



Avaya Aura™ Session Manager Overview

03-603323, Issue 2
Release 5.2
November 2009

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER, AND 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 End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

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.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://www.avaya.com/support/Copyright/>.

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 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 Web site: <http://www.avaya.com/support/>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura™ System Manager, and Avaya Aura™ Session Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Contents

Chapter 1: Overview.....	5
What is Session Manager?.....	5
What does Session Manager do?.....	5
Normalization of disparate networks.....	7
Centralized routing and dial plan.....	8
Tail end hop off.....	9
Centralized SIP trunking.....	9
Centralized applications.....	10
Sequenced applications.....	10
Session Manager architecture.....	11
SIP entities.....	12
Hardware.....	13
SM100.....	14
Secure Access Link.....	14
High availability.....	15
Security.....	15
System Manager.....	16
Licensing.....	16
Other documents.....	16
Index.....	19

Chapter 1: Overview

What is Session Manager?

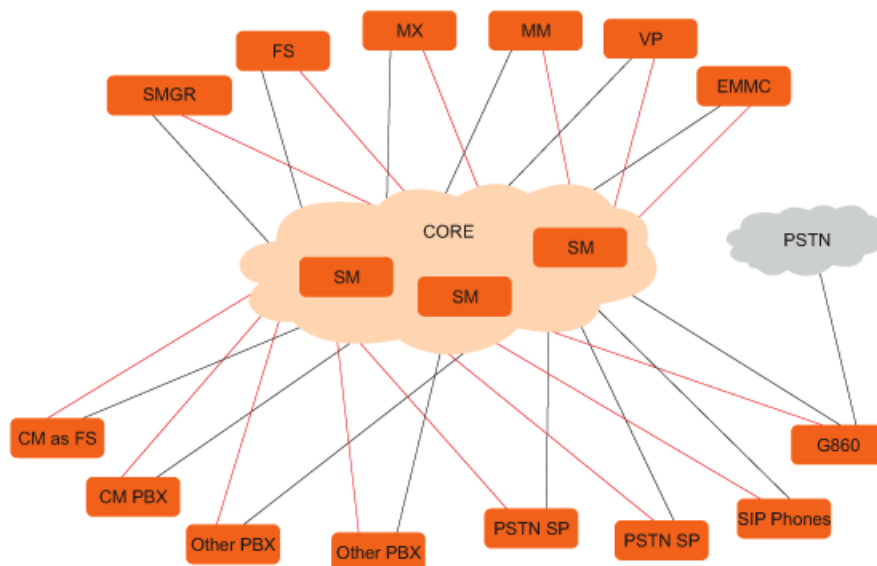
Companies typically have a diverse set of communications products within their corporate intranet that cannot communicate with each other. A standard signaling protocol is needed so these diverse products can work together. Avaya has adopted the Session Initiation Protocol (SIP) as that signaling protocol for communication.

Avaya Aura™ Session Manager is a SIP routing and integration tool and the core component within the Avaya Aura™ Enterprise Edition solution. It integrates all the SIP entities across the entire enterprise network within a company. Session Manager offers a new perspective on enterprise communication where individual locations are no longer managed as separate units within the enterprise. Each location, branch, or application is part of the overall enterprise, managed as an enterprise, and seen as an enterprise.

Session Manager offers a simplified network-wide feature deployment; centralized routing, SIP trunking, and user profiles; cost-effective scalability (from small to very large deployments); high availability with geographic redundancy; and a secure environment that conforms to specific SIP standards and practices.

What does Session Manager do?

Session Manager offers a core communication service that builds on existing equipment but adds a SIP-based architecture.



cysmtosol2 PVC 041309

SM	Avaya Aura™ Session Manager
SMGR	Avaya Aura™ System Manager
FS	Feature Server
MX	Avaya Meeting Exchange
MM	Avaya Modular Messaging
VP	Avaya Voice Portal
EMMC	Avaya Expanded Meet-Me Conferencing
CM as FS	Avaya Aura™ Communication Manager as a Feature Server
CM PBX	Avaya Aura™ Communication Manager as a private branch exchange
Other PBX	Third-party private branch exchanges, such as Cisco CallManager and Nortel CS1000
PSTN SP	Public switched telephone network service providers, such as AT&T and Verizon
SIP Phones	Avaya 96xx SIP telephones
G860	Avaya G860 Trunk Gateway

Session Manager connects Communication Manager as a feature (SIP) server and both Avaya enterprise PBX and small key PBX systems within branch offices, third-party PBXs, gateways, service providers, SIP-enabled adjuncts, and SIP telephones. It also integrates locations and applications. Specifically, Session Manager

- Normalizes disparate networks
- Routes SIP sessions across the network
- Provides the gateway for the enterprise for external SIP trunking
- Scales to support up to 7200 stations
- Is highly available with redundancy across different geographic regions
- Offers centralized management, including user profiles, through System Manager.

Each Session Manager installation combines several or all of the following configurations:

- Centralized routing and dial plan
- Policy-based routing
 - Time of day routing
 - Alternate routing
 - Load balancing
 - Call admission control
- Tail end hop off (TEHO)
- Centralized SIP trunking
- Centralized applications
- Sequenced applications

Related topics:

[Normalization of disparate networks](#) on page 7

[Centralized routing and dial plan](#) on page 8

[Tail end hop off](#) on page 9

[Centralized SIP trunking](#) on page 9

[Centralized applications](#) on page 10

[Sequenced applications](#) on page 10

Normalization of disparate networks

Session Manager normalizes and adapts disparate SIP protocols to meet the strict SIP standards of the network. This allows third party PBXs to work with each other and with Avaya equipment, allowing customers to realize true vendor interoperability.

An example is the ability to connect Cisco and Nortel PBXs with Session Manager so they operate with each other and with Avaya equipment. Session Manager converts the headers in the SIP messages that are used to display calling and called-party information between the format required by each switch in a call.

Centralized routing and dial plan

Session Manager provides the centralized, global dial plan for an enterprise and access to external SIP trunking. The dial plan is managed through a centralized management console and governs PBXs that connect using SIP to one or more Session Manager instances. For example, an enterprise might have two instances of Session Manager in two different data centers with two different SIP trunking service providers.

Dual dial plan

Within Session Manager, dial plans are administered without requiring the various PBXs to change their dial plans or digit manipulations. Session Manager also does not require that the PBXs send or accept numbers that are unique across the enterprise, sometimes called the enterprise canonical form. This saves customers from having to re-administer or re-engineer each PBX.

Mixed, diverse enterprise

Many enterprises consist of several smaller dial plan domains that are a result of multiple mergers or acquisitions. Session Manager supports these enterprises and moves the administration of these various dial plans to the Session Manager core so that one single point of management is possible. This not only eliminates the need to administer and maintain these various dial plans in each PBX, but it allows the users in these locations to maintain the status quo and eliminates the need for users to change their dialing patterns.

Policy-based routing

With Session Manager customers can define their call routing policy. These policies allow customers to control when calls are made, how the call load is balanced, and how they are routed during network failures.

Least-cost routing, also called time-of-day routing, chooses the lowest cost route from a list of service providers on a time-of-day or time-of-week basis. This produces a cost savings for the enterprise. The routing table shows an example of setting up time-of-day routing.

Route #	Route Priority	D	Start Time 1	Host 1		Start Time 6	Host 6
1	1	Mon	0:00	Service Provider 1	○ ○ ○	20:00	Service Provider 2
			○				○
			○				○
			○				○
	2	Sun	0:00	Service Provider 2		20:00	Service Provider 1
		Mon	0:00	Service Provider 3		18:00	Service Provider 4
			○				○
			○				○
	6	Sun	0:00	Service Provider 4		18:00	Service Provider 3
			○				○
			○				○
			○				○
		Mon	0:00	Service Provider 5		14:00	Service Provider 6
			○				○
			○				○
		Sun	0:00	Service Provider 6		14:00	Service Provider 5

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 to a SIP entity between multiple IP addresses. It is necessary for Avaya Voice Portal MPPs, Avaya Modular Messaging MASs, and SIP entities that are routed to more than one Session Manager to create redundancy. Load balancing uses priority and weights when selecting routes. Session Manager can be administered to choose between multiple IP addresses for a given entity and select these hosts based upon administered priorities and weights. If some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights, with a lower weight receiving a higher priority.

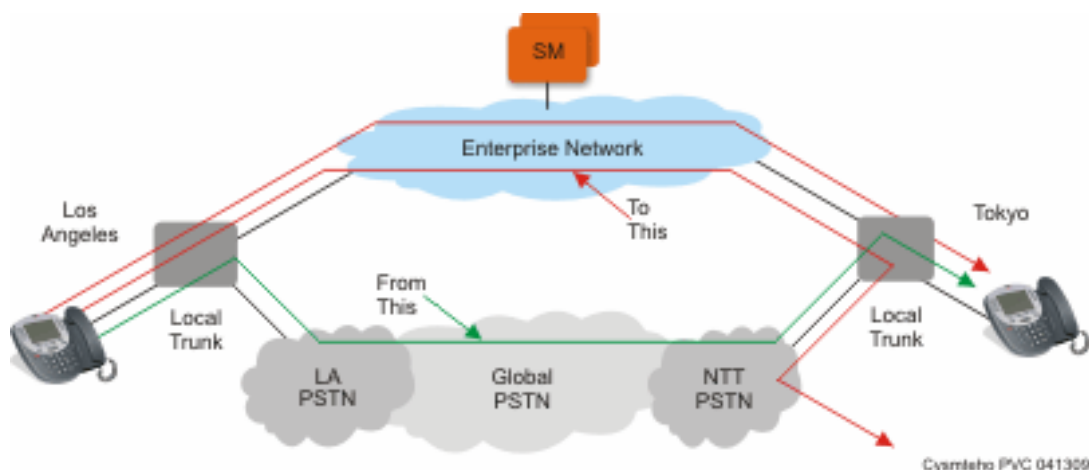
Call admission control allows calls to be rerouted when the WAN link to a branch fills up. Session Manager maintains the status of the link to each location, using administrator-set limits on each link.

Tail end hop off

Session Manager supports using the local trunks at each location to allow all users across the network enterprise to save toll charges for calls that go off the network. Outgoing calls are directed to local trunks on each location.

For example, calls from Tokyo to Los Angeles through a company's intranet are routed through the PSTN from the Los Angeles PBX, basically making it a *local* call from Los Angeles. And calls bound for Tokyo are routed through the Tokyo PBX. Local PBXs may not accept the full E.164 number, but Session Manager can change them to numbers that the PBXs can understand.

The figure provides a typical example of how tail end hop off works.



Centralized SIP trunking

Centralized SIP trunking allows SIP trunks to be shared within an enterprise. SIP trunks route calls from one PBX through a service provider over the network through a second service

provider to another PBX. This requires each PBX to provide the SIP trunks. With Session Manager as the core, the individual PBXs share the SIP trunks. As a result, companies

- require fewer SIP trunks to provide the same level of service
- are able to buy SIP trunks in bulk
- eliminate local access costs, accessing the SIP trunking service provider directly.

Centralized applications

Session Manager provides connectivity for centralized Avaya applications like Avaya Modular Messaging, Avaya Voice Portal, and Avaya Meeting Exchange. Each PBX, gateway, or location connects to Modular Messaging through the Session Manager core rather than individually. Session Manager also connects to SIP-enabled adjuncts, making the management and deployment of adjuncts infinitely simpler than the mesh-connect methods where each PBX connects to its own adjunct.

Sequenced applications

Sequenced applications is a series of applications that engage automatically. The sequence can be different or the same for each user. Each user is given a template of applications that are applied to every incoming, outgoing, or combined call for that user. Each application in a sequence sees all requests and can deny, modify, or forward initial SIP requests. Examples of sequenced Avaya applications are

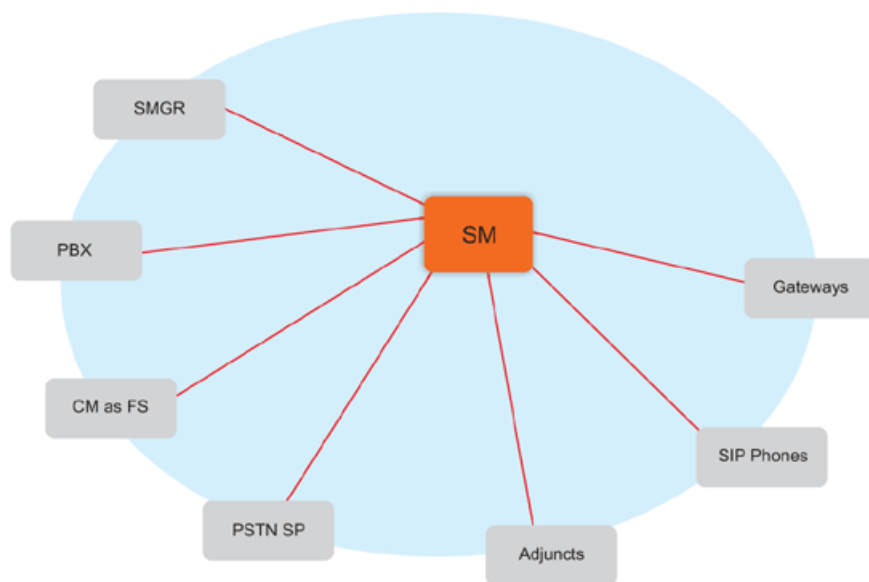
- Billing Service
- Voice Monitor
- Communication Manager as a feature server
- Call Blocker
- Personal assistant
- Meeting Coordinator.

Session Manager also supports third-party PBX endpoint application sequencing. Because calls to and from users on non-Avaya PBXs are directed to the Session Manager core, applications are applied to calls to and from these endpoints. Session Manager creates a profile for third-party PBX users, and applies these applications to these users. Typical applications include blocking calls based on user preferences, directing calls to these users when they move across the Avaya Aura™-powered enterprise, and augmenting caller identification information for incoming and outgoing calls. This capability is available without upgrading or modifying code on existing third-party PBX equipment.

Session Manager architecture

Session Manager is the core of the network with SIP entities connecting to it. A grouping of Session Manager with Avaya Aura™ System Manager and SIP entities is called a Session Manager instance.

The figure shows a typical Session Manager instance with multiple SIP entities.



Cysminstan2 P/C 041309

SM	Avaya Aura™ Session Manager
SMGR	Avaya Aura™ System Manager
PBX	Private branch exchanges, such as Avaya Aura™ Communication Manager, Cisco CallManager, and Nortel CS1000
CM as FS	Avaya Aura™ Communication Manager as a Feature (SIP) Server
PSTN SP	Public switched telephone network service providers, such as AT&T and Verizon
Adjuncts	SIP-enabled adjuncts that work with PBXs to provide services such as voice mail and conferencing abilities.
SIP Phones	Avaya 96xx SIP telephones
Gateways	SIP-enabled gateways that work with non-SIP service provider networks

A *Session Manager instance* consists of one server supporting up to 25,000 SIP entities. An enterprise network can support up to 3 instances. These Session Manager instances can be installed in the same data center or in multiple data centers and in geographically redundant locations with virtually unlimited distance restrictions. All of the instances support mix and match.

A *SIP entity* is a logical element that either initiates requests, responds to requests, or both. Session Manager supports the following SIP entities:

- Feature (SIP) servers
- Private branch exchanges (PBXs)
- SIP gateways
- PSTN service providers
- SIP-enabled adjuncts
- SIP-enabled telephones

System Manager is the application used to manage Session Manager. It runs on a separate server, and only one is required for the entire network, not per instance.

Related topics:

[SIP entities](#) on page 12

[Hardware](#) on page 13

[SM100](#) on page 14

[Secure Access Link](#) on page 14

SIP entities

Session Manager, Release 5.2, supports several PBXs, gateways, telephones, and other SIP entities and SIP-enabled adjuncts.

Feature servers

A feature server is the component that provides call-related features and, when SIP-enabled, registers with the Session Manager core. Avaya Aura™ Communication Manager is supported as a feature server. A feature server processes a half-call to provide features separately at the origination phase(s), termination phase(s), or both. Calls that route via the feature server operate much like tandem Communication Manager SIP trunks but can also provide station features at the appropriate phase. Communication Manager as a feature server supports only a subset of the standard Communication Manager functions.

PBXs

A PBX serves a particular business or office, providing the telephone features to the employees. Session Manager connects both enterprise-wide and small key systems generally used in branch offices. Session Manager connects to and acts as a system-wide dial plan for call processing applications such as:

- Avaya Aura™ Communication Manager and later using direct SIP connections. Connections using SIP Enablement Services (SES) are not supported.
- SIP-enabled Cisco Unified CallManager.
- Nortel CS1000 SIP-enabled PBX.

SIP gateways

SIP gateways work with the non-SIP service provider network. Session Manager works with SIP peer systems within the enterprise in the same way. These include non-Avaya SIP systems, SIP-enabled PBXs, and Communication Manager. Such SIP gateways are supported both for trunking services or line-side services. SIP gateways include trunk gateways, such as the Avaya G860 Trunk Gateway.

SIP PSTN service providers

Service providers are treated as SIP peer network elements with which Session Manager maintains a trunking relationship. Foreign domain PBXs or SIP switching equipment are treated essentially the same as the SIP service providers, that is, as a SIP peer network element over a SIP trunk. Service providers supported include AT&T and Verizon.

SIP-enabled adjuncts

SIP-enabled adjuncts provide supplemental services to PBXs, such as voice mail and conferencing capabilities. Avaya products supported include Avaya Voice Portal on the latest firmware, Avaya Modular Messaging Release 5.1, and Avaya Meeting Exchange and Avaya Expanded Meet-me Conferencing Release 1.0.21.

SIP devices

SIP devices, particularly the Avaya 96xx-series SIP telephones, may register to the Session Manager core. Session Manager can support up to 7000 Avaya SIP devices. Session Manager provides SIP proxy, registrar, location services, and more to this initial set of devices.

Hardware

The Session Manager application is installed on either the Avaya S8800 1U Server or the Avaya S8510 Server Family. For a list of components and specifications for these servers, see the *Installing and Upgrading Avaya Aura™ Session Manager* (03–603473) or *Installing the Avaya S8510 Server Family and Its Components* (03–602918). The servers used for Session Manager include the following specifications:

- 2 quad core, 2-gigahertz processors
- 8 gigabytes (S8510) or 12 gigabytes (S8800) of memory
- 2 power supplies to provide power redundancy
- RAID 1 disk array
- an SM100 TLS accelerator card.

The servers are shipped with all the required components and software applications installed. The server is connected to the customer's network and the System Manager server using

customer-provided Category 5 (CAT5) Ethernet cables. Remote access is through the network only; modem access is not supported.

System Manager is installed on either the Avaya S8800 Server or the Avaya S8510 Server Family.

SM100

The SM100 is the security module that manages SIP connections between Session Manager and all other SIP elements. The SM100 module is a PCI-based Network Interface Card (NIC) installed in the server. The SM100 has hardware security accelerators and multicore MIPS processors that perform security processing for Session Manager.

The SM100 supports connectivity using UDP and TCP in nonsecure deployments. External SIP elements connect to Session Manager through the SM100 card.

The SM100 module's primary functions are to offload most of the heavy security processing and provide a framework for Session Manager security, for example:

- The SM100 module terminates all the SIP TLS connections for Session Manager.
- It physically separates Session Manager from the voice network.
- It offers network and transport firewall and network denial-of-service protection.
- It offers SIP firewall and SIP denial-of-service protection.
- It uses PKI validation techniques to ensure that only trusted SIP elements connect to Session Manager.

Secure Access Link

Secure Access Link (SAL) is a method to monitor the equipment and software. It is centralized and accessible through System Manager and has access to all the Session Manager equipment and software. SAL provides alarming and logging.

The major Session Manager components that are monitored include

- Server and all applicable components, including the SM100 card
- Operating system
- System Manager platform, including Network Routing Policy
- Session Manager solution.

High availability

Session Manager provides an opportunity for redundancy by supporting up to 3 Session Manager instances in an enterprise. The multiple Session Manager instances provide redundancy and are implemented in the same data center or in ones separated geographically, even around the world. No need exists for them to be on the same subnet.

Session Manager redundancy supports networks with round trip delays of less than 1 second.

Session Manager uses the active-active approach where two instances are simultaneously active, meaning any request goes to either instance and is served. Requests use either instance freely. This is an important concept for distributing traffic across the network.

Active-active redundancy requires that the Session Manager instances be interconnected over an IP network with sufficient bandwidth and low enough latency to synchronize runtime data.

Configuring more than one Session Manager in a network means that

- A failure of one of the Session Manager instances does not interrupt service. All calls that were stable before the failure remain stable with no discernible gaps in voice connectivity. New calls may be placed immediately after the failure with no more than 3 seconds of delay.
- A centralized enterprise-wide dial plan can be entered and managed using terminals logically connected to the server running System Manager.
- The centralized dial plan governs Avaya and third party PBXs (particularly Nortel and Cisco) and enables them to connect via SIP (either directly or via a SIP gateway) to one of the Session Manager instances.

Security

Session Manager is the SIP routing element between SIP entities. As the SIP router, all SIP sessions flow through Session Manager, allowing it to provide the following security capabilities to centralized SIP applications:

- TLS session connection termination for SIP trunks
- Network/transport firewall and denial of service (DoS) protection
- SIP DoS protection
- Access control to Avaya applications where only authenticated SIP elements are allowed access
- White listing and black listing of SIP elements.

System Manager

Central management of Session Manager is handled through the Avaya Aura™ System Manager application. System Manager delivers a set of shared, secure management services and a common console across multiple products. System Manager includes the following central management services:

- User Management: Allows for the administration of users and user groups.
- Communication System Management: Allows for the administration of individual and group stations and mailboxes.
- Network Routing Policy: Allows for the administration of routing policy for all Session Manager instances within an enterprise.
- Alarm Management Service: Supports alarm monitoring, acknowledgement, configuration, clearing, and retiring.
- Logging Service: Receives log events formatted in the common log format.
- Session Manager: Provides miscellaneous functions for Session Manager elements, including administering instances, configuring SIP firewalls, sequencing applications, monitoring SIP entities and the security module, and managing bandwidth usage.

A central database that resides on the System Manager server stores all the System Manager central data, the Session Manager administration data, and the Central Data Distribution Service information. The last item is used to detect changes to the System Manager central database and then distribute these changes to the Session Manager instances. All communications between System Manager and Session Manager instances is done over secure links.

Licensing

Session Manager requires a single license file. It is a one-time, nontransferable license and is based on the number of Session Manager instances. Licensing for Session Manager is downloadable from the Avaya Product Licensing and Delivery System Web site. License files for Session Manager run on the System Manager server.

Other documents

Session Manager comes with a complete set of documents. The following list provides the title, document number, and a brief description of all of the documents in the documentation set.

- *Avaya Aura™ Session Manager Overview* (03–603323) — Provides descriptions of Session Manager and its components (this book).
- *Installing the Avaya S8510 Server Family and Its Components* (03–602918) — Provides information and specifications on the Avaya S8510 Server Family and procedures for physically installing it in a rack.
- *Installing and Upgrading Avaya Aura™ Session Manager* (03–603473) — Provides information on installing the Avaya S8800 Server and installing and upgrading Session Manager on a server.
- *Administering Avaya Aura™ Session Manager* (03–603324) — Provides information on administering Session Manager through System Manager.
- *Administering Avaya Aura™ Communication Manager as a Feature Server* (03–603479) — Provides information on administering a feature server as a SIP entity.
- *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (03–603325) — Provides information on maintaining and troubleshooting Session Manager, including logging and alarming.
- *Avaya Aura™ Session Manager Case Studies* (03–603478) — Provides real-life scenarios for administering various SIP entities and administering user profiles, stations, and mailboxes.
- *Security Design for Avaya Aura™ Session Manager* — Provides information on making Session Manager secure on the network.

Index

A

applications	
centralized	10
sequenced	10
availability	15

C

central management	16
centralized	
applications	10
dial plan	8
routing	8
SIP trunking	9

D

dial plan	8
documentation set	16

F

features	5
----------------	-------------------

G

global routing	8
----------------------	-------------------

H

hardware	13
----------------	--------------------

L

legal notices	2
licensing	16
load balancing	8

N

normalized network	7
notices, legal	2

P

policy-based routing	8
----------------------------	-------------------

R

routing	
alternate	8
global	8
policy-based	8

S

SAL, see Secure Access Link	14
Secure Access Link	14
security	15
security module	14
sequenced applications	10
servers	13
Session Manager architecture	11
SIP entities	
SIP-enabled adjuncts	12
feature servers	12
PBX	12
service providers	12
SIP gateways	12
SIP telephones	12
SM100	14 , 15
System Manager	16

T

Tail end hop off	9
------------------------	-------------------

