication Manager performs CAC in terms of bandwidth limits between two specific Network Regions, while Session Manager performs CAC as per limits covering all traffic into or out of a Location, regardless of the far-end location.

IGAR and traffic engineering

Inter-Gateway Alternate Routing (IGAR) provides alternative routing over the PSTN for inter gateway calls that would otherwise be precluded from traversing the IP network. Communication Manager offers the capability to use H.323 and SIP trunks in the alternative routes. The reasons for an intergateway call to be rerouted over the PSTN include:

1. The Call Admission Control limit for the link in question was already reached
2. VoIP RTP resources are unavailable
3. The parties on the call are members of incompatible (in the sense of codec) network regions
4. The call was forcibly redirected over the PSTN for testing or debugging purposes

Dial Plan Transparency is somewhat similar to IGAR in that calls whose primary routes are through IP networks are rerouted through the PSTN. However, IGAR applies only to intra-Communication Manager calls, and Dial Plan Transparency applies only to inter-Communication Manager calls. For example, consider a Communication Manager system in which endpoints in two distinct geographic sites can only talk to each other via a particular WAN or via the PSTN. Suppose that the WAN is lost because of a failure, and that the main server complex is coresident with one of the two sites. In that case, the other site must have a survivable core or remote server to keep the endpoints in that site active. In such a scenario, the call in question becomes an inter-Communication Manager call (that is, a call between an endpoint controlled by the main server and an endpoint controlled by a survivable server), and could be rerouted through the PSTN through the use of Dial Plan Transparency. IGAR would not apply to such a scenario.

When engineering a configuration supporting IGAR or Dial Plan Transparency, it is important to engineer the PSTN trunks to be able to support the traffic that would be rerouted if IGAR or Dial Plan Transparency was invoked. For example, if Dial Plan Transparency is being used to provide inter-site connectivity over the PSTN in the event of a WAN failure, the PSTN trunks in both sites should be engineered to an appropriate grade of service, assuming the PSTN call usage includes all of the traffic that would be rerouted pursuant to a WAN failure. For more information see Sizing of PSTN trunks.

Signaling bandwidth

The signaling bandwidth is normally considerably smaller than the corresponding media bandwidth. However, we often must estimate it, especially in SIP configurations and when separating the bearer and signaling network. Two components typically make up signaling bandwidth:

- Bandwidth supporting keep-alive signaling
- Bandwidth supporting per-call signaling.

The value of the keep-alive signaling and per-call signaling associated with a particular configuration depends on the types of endpoints and gateways involved and must be determined empirically. Once we determine the per-call signaling bandwidth for the various call types involved, those values are multiplied by the corresponding call rates, and those results are then added together.

We can then apply the Erlang B formula with a P001 grade of service to determine the 99.9th percentile bandwidth. See 99.9th percentile traffic on page 165.

Chapter 10: Resources

Documentation

The following table lists the documents related to the components of Avaya Aura® Release 10.2.x. Download the documents from the Avaya Support website at https://support.avaya.com.

Title	Description	Audience
Implementation		
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy the Avaya Aura® System Manager application in a virtualized environment.	Implementation personnel
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy the Avaya Aura® System Manager application in a software only and Infrastructure as a Service Environments	Implementation personnel
Upgrading Avaya Aura® System Manager	Upgrade the Avaya Aura® System Manager application.	System administrators and IT personnel
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager in virtualized environment.	Implementation personnel
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager in a software only and Infrastructure as a Service environments.	Implementation personnel
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	System administrators and IT personnel
Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Implementation personnel
Deploying Avaya Aura® Session Manager in Software-Only and Infrastructure as a Service Environment	Describes how to deploy the Session Manager in a software only and Infrastructure as a Service environments.	Implementation personnel

Table continues…

Title	Description	Audience
Upgrading Avaya Aura® Session Manager	Provides common administration scenarios.	System administrators and IT personnel
Deploying Avaya Aura® Application Enablement Services in Virtualized Environment	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments	Deploy Application Enablement Services applications in a software only and Infrastructure as a Service environments.	Implementation personnel
Upgrading Avaya Aura® Application Enablement Services	Upgrading Application Enablement Services applications.	System administrators and IT personnel
Administration		
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network components of Communication Manager, such as gateways, trunks, FAX, modem, TTY, and Clear-Channel calls.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® Communication Manager	Describes the procedures and screens used for administering Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® System Manager	Describes the procedures for configuring System Manager Release 10.2.x and the Avaya Aura® applications and systems managed by System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Avaya Aura® Presence Services Snap-in Reference	Describes the steps to deploy and configure Presence Services.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches on Avaya Aura® applications.	System administrators
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Table continues…

Title	Description	Audience
Avaya Aura® Communication Manager Screen Reference	Describes the screen and detailed field descriptions of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® Session Manager	Describes how to administer Session Manager by using System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Planning for Deploying Avaya Aura® applications	Provides planning information for deploying Avaya Aura® applications on supported platforms.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Planning for Upgrading Avaya Aura® applications	Provides planning information for upgrading Avaya Aura® applications on supported platforms.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Maintenance and Troubleshooting		
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateway and Servers	Provides commands to monitor, test, and maintain hardware components of Avaya servers and gateways.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Training

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

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components

Table continues…

Course code	Course title
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.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at https://support.avaya.com and log in.
2. On the top of the page, in **Search Product**, type the product name.

   The Avaya Support website displays the product name.
3. Select the required product name.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. On the product page, click **Product Documents**.
6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.
7. Select the appropriate filters as per your search requirement.

   For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new service packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to https://support.avaya.com and search for “Guide to Managing Your Avaya Access Profile for Customers and Partners”.

   Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.

2. Set up e-notifications.

   For detailed information, see the **Subscribe to E-Notifications** procedure.

Index