Avaya Aura® Session Manager Overview and Specification

Release 6.3
Issue 5
December 2014

© 2014 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

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

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

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Copyright

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

Third Party Components

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

Virtualization

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United

States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

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

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, 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 Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 6
Purpose 6
Intended audience 6
Document changes since last issue 6
Related resources 6
Documentation 6
Training 8
Viewing Avaya Mentor videos 9
Support 9
Warranty 10
Chapter 2: Avaya Aura® Session Manager overview 11
Feature description 11
Policy-based routing 12
Centralized applications 12
SIP Proxy and Registrar functionality 12
Normalization of disparate networks 12
Application Sequencing 12
Personal Profile Manager 13
Centralized SIP trunking 13
Call Detail Recording on Session Manager 14
Security enhancements: Removal of Default Certificates 14
Security enhancements: NIST Support 15
Transport Layer Security 16
Session Manager Scale increases 16
Online/Offline Call Journal (Call History) 17
System Manager Web Services 17
SIP Phone Configuration template 18
Limit Number of Concurrent Calls for SIP endpoints 19
Inter-gateway Alternate Routing for SIP endpoints 20
Feature pack to release mapping 21
Supported servers 21
Chapter 3: What's new in Session Manager 22
SIP Endpoint Concentrator Connection Policy 22
Role Based Access Control Permission restoral 23
Chapter 4: Interoperability 24
Product compatibility 24
Supported Avaya endpoints 24
Deployment options 26
Operating system compatibility 27

Third-Party PBX Integration..... 27
Chapter 5: Performance and capacity specifications..... 28
Capacity and scalability specification..... 28
Alternative H.323 Endpoint administration considerations and impacts..... 31
Dial plan specification..... 32
Tail end hop off..... 32
Call Admission Control specification..... 33
Redundancy and high availability..... 33
Survivable Core..... 35
Survivable Remote..... 35
Chapter 6: Security..... 36
Security specification..... 36
Port assignments..... 36
Chapter 7: Licensing requirements..... 37
Glossary..... 38

Chapter 1: Introduction

Purpose

This document describes tested Avaya Aura® Session Manager characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Intended audience

This document is intended for people who want to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations.

Document changes since last issue

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

- Added information regarding an alternative method for administering H.323 endpoints and how the method affects the number of SIP devices.

Related resources

Documentation

The following documents are available at http://support.avaya.com.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		

Title	Description	Audience
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management System administrators
Avaya Aura® Virtualized Environment Solution Description	Describes the Avaya Virtualized Environment, design considerations, topology, and resources requirements.	Sales engineers Implementation engineers Support personnel
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager 6.3.x Release Notes	Contains enhancements, fixes, and workarounds for the various Session Manager 6.3 releases.	System administrators Services and support personnel
Implementation		
Deploying Avaya Aura® Session Manager	Describes how to install and configure a Session Manager instance.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager.	Services and support personnel
Deploying Avaya Aura® Communication Manager on System Platform	Describes how to install the appropriate Communication Manager template, including Branch Session Manager, on the server.	Services and support personnel
Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment	Describes how to deploy the Session Manager virtual application in a VMware environment.	Services and support personnel
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides common administration scenarios.	System administrators
Installation and upgrades		
Installing Service Packs for Avaya Aura® Session Manager	Describes the procedures to install service packs on Session Manager.	Services and support personnel
Installing Patches for Avaya Aura® Session Manager	Describes the procedures to install patches on Session Manager.	Services and support personnel

Title	Description	Audience
Installing the Avaya S8800 Server for Avaya Aura® Communication Manager	Describes the installation procedures for the S8800 Server.	Services and support personnel
Installing the Avaya S8510 Server Family and Its Components	Describes the installation procedures for the S8510 Server.	Services and support personnel
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620server.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade a Session Manager to the latest software release.	Services and support personnel
Maintaining		
Maintaining and Troubleshooting Avaya Aura® Session Manager	Describes the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Training

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

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Avaya Aura® Session Manager 6.2 Delta Overview
5U00104W	Avaya Aura® Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Avaya Aura® Session Manager General Overview

Course code	Course title
ATC00175OEN	Avaya Aura® Session Manager Rack and Stack
ATU00170OEN	Avaya Aura® Session Manager Technical Overview
ATC01840OEN	Survivable Remote Avaya Aura® Session Manager Administration
3U00100O	Designing Avaya Aura 6.2 Part 1
3U00101O	Designing Avaya Aura 6.2 Part 2

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.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

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

Warranty

Avaya provides a 90-day limited warranty on Session Manager. For more information about the terms of the limited warranty, see the sales agreement or other applicable documentation . In addition, see the standard warranty and details about Session Manager support during the warranty period on the Avaya Support website at https://support.avaya.com under **Help & Policies> Policies & Legal > Maintenance and Warranty Information**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: Avaya Aura® Session Manager overview

Avaya Aura® Session Manager is a SIP routing and integration tool. Session Manager integrates all SIP devices across the entire enterprise network within a company and leverages the existing PBX infrastructure.

Feature description

Session Manager integrates and simplifies the existing communication infrastructure, combining existing PBXs and other communications systems, regardless of the vendor, into a cohesive, centrally managed, SIP-based communications network.

Specifically, Session Manager:

- integrates with third-party equipment and endpoints to normalize disparate networks.
- Provides centralized routing of calls using an enterprise wide numbering plan.
- Offers centralized management through System Manager, including configuration of user profiles and efficient deployment of enterprise-wide centralized applications.
- Interconnects Communication Manager and Avaya Communication Server 1000 and provides multiple feature support for SIP and non-SIP endpoints.
- Enables third-party E911 emergency call service for enterprise users.
- Centralizes Presence Services, providing scale and reduced network complexity with a variety of endpoints and communication servers.
- Supports converged voice and video bandwidth management.
- Provides application sequencing capability, enabling incremental application deployments without PBX upgrades.
- Provides outstanding geographic redundancy.
- Provides mobility of SIP telephones and enterprise mobility for SIP users.

Policy-based routing

Customers can use Session Managerto define the routing policy. The routing policy controls when calls are made, how the call load is balanced, and how calls are routed during network failures.

- **Least-cost routing**, also called time-of-day routing, uses the lowest cost route from a list of service providers on a time-of-day or time-of-week basis.
- **Alternate routing** routes calls around network failures on a global basis and uses global PSTN fallback when the internal network is unavailable.
- **Load balancing** distributes calls. For a given SIP entity, you can administer Session Manager to select a host from multiple IP addresses based on administered priorities and weights.
- **Call admission control** reroutes calls when the bandwidth allocation for WAN link is exceeded.

Centralized applications

Session Manager provides connectivity for centralized Avaya applications such as Avaya Aura® Messaging, Avaya Voice Portal, and Avaya Meeting Exchange™. Each PBX, gateway, or location connects to the centralized application through Session Manager rather than individually. Session Manager also connects to SIP-enabled adjuncts, making the management and deployment of adjuncts much simpler than methods where each PBX connects to its own adjunct.

SIP Proxy and Registrar functionality

Session Manager functions as the SIP Proxy and Registrar server of the enterprise network.

Normalization of disparate networks

Session Manager normalizes and adapts disparate SIP protocols to meet the strict SIP standards of the network. With normalization of disparate networks, third-party PBXs work with each other and with Avaya equipment enabling customers to realize true vendor interoperability.

For example, Cisco and other PBXs can connect with Session Manager and operate with each other and with Avaya equipment. Session Manager converts the headers in SIP messages that display calling and called-party information in the format required by each switch in a call.

Application Sequencing

With Application Sequencing, you can define and manage a set of applications for call sequencing based on the communication profile of the user. Each application in a sequence processes all

requests to deny, modify, or forward initial SIP requests. Some examples of sequenced applications are:

- Billing Service
- Voice Monitoring
- Communication Manager Feature Server
- Call Blocker
- Personal assistant
- Meeting Coordinator

Session Manager also supports third-party PBX endpoint application sequencing. Typical applications include blocking calls based on user preferences, redirecting calls to users in the Avaya Aura® enterprise, and augmenting caller identification information for incoming and outgoing calls. You can enable Application Sequencing without needing to upgrade or modify the code on existing third-party PBX equipment. For more information about Application Sequencing, see *Administering Avaya Aura® Session Manager*.

Enhanced Session Manager Application Sequencing

Starting with Session ManagerRelease 6.3.8, implicit sequencing definitions can be applied to SIP users.

Avaya recommends that customers segregate the Implicit User applications from the Explicit User applications. SIP users are administered as Explicit Users. Non-SIP users are administered as Implicit Users. Unless the enterprise SIP users and non-SIP users have completely different number prefixes, customers might see inadvertent Implicit User applications invocation for the SIP users. To avoid such issues, the implicit sequencing definition for SIP users feature is disabled by default.

Personal Profile Manager

The Personal Profile Manager (PPM) maintains and manages the personal information of the end user in the system. SIP endpoints communicate with PPM to:

- retrieve configuration information such as dial plans, buttons, and contact lists.
- add or update contacts.
- save device-specific data.

The PPM provides an interface for endpoints to attach to the network to download profile data and store data back in the network for easy access across multiple user devices.

Centralized SIP trunking

Centralized SIP trunking routes all network traffic, including branch site traffic, through the enterprise core site. Session Manager provides redundant connections to a SIP service provider using the Gateway or Session Border Controller (SBC).

Customers can use centralized SIP trunking to save on operational costs. However, the setup should have more than one hub-site to avoid the risk of a single point of failure.

Call Detail Recording on Session Manager

The Call Detail Recording (CDR) feature records information on calls. When you enable CDR, the CDR records are saved in a special directory on the local hard drive of the server.

The call record contains information regarding:

- The time of the call
- The duration of the call
- The dialed number
- The calling party
- The terminating SIP entity
- The originating SIP entity
- The bandwidth indicator

For each Session Manager, you can administer CDR as either disabled or enabled. CDR records are created if you enable the CDR in at least one of two Session Manager entities.

Note:

Survivable Remote Session Manager (Branch Session Manager) does not support CDR.

CDR records on Session Manager are created on connected calls.

In route-through scenarios, where one Session Manager routes directly to another Session Manager, CDR is generated only on the originating Session Manager if so administered, not on the terminating Session Manager.

For sequenced applications (implicit or administered for a user), only one CDR record is generated for a given call.

If the secondary Session Manager of a user receives a call, the call is routed to the primary Session Manager of the user as per user registration. In that case, the CDR is still generated on the secondary Session Manager and not on the primary Session Manager.

Security enhancements: Removal of Default Certificates

Starting with Session Manager Release 6.3.8, default certificates are no longer supported for new installations. Default certificates, also known as demo certificates, are non-unique identity certificates which were automatically installed on newly shipped Session Manager servers. Default certificates are not secure and do not meet current NIST standards (SHA–256 hashing and 2048–bit RSA keys).

New Session Manager servers no longer use the default certificates that were Avaya SIP Product CA issued. New customer networks can request an Identity Certificate from the System Manager Trust Management that is signed by the System Manager Certificate Authority.

For upgrades, Session Manager preserves the previous certificate. If a demo certificate was in use in the previous release, the certificate is preserved through the upgrade.

Existing customers who either need to replace a Session Manager server or want to add a Session Manager to an existing network of Session Managers can download old certificates. However, Avaya recommends that customers use the newer certificates as soon as possible.

To manage certificates:

- Use the new Identity Certificate issued by System Manager (default).
- Use third-party ID certificates.

Security enhancements: NIST Support

The National Institute of Standards and Technology (NIST) develops cryptographic standards for the United States government. NIST recommends that starting in 2014, the digital signatures of Identity Certificates use the SHA–2 signing algorithm and 2048–bit encryption keys. NIST requires at least 2048 bit keys. Customers have the option to create larger keys, such as 4096.

Starting with Release 6.3.8, Session Manager:

- uses SHA–256 and 2048–bit RSA keys for signing new Identity Certificates by default.
- uses SHA–512 for passwords.

A new Connection filter, **Non-Compliant NIST TLS Only:**, helps users identify non-NIST compliant connections. The filter appears on the Security Module Status page. New fields on the page include:

- **Cert Sign**
- **Key Exch**
- **Encryption**
- **MAC**
- **TLS Version**

These fields display the following status for NIST SP800–131a compliance:

- **Acceptable**
- **Deprecated**
- **Disallowed**
- **Not Approved**
- **Restricted**
- **Unknown**

Transport Layer Security

Session Manager Release 6.3.8 supports Transport Layer Security (TLS) 1.2.

TLS 1.2 provides:

- a higher level of security than earlier versions to protect users from known attacks.
- flexibility for defining cryptography algorithms.

The TLS protocol provides three essential services to all applications running above it: encryption, authentication, and data integrity.

By default, Session Manager uses TLS 1.2. If the other end of the connection cannot use TLS 1.2, Session Manager reverts to TLS 1.0.

You can view the TLS version on the Connection Status page in the **Transport** field.

Session Manager Scale increases

For Avaya Common Servers Release 1, HP supplies the HP ProLiant DL360 G7 servers and Dell provides the Dell™ PowerEdge™ R610 servers.

For Avaya Common Servers Release 2, HP supplies the HP ProLiant DL360p G8 servers and Dell supplies the Dell™ PowerEdge™ R620 servers.

Using an Avaya Common Servers R2 server, you can significantly increase the capacity of a single Session Manager. A VMware footprint identifies the capacities of the R2 server.

A distinction no longer exists between SIP users and SIP devices. Instead, only SIP devices are used for determining Session Manager capacities. Capacities decrease in scenarios where a device has a larger impact than a typical device. For example, Call Center Agents subscribe to an additional package.

Session Manager on Common Server R1 supports:

- 10,000 SIP users during normal operations
- a maximum of 12,000 SIP users in a failover scenario
- 100 sessions per second (360K per hour)
- 90K simultaneous sessions

Session Manager on a Common R2 Server supports:

- 21,500 SIP devices during normal operations
- a maximum of 25,000 SIP devices in a failover scenario
- 150 sessions per second (540K sessions per hour)
- 160K simultaneous sessions

A Session Manager configuration supports up to 12 interconnected Session Managers.

Up to 125K SIP users or 150K SIP devices are supported by any N+M sparing Session Manager configuration consisting of Common Server R2 or comparably sized VMware servers. The customer must adequately distribute devices across primary and secondary servers to accommodate the configuration. For example, the typical Session Manager solution with N+1 sparing supports 150K SIP devices across 7 Session Managers for a single Session Manager failure. Similarly, a dual data center (N+N) supports 150K SIP devices across 12 Session Managers (6 in each data center).

Online/Offline Call Journal (Call History)

Previously, when an endpoint/client was not logged in, incoming calls were not included in the call log of the device. Users could be confused as the call logs on their multiple devices did not have the same calls if the users were logged into some of the devices but not others when a call occurred.

Starting with Session Manager Release 6.3.8, the call log of a device includes incoming calls when the device is not logged in. In addition, if a call cannot be delivered to an endpoint due to the Limit the Number of Concurrent Calls (LNCC) feature, the calls is also logged.

- For H.323 endpoints, Communication Manager stores logged out missed calls and downloads the Call History logs when the endpoint logs in. The maximum number of H.323 Call History logs is 10.
- For SIP endpoints, the primary Session Manager stores all call logs and downloads the logs to the endpoint during login. The endpoint maintains the logs locally while logged in.

Call logs are only stored on the primary Session Manager of the user. There is no redundancy for storing call logs. The primary Session Manager stores the call logs in the User Data Storage database.

You enable Call History logging on the Session Manager Communication Profile for the user by enabling **Enable Centralized Call History**. The default is **off**. The maximum number of call logs per Communication Profile is 100.

SIP phones:

- Download call logs during login only.
- Maintain call logs locally while logged in.

System Manager Web Services

The System Manager Web Services interface for routing and dial plan management provides remote programmatic access for querying, creating, and deleting all Session Manager routing domain data. The routing data that the service accesses and modifies is the same routing data supported by the routing bulk import and administration GUI. The primary routing domain data types are:

- Domains
- Locations
- Adaptations

- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expression data

The System Manager Web Services API enforces the same level of data integrity as the GUI and import interfaces. The API components enforce the same validation logic the GUI and Import interfaces use.

Use the System Manager Web Services interface for provisioning only. Do not use the Web Service API for real-time application access or SIP application integration. The System Manager Web Service API is appropriate for automating normal administrative tasks and has the same administration data propagation delay to the Session Managers as the Routing GUI and bulk import interfaces.

The System Manager Web Services API uses RESTful current best practices. The service provides for XML payloads by default but can optionally support JSON payloads.

Users can select any desired REST client implementation technology. Users must have Web Service development level skills for REST client development.

The System Manager Web Services interface documentation includes a programmers guide, detailed schema definition, and examples and samples.

SIP Phone Configuration template

Starting with Avaya Aura® 6.2 Feature Pack 4, Avaya supports pre- or post-configuration of phone settings and button assignments. Administrators can centrally configure SIP phone settings from System Manager that were previously only accessible from the SIP phone device. Administrators can standardize specific SIP phone button configurations and terminology without having to rely on employees to make the phone configuration changes or having to dispatch a technician to make the changes local to the SIP device. Settings include:

- Button Label fields on SIP Phones defined by the administrator.
- Favorite Key check box to enable specific buttons to appear on the device home page.
- New Phone Settings, such as Call Setting Options, Screen and Sound Options, and Language/ Region Settings.

You can change the Phone Settings and Button Assignments by using the:

- UPM Communication Manager Endpoint Profile Endpoint Editor screen.
- Communication Manager Manage Endpoint screen.

Using the 96x1/1XC phone GUI, you can change the button label and the **favorite** status of the button. You cannot change the button type.

The following are the supported use cases for the SIP Phone pre-configuration template:

- Create a new custom template from an Avaya-provided default template.
- Apply a template to a new user.
- Apply a template to an existing user.
- Modify endpoint settings for an existing user.
- Modify endpoint settings for a group of existing users.
- User can make an update that overrides the template settings.
- Remove a template.

The following use cases are *not* supported at this time:

- Apply a template to a group of existing users.
- Update a template and propagate the changes to all users ad devices assigned to that template.

Phone Settings:

- 14+ parameters are available to set or change.
- SIP endpoints:
  - remove phone settings the endpoint does not use or understand.
  - remove badly formatted settings.
  - replace any missing settings with default values.
- All AST phone buttons are configurable with personal labels, and most buttons can be configured as favorite buttons.

This feature supports the 96x1 endpoints, including the 9611, 9621, 9641, and the Call Center versions of these endpoints. Default phone templates already exist in the System Manager database. Users can create custom templates using the default templates.

Limit Number of Concurrent Calls for SIP endpoints

The Limit Number of Concurrent Calls (LNCC) feature causes a multi-call appearance endpoint to behave as a single line appearance endpoint. When the LNCC feature is enabled and the user is active/busy on one call appearance, subsequent incoming calls receive a busy signal or follow normal busy treatment such as coverage and are tagged as missed calls.

LNCC works on all H.323 and DCP endpoints and any SIP endpoint that supports call appearances.

A user controls this feature using a feature button or feature access code (FAC). Normal operation allows two incoming calls. The user must enable LNCC to allow only one call.

LNCC allows:

- outgoing calls, incoming priority calls, and emergency callback for SIP stations.

- outgoing calls, incoming priority calls, emergency callback, and crisis alert for H.323 and DCP stations.

LNCC works with the Dual Registration and Multiple Device Access features. The user applies LNCC at the user level, and all devices associated with the user inherit the LNCC feature.

For example:

- Most of the time, Steve wants to be active on only one call at a time, so he activates LNCC.
- Andy calls Steve, and they talk for 15 minutes.
- During their conversation, Cindy calls Steve. Because LNCC is active, Cindy's call goes straight to coverage.
- Cindy does not leave a message, but Steve's endpoint still records her call as a missed call. Steve calls Cindy after he finishes his conversation with Andy.

The LNCC feature administration field appears on the station screen and is saved as part of the station record by the **`save translations`** command. Subsequent resets restore the LNCC settings to the state when the **`save translations`** was performed. A user activates and deactivates the feature by using the limit-call feature button or by using two Feature Access Codes: **Limit Number of Concurrent Calls Activation/Deactivation**. The limit-call button indicates whether the LNCC feature is active or not.

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

Inter-gateway Alternate Routing for SIP endpoints

Inter-gateway Alternate Routing (IGAR) provides voice connectivity using a public service provider (PSTN) if not enough bandwidth is available on the private network. If the Corporate Data Network cannot handle the call, the bearer connection is routed over the Public Voice Network.

You can use IGAR when calling to or from a SIP endpoint that is registered to a Session Manager server.

The IGAR triggers include:

- The inter-branch bandwidth limit is reached.
- IGAR is always on for branches with low-bandwidth connectivity.

The source and destination of the call must be associated with the same Communication Manager. Video calls are automatically downgraded to audio if IGAR is triggered.

Use Cases

- Case #1: Vijay in Bangalore and Michael in London both have SIP endpoints and are served by Communication Manager. At peak hours, bandwidth between Bangalore and London is insufficient to carry audio calls with proper quality. With IGAR, Communication Manager automatically sends the audio media over the PSTN, ensuring excellent audio for the call.
- Case #2:

An enterprise has a small branch gateway in Reykjavik with all SIP endpoints registered to an Avaya Aura® data center in Stockholm. The low-cost data connection to Iceland has insufficient bandwidth to carry more than a few audio calls. With IGAR, every call to or from Reykjavik is carried over a low-cost PSTN connection using the “always on” option.

Feature pack to release mapping

Avaya Aura® 6.2 Feature Pack	Avaya Aura® Session Manager Release
Avaya Aura® 6.2 Feature Pack 1	Session Manager 6.3
Avaya Aura® 6.2 Feature Pack 2	Session Manager 6.3.2
Avaya Aura® 6.2 Feature Pack 3	Session Manager 6.3.4
Avaya Aura® 6.2 Feature Pack 4	Session Manager 6.3.8
Avaya Aura® 6.2 Feature Pack 4 Service Pack 1	Session Manager 6.3.9

Supported servers

Session Manager Release 6.3 supports:

- S8510 and S8800 servers for upgrades only.
- S8300D server for Survivable Remote.

Session Manager supports the following servers:

Release	Servers
6.3 6.3.2	Dell R610, HP DL360 G7
6.3.4 6.3.8 6.3.9	Dell R610, Dell R620, HP DL360 G7, HP DL360 G8

HP and Dell will discontinue HP DL360 G7 and Dell R610 servers in the near future. For more information, see the respective vendor websites.

Avaya has issued End of Sale notices for the S8800 and S8510 servers. Avaya supports these servers for existing installations only. For information about the effective dates, see the Avaya support website at http://support.avaya.com/.

Chapter 3: What's new in Session Manager

The following sections describe the new features and enhancements for Avaya Aura® Session Manager Release 6.3.9

SIP Endpoint Concentrator Connection Policy

Customers want to deploy virtual desktop solutions to reduce the overhead of managing individual personal computers and to improve overall security.

Virtual Desktop (VDI) software from Citrix and VMware apply a common IP address for virtual users to register to servers. The single IP address is shared by multiple Windows instances running on a Virtualized server.

Currently, when 1xC or ACA clients deploy in the virtualized environment, the clients utilize the shared IP address of the Windows OS instance in which they run. These clients are limited to six registrations on Session Manager with a single IP address on a single port.

In the traditional model, the 1xC client is hosted on the user's physical desktop that is in the user's proximity. However, when the 1xC client is hosted in a virtualized application environment, the 1xC client moves to the remote data center. Since multiple clients are hosted on a single server or a small number of servers, multiple client connections are established between the server hosting 1xC clients and Session Manager. To prevent potential security threats, Session Manager limits the number of connections originating from a single IP address. This policy is problematic for virtualized application environments where more than six clients are hosted on a single server.

In order to inter-operate with virtualized desktop solutions, such as a Citrix server hosting 1xC, Session Manager Release 6.3.9 introduces a new connection policy that allows for up to 1000 connections from a single IP address. This type of connection is called an **Endpoint Concentrator** policy.

A new connection policy, **endpt conc**, can be assigned to a SIP entity link. The Session Manager (ASSET) allows up to 1000 connections on that SIP entity link. The **endpt conc** policy is an untrusted policy based on the current **Default** (endpoint) policy. That is, the requests arriving over the SIP entity link with the connection policy **endpt conc** are challenged as for any other endpoint. To identify and administer the SIP entities hosting multiple endpoints, this release introduces a new entity type, **Endpoint Concentrator**.

When the customer administers a SIP entity as an **Endpoint Concentrator** on the SIP entity page, all subsequently added SIP entity links towards that entity will have the **endpt conc** connection policy by default.

The **endpt conc** policy cannot be used for remote office (REMO) configurations. With a REMO configuration, the Session Border Controllers use a single connection in the SIP entity link towards Session Manager to multiplex multiple calls. For such configurations, the connection policy must allocate large amounts of memory and buffers for a single connection.

Note:

SIP Link Monitoring is not available for SIP entities of type **Endpoint Concentrator**.

Role Based Access Control Permission restoral

In the Avaya Aura® 6.2 Feature Pack 1 release, administrators could assign read-only or read-write permissions to specific web pages.

Due to design and implementation changes for Avaya Aura® 6.2 Feature Pack 2, permissions could no longer be applied to specific web pages.

Avaya Aura® Session Manager 6.2 Feature Pack 4 Service Pack 1 (Release 6.3.9) restores the ability to assign permissions specific to Session Manager and Routing web pages. A user can access or change only those fields on a page for which the user has permission. Permissions include:

- Total read/write permissions. The administrator can view the page and has the ability to make changes to all the administered fields that are part of the page.
- Read-only permissions. The administrator can view the entire page but cannot make any changes to the fields on the page.

Chapter 4: Interoperability

Product compatibility

Session Manager 6.3.9 is compatible with the following Avaya Aura® 6.2 Feature Pack 4 product components.

Product	Release Supported
Avaya Aura® Contact Center	6.2
Avaya Aura® Conferencing	8.1
Agile Communication Environment™	6.2
Avaya Aura® Experience Portal	6.0
Avaya B5800 Branch Gateway	6.2
Avaya Aura® Messaging	6.3
Avaya Aura® Collaboration Environment	3.0
Avaya Aura® Communication Manager including Communication Manager Messaging and Avaya Aura® Call Center Elite	6.3.6
Avaya Communication Server 1000	7.6 (SP4)
Avaya Aura® System Manager	6.3.9
Avaya Aura® System Platform	6.3.4
Avaya Aura® Presence Services	Presence Services 6.2.4
Avaya Aura® Application Enablement Services	Application Enablement Services 6.3.3
Media Gateway G860	3.0
G430/G450 Branch Gateway	6.3.6
Avaya Aura® Utility Services	Utility Services 6.3.6

For the latest and most accurate compatibility information, see https://support.avaya.com/CompatibilityMatrix/Index.aspx on the Avaya support website.

Supported Avaya endpoints

Session Manager 6.3 supports the following Avaya endpoints:

Endpoints	Notes
9600 Series IP Deskphones with Deskphone SIP 2.6.6, 6.0, 6.1, or 6.2. Specifically: • 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, 9650C with Deskphone SIP 2.6.6, 2.6.10 • 9601, 9608, 9611, 9621, 9641 with Deskphone SIP 6.2.2	
96x1 Series SIP endpoints (9608SIP, 9611SIP, 9621SIP, 9641SIP, 9611SIPCC, 9608SIPCC, 9621SIPCC, 9641SIPCC) – fw 6.3	
Call Center Agent endpoints (9621 and 9641 with custom faceplates) - 6.2, and one-X Agent (6.2.2)	
ADVD	Administered as a 9640SIP phone, with 1.1.2
Flare Communicator Windows 1.0	
Flare Experience Windows 1.0 and 1.1	
Flare Communicator iPad 1.0	
Flare Experience iPad 1.0 and 1.1	
VDI Communicator 1.0	Supported as an endpoint controlled by one-X Communicator 6.1.7 as a SIP client in shared control mode
one-X Communicator 6.1 for Windows	For CS1000 7.5 and Session Manager. Supports all three audio modes. One-X communicator does not support Session Manager prior to Session Manager 6.0.
one-X Communicator for MacOS 1.0.4	SIP only and does not support CES. Supports all three audio modes. One-X communicator does not support Session Manager prior to Session Manager 6.0.
One-X Mobile iOS SIP Client – 6.2 (or later)	This version does not support the Multi Device Access (MDA) feature.
11xx and 12xx SIP endpoints.	Treated as 3rd party endpoints. PPM cannot download data to these endpoints.
Radvision SIP endpoints: XT1000, XT1000 Piccolo, XT1200, XT4000, XT5000	Treated as 3rd party endpoints. PPM cannot download data to these endpoints.
Konftel	Treated as 3rd party endpoints. PPM cannot download data to these endpoints.
1603SW-I SIP endpoint, such as Blaze	

Avaya 10x0 video endpoints (such as Lifesize, aliased as 96x0SIP) as follows: • 1010/20: AV_PP1_4_7_3_5.cmg • 1030/40/50: AV_RM1_4_7_3_5.cmg	
46xx endpoints	

Note:

UniSTIM is a non-SIP endpoint that is supported as part of the overall Avaya Aura® solution. UniSTIM endpoints do not register with a Session Manager but register to a CS1000.

The following earlier endpoint releases support the specified Session Manager releases:

Endpoint	Version	Supported Session Manager Release
Avaya one-X® Communicator	6.0	6.0
Avaya one-X® Communicator	6.1	6.0 6.1
Avaya one-X® Communicator	6.2	6.1 6.2
Flare Communicator	1.0	6.1 6.2
Flare Experience	1.0	6.2 Requires Session Manager 6.2 and AAC 7.0

Older SIP endpoints do not support all features of Session Manager Release 6.3, but can still register to Session Manager (for example, 46xx).

Deployment options

You can deploy Avaya Aura® Session Manager using the following methods.

Deployment Model	Documentation Reference
Session Manager on a standalone server.	*Deploying Avaya Aura® Session Manager*
Session Manager in a VMware virtualized environment.	*Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment*
Session Manager as a component of Midsize Enterprise.	*Implementing Avaya Aura® Solution for Midsize Enterprise*
Branch Session Manager as a component of a Communication Manager template.	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394

Operating system compatibility

Session Manager 6.3 and Branch Session Manager 6.3 support Red Hat Enterprise Linux (RHEL) 6.2. The underlying SIP container is IBM WAS 8.0.x server.

RHEL 6.2 is the underlying operating system for the Branch Session Manager and the Session Manager components running on Avaya Aura® Solution for Midsize Enterprise.

Third-Party PBX Integration

With direct SIP connections, Session Manager works with the following systems:

- Cisco UCM
- Siemens (Unify) HiPath
- Alcatel Lucent OmniPBX
- Aastra

You can program each of the third-party PBXs so that Session Manager can perform inter-PBX routing.

Chapter 5: Performance and capacity specifications

Capacity and scalability specification

You can arrange Session Managers in multiple sparing models to support desired capacities and failure characteristics. Sparing models range from N+1 through N+N.

N+1 Example: An N+1 model to support 150,000 SIP devices consists of seven Session Managers. If one Session Manager fails or is taken out of service, the remaining six Session Managers support all 150,000 SIP devices.

N+N Example: An N+N or redundant data center model supports 150,000 SIP devices and consists of six Session Managers in two data centers (12 Session Managers total). If one data center fails or is taken out of service, the remaining six Session Managers in the second data center support the 150,000 SIP devices.

Important:

Assigning a SIP profile to an H.323 endpoint reduces the total SIP capacity by that many endpoints. See Alternative H.323 Endpoint administration considerations and impacts on page 31.

The following table contains the type of SIP entity, maximum number of entities supported per Session Manager, and clarifying notes.

Entities	Numbers (supported limits)	Notes
Core Avaya Aura® Session Manager (SM) instances	12	
Dial Patterns * Locations/ Pattern * Routing Policies	300,000	Assuming 20 telephone numbers for each SIP Entity. The number can be interpreted as only 300,000 individual phone numbers can be routed, but these are patterns. If the numbers can be grouped for a given destination, fewer entries are required.
SIP Domains	1,000	
SIP Entities	25,000	
SIP Entity Links	75,000	1. Assuming 3 links for each SIP entity such as UDP, TCP, and TLS links.

Entities	Numbers (supported limits)	Notes
		2. Assuming that each SIP Entity is linked to two Session Managers (for redundancy) with only one transport protocol used. In this case, there would need to be 50,000 links. In both cases, the inter-Session Manager entity links need to be counted towards the limit.
SIP Entity Links / SM	10,000	
Adaptations	25,000	Assuming one Adaptation for each SIP Entity. At the most, there can be one Adaptation for each SIP Entity and some SIP Entities may not require any Adaptation.
Adaptation Entries	250,000	Full system limit. Includes both ingress and egress entries.
Adaptation Entries/SM	45,000	
Regular Expressions	100	
Routing Policies	25,000	Assuming one routing policy for each SIP Entity.
Time Ranges	1,000	
Locations	25,000	Takes into account the use of locations to control bandwidth.
Location IP Address Patterns	50,000	Used to identify if a given SIP endpoint is associated with the location. Based on the assumption that on an average two patterns are used to define a location.
Local Host Name Resolution Entries	25,000	Based on an average of one for each SIP Entity.
User Records	125,000	
Handles/User	3	
Buddy List/Contacts for each User	25	Assuming an average of 25 per user (maximum of 250).
Simultaneously Registered Devices/SM	43,000	On the Common R2 servers. 21,500 Primary Registered Devices 21,500 Secondary Registered Devices Assuming 125,00 users but 150,000 SIP devices, each with a primary and secondary Session Manager registration for failure recovery distributed across Session Managers in the configuration. A total of 150,000 primary and 150,000 secondary registrations distributed across an N+1 sparing model configuration of 7 Session Managers would be approximately 21,500 primary and 21,500 secondary registrations per Session Manager.

Entities	Numbers (supported limits)	Notes
Active (Primary) SIP Devices/SM	21,500 (normal conditions) 25,000 (temporarily under failure conditions)	If a user has multiple registered SIP devices, be careful when distributing users across Session Managers to avoid exceeding the SIP device capacities of an individual Session Manager. For example, 15,000 users each have two registered SIP devices, but 30,000 devices exceed the capacity of a single Session Manager. Instead, assign only 10,750 users to the individual Session Manager to not exceed the 21,500 device capacity limit.
CC Agents/SM	18,000 (normal conditions) 21,00 (failure conditions)	Call Center (CC) Agent SIP devices consume more resources per Session Manager. 18.000 is the maximum for CC Agent SIP devices, assuming all devices are CC agents. When configuring for systems that may support fewer CC Agents, assume that five CC Agent devices are the equivalent of six regular SIP devices.
Presence	18.000 (normal conditions) 21,000 (temporarily during failure conditions)	
Simultaneously Registered Devices/User	10	A SIP user/station can have more than one registered SIP device per user, such as an Avaya one-X® Communicator in Shared Control. Session Manager capacities are based on the number of active SIP devices. The number of registered devices per user is important to know to adequately distribute users and devices across Session Manager instances.
Users/SM on VMware		See *Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment* on the Avaya support site.
System Manager administrators	250	
System Manager Simultaneously Active Sessions	50	
Branch SM instances	250	
Per Branch SM performance • Devices/survivable embedded • Devices/survivable	• 700 • 2,000	

Entities	Numbers (supported limits)	Notes
Busy Hour Sessions/ SM	540,000	The type of call determines the number of SIP sessions. An SRE call is a single session, so Busy-Hour Session is equivalent to BHCC. Conversely, a SIP station-to-SIP station call creates three sessions, and the BHCC is calculated accordingly.
Session creations/second/SM	150	
Session creations /second/ BSM	10	
Session creations/ second / survivable embedded SM	3	
Simultaneous sessions/SM	180,000	

Alternative H.323 Endpoint administration considerations and impacts

The current method for administering H.323 endpoints is to use either of the following:

- System Manager to create an H.323 endpoint without a SIP profile.
- The Communication Manager SAT.

You must configure Session Manager to route calls to the correct Communication Manager.

Alternative method for administering H.323 endpoints

An alternative method for administering H.323 endpoints is to use System Manager to create a SIP profile for an H.323 endpoint. URE routing will automatically route calls to the correct Communication Manager.

The alternative method:

- Simplifies Session Manager routing configuration.
- Provides Dual Registration (H.323 and SIP endpoints on the same extension) with no further System Manager configuration.
- Provides an easy migration to a SIP endpoint by changing the endpoint type and removing the H.323 station.

Use Case

A customer has H.323 endpoints with DID numbers scattered randomly among different Communication Manager servers. This arrangement makes it cumbersome to configure Session Manager routing to send calls for H.323 endpoints to correct Communication Manager.

The Customer uses the new technique to take advantage of URE routing in place of manually administering Session Manager routing policies.

Impact on capacities

Important:

This method assigns a SIP profile to an H.323 endpoint. Using this method reduces the total SIP endpoint capacity by the number of H.323 endpoints assigned a SIP profile.

For example, if you configure 200 H.323 stations using the alternative method, you reduce the maximum number of SIP devices by 200.

Dial plan specification

With Session Manager, call routing is controlled by two interdependent schemes:

- A global enterprise-wide numbering plan used for centralized routing that is administered on a centralized management console.
- One or more local, geographically significant dial plans administer on Avaya Aura Communication Manager, or other vendor PBX. Local dial plans specify the actual digits dialed within the constraints of the numbering plan.

Session manager adjusts routing information (digits and domains) to accommodate the numbering plan or dial plans as required.

The numbering plan describes the overall numbering scheme that the enterprise uses for centralized routing. Session Manager uses two different numbering plans for analysis and routing:

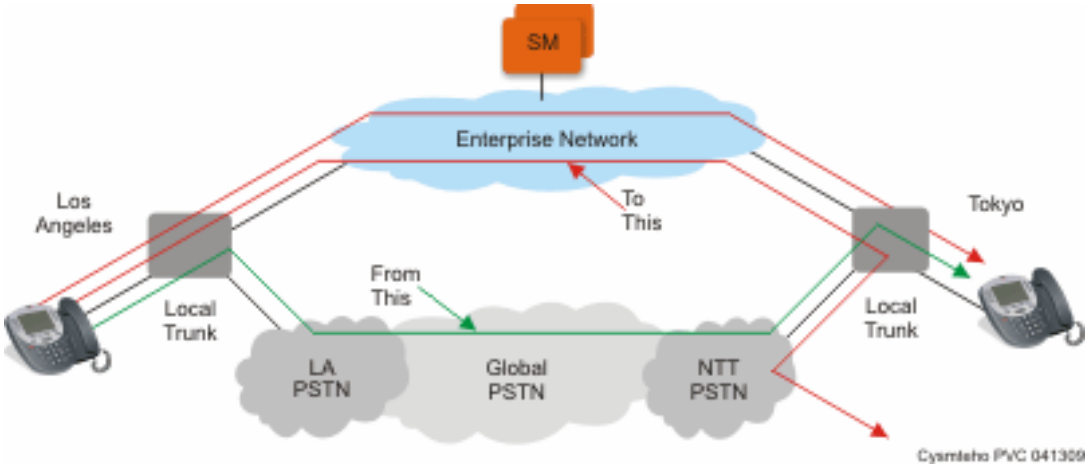
- E.164 Public Numbering Plan
- Enterprise Canonical (Private Numbering Plan)

Tail end hop off

Session Manager can route outgoing calls to local trunks at each location so that all users across the network enterprise can save toll charges for calls that go off the network. This configuration is called tail end hop off (TEHO).

For example, a call from Tokyo to Los Angeles can be routed through a company intranet and then sent to the PSTN from the Los Angeles PBX, which is similar to a *local* call from Los Angeles. And calls bound for Tokyo are routed through the Tokyo PBX.

The following figure illustrates how TEHO works:



Call Admission Control specification

Session Manager supports truly converged voice and video bandwidth management with Avaya Aura® System Manager centralized administration and control. You can administer bandwidth allocations between voice and multimedia traffic with an option to allow voice to use bandwidth from unused video allocations when network conditions require. Session Managerr intercepts every SIP request for service, examines the SIP messages for the requested bandwidth, and allocates the actual bandwidth requested and accepted. However, Session Manager denies as well as downspeeds calls if the bandwidth allocation is exceeded. In addition, Session Manager can automatically downspeed video calls to the bandwidth available and enable video calls to complete at lower bandwidths.

Session Manager provides advanced control of video and multimedia bandwidth allocation. Administrators can configure:

- The maximum allowed bandwidth for a multimedia call with separate controls for inter-location (where resources are scarce) and intra-location (where more bandwidth is generally available so higher quality can be allowed) on a per-location basis.
- The minimum *downspeed-able* video bandwidth by location to insure a level of video quality.

Administrators can see the current bandwidth usage and the number of calls for accurate management.

Redundancy and high availability

An enterprise supports up to 12 Session Managers. You can implement the Session Manager instances in the same data center or in data centers that are separated geographically around the world. These instances need not exist on the same subnet.

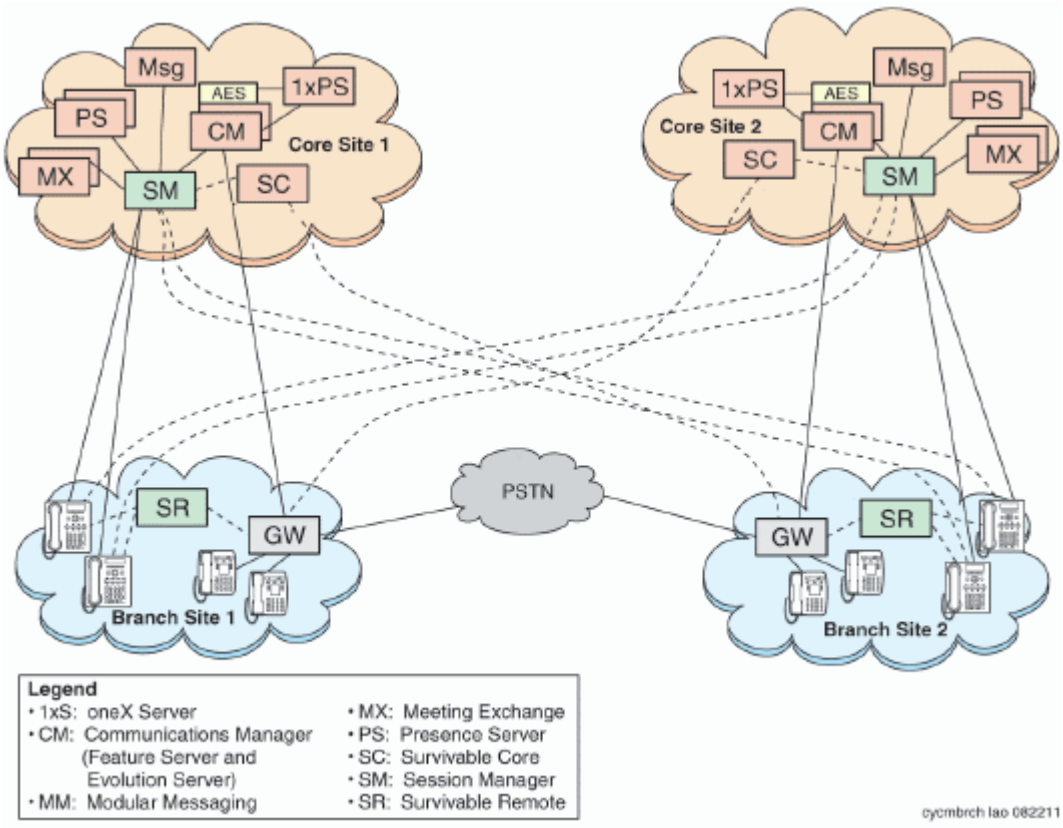
Session Manager redundancy supports networks with round trip delays of less than one second.

Session Manager uses the active-active approach where two instances are active simultaneously and either of the instances can process any request. This feature is important for distributing traffic across the network.

Configuring more than one Session Manager in a network has the following benefits:

- A failure of one of the Session Manager instances does not interrupt service.
- You can use one System Managerto administer all the Session Managers.
- The centralized dial plan is in effect for Avaya and third-party PBXs. The centralized dial plan connects the PBXs, using SIP either directly or using a SIP gateway, to one of the Session Manager instances.
- When SIP endpoints register simultaneously with two Session Managers at the core and with one Branch Session Manager, the SIP endpoints continue to be operational if any one of the associated Session Managers fails.

The following figure shows solution-level survivability in the enterprise:



Survivable Core

Survivable Core (SC) provides geo-redundant Communication Manager Feature Server redundancy. It supports multiple Data Centers for a failed or unreachable main Communication Manager. Session Manager works with the Survivable Core as follows:

- After the main Communication Manager goes down, Session Manager starts sending SIP messages to the Survivable Core.
- When the main Communication Manager recovers, Session Manager again starts sending SIP messages to the main Communication Manager instead of the Survivable Core.

Survivable Remote

Survivable Remote sites include a Survivable Remote Session Manager and Survivable Remote Communication Manager (either a Feature Server or an Evolution Server, depending on the main Communication Manager to which it is connected). SIP phones simultaneously register to the main Session Manager, a backup main Session Manager, and the Survivable Remote Session Manager. During a WAN outage that removes the communication path between phones and the associated Session Manager, the phones failover to the Survivable Remote Session Manager and the Survivable Remote Communication Manager.

Chapter 6: Security

Security specification

All SIP sessions flow through Session Manager, which is the SIP routing element. Session Manager protects the Unified Communications (UC) applications and servers from Network and Transport Denial of Service (DoS) attacks, SIP DoS attacks, and other network attacks. Session Manager also enforces access control policy for UC applications. As a SIP Registrar, Session Manager authenticates and authorizes user access to protect customers from toll fraud and other malicious attacks.

Session Manager runs on the RHEL Linux operating system. The operating system is hardened to provide only those functions necessary for securing critical call processing applications.

Using Session Manager, an administrator can select TLS to secure the SIP signaling to ensure the privacy of the application credentials of the user, as well as to secure the keys used for securing the media stream with SRTP.

Session Manager ensures that security defenses, encryption, authentication, and certificate use are embedded at all levels across the enterprise network to maintain secure continuous communications between all endpoints without compromising performance.

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

Port assignments

For complete port matrix information, see the Port Matrix Documents section at http://support.avaya.com/security.

Chapter 7: Licensing requirements

For licensing, Branch Session Manager and core Session Manager require:

- Product Licensing and Delivery System (PLDS) for license entitlement management, license activation, and license file delivery.
- Web License Manager (WebLM) for license management, including the use of the WebLM server.

You can download the license file from PLDS and install the license as well as the authentication file. Alternately, Avaya or an authorized Business Partner can download and install the license file.

Software licenses for upgrades to major releases of Session Manager are chargeable. Software licenses for upgrades to the next minor upgrade release are not chargeable.

The number of users administered and the number of Session Manager instances administered is licensed.

The Session Manager license file contains the total number of authorized Session Manager licenses available for the enterprise. With Session Manager you can monitor the Session Manager licenses used in the system, based on the number of concurrent sessions. Session Manager raises an alarm when the number of licenses used exceeds the number of authorized Session Manager licenses available for the system. The system does not block the calls or disable the feature. You can:

- Purchase additional Session Manager licenses from Avaya.
- Analyze the Session Manager license usage and reschedule the planned usage of the system.

Note:

Licensing provides a 30-day grace period for all license errors, including no license file present on initial installation, before applying any license enforcement.

Glossary

Call Admission Control	Prevent the over subscription of VoIP and protects the flow of voice traffic to ensure that there is enough bandwidth for authorized call flows.
Centralized Applications	A set of core Avaya SIP applications such as Modular Messaging, Media Exchange and Voice Portal.
Centralized SIP Trunking	A consolidation of trunks to a common core location as opposed to the network edges.
DNS Server	A server that maintains a database of mappings of DNS domain names to various types of data, such as IP addresses.
Internet Protocol Security (IPsec)	A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. It is a dual-mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3.
Local Host Name Resolution	Host name resolution is the process of resolving a host name to an IP address.
Network Address Translation (NAT)	The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.
Secure Access Link (SAL)	Avaya equipment designed to enable remote access to Aura equipment for troubleshooting and diagnostic purposes.
Sequenced Applications	A collection of SIP applications that engage automatically based on the user's profile. These applications are added to a call path during the logical progression of the call (incoming or outgoing).
Session Border Controller (SBC)	A device used in some Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.
Tail End Hop Off (TEHO)	In a private network, a call which is carried over flat rate facilities (Inter-machine Trunks or IMT) to the closest switch node to the destination of the call, and then connected into the public network as a local call.

Time of day routing	A configuration which determines how calls are routed during specific times of day across the network.
Toll Avoidance / By-pass	A configuration which allows calls to be routed to and from the service provider without incurring any cost.
Trunk	Connection between two switches, can be multiplexed to provide higher bandwidths such as DS-1 and DS-3.

Index

A

alternate routing 12
applications
  centralized 12
  sequencing 12
Application Sequencing
  enhanced 13
Avaya Learning 8

C

CAC 33
Call History 17
capacity specification 28
CDR 14
centralized
  applications 12
  dial plan 32
  routing 32
  SIP trunking 13
Communication Manager
  IGAR 20
  LNCC 19
connection policy
  SIP endpoint concentrator 22
courses 8

D

default certificates
  not supported 14
deployment options 26
dial plan 32
documentation
  related 6
document changes 6

F

feature pack to release mapping 21
features 11

G

global routing 32

H

H.323 endpoint considerations 31

I

inter-gateway alternate routing for SIP endpoints 20

L

least-cost routing 12
legal notices .....
licensing 37
Limit Number of Concurrent Calls 19
load balancing 12, 32

M

mapping
  feature packs to releases 21

N

NIST support 15
normalized network 12
notices, legal .....

O

Online/Offline Call Journal 17
operating system
  compatibility 27
options for deployment 26

P

permissions
  RBAC 23
Personal Profile Manager 13
policy-based routing 32
port assignments 36
PPM 13
pre-configuration template
  for SIP phone 18
product compatibility 24
Proxy and Registrar 12

R

RBAC
  permissions 23
redundancy 33
related documentation 6
routing
  alternate 32

routing *(continued)*
global 32
policy-based 32

S

scalability 28
scale increases 16
security
NIST support 15
removal of default certificates 14
security specification 36
sequenced applications 12
servers
supported for Session Manager 21
Session Manager 11
Session Manager Application Sequencing 13
SIP endpoint concentrator
connection policy 22
SIP phone
pre-configuration template 18
SIP trunking 13
support 9
supported endpoints 24
supported servers 21
Survivability 33
Survivable Core 35
Survivable Remote 35
System Manager
web services 17

T

tail end hop off 32
Third-party connectivity 27
TLS 1.2 16
training 8
Transport Layer Security 16

V

videos 9

W

warranty 10
web services
System Manager 17