Avaya Aura™ Session Manager Overview

Issue 3
03-603323
Release 6.0
June 2010

© 2010 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

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/ 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 7

What is new in this release 7
What is Session Manager? 7
What does Session Manager do? 8
Normalization of disparate networks 9
Centralized routing and dial plan 9
Tail end hop off 11
Centralized SIP trunking 11
Centralized applications 12
Sequenced applications 12
Session Manager architecture 13
SIP entities 14
Secure Access Link 16
Survivable Core 16
Survivable Remote 17
High availability 18
Security 19
System Manager 19
Licensing 20
Related documents 20

Index 23

Chapter 1: Overview

What is new in this release

Avaya Aura™ Session Manager 6.0 provides following set of functionality:

- Fully SIP redundant core provides active-active N+1 redundancy with up to six Session Manager instances in an enterprise
- Support for upto 250 SIP survivable branches
- Enhanced SIP feature set and connects to any IETF compliant SIP solution.
- Support for mixed H.323, DCP, and SIP endpoints at the redundant core and at the survivable branch.
- New scalability upto 100,000 users overall, 50,000 SIP stations, and 25,000 SIP entities.
- Expanded centralized management with Avaya Aura™ System Manager 6.0 and can handle up to 25,000 locations in a full deployment with up to 750,000 BHCC of inter-location calling.

The left navigation pane for Avaya Aura™ System Manager 6.0 web console has changed and **Session Manager** functionality now falls under **Elements** menu. **Network Routing Policy** menu has been renamed as **Routing** and **SIP Domains** as **Domains**.

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 required to make these products work together. Avaya has adopted the Session Initiation Protocol (SIP) as the 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
- 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.

Session Manager connects Avaya Aura™ 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 and non-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
- Integrates with third-party equipment and endpoints
- Offers centralized management, including user profiles, through System Manager
- Supports SIP survivable branches
- Communicates with a Session Border Controller and provides protection at the edge of the enterprise network

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

- Centralized routing and dial plan management
- 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

It also handles all call re-direction, internal network call accounting feeds, toll by-pass, inter-office routing, and international least-cost routing.

Related topics:

Normalization of disparate networks on page 9
Centralized routing and dial plan on page 9
Tail end hop off on page 11
Centralized SIP trunking on page 11
Centralized applications on page 12
Sequenced applications on page 12

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

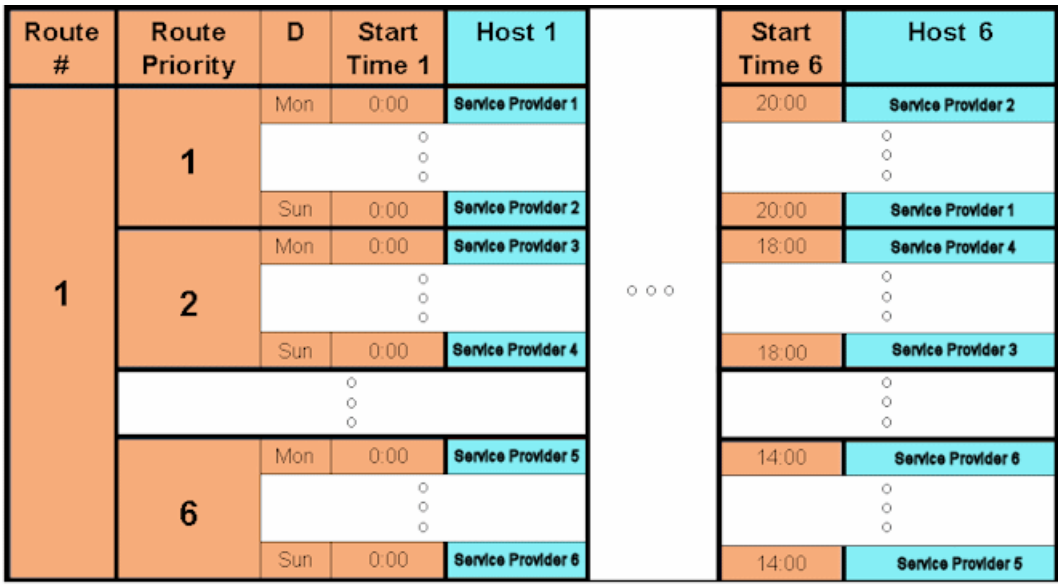
Many enterprises consist of several smaller dial plan domains that are a result of multiple mergers or acquisitions. Session Manager supports these enterprises and moves the administration of these various dial plans to the Session Manager core so that one single point

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

Customers can define their call routing policy with Session Manager. These policies allow customers to control 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, chooses the lowest cost route from a list of service providers on a time-of-day or time-of-week basis. This results in cost savings for the enterprise. The routing table shows an example of setting up time-of-day routing.



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.

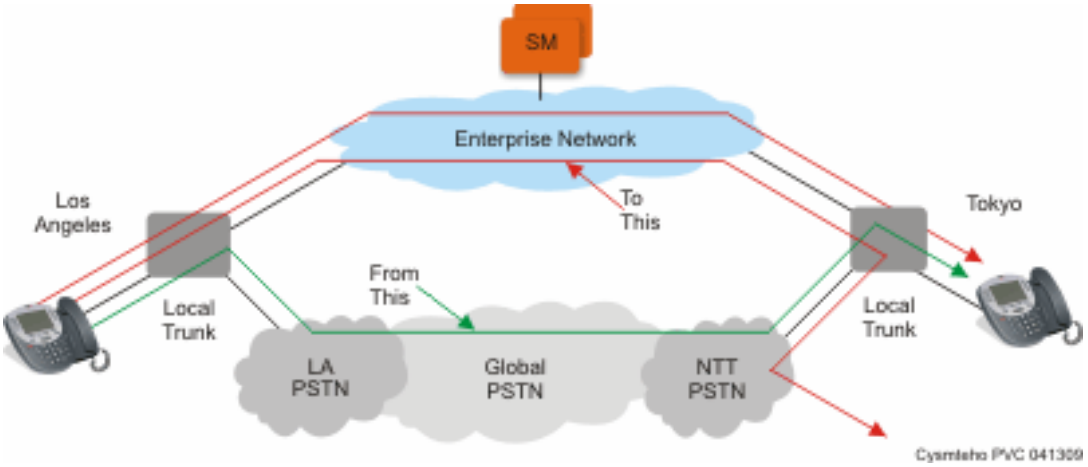
Call admission control allows calls to be rerouted when the WAN link to a branch fills up. Session Manager maintains the status of the link to each location, using administrator-set limits on each link.

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 such as 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 are 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 is 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

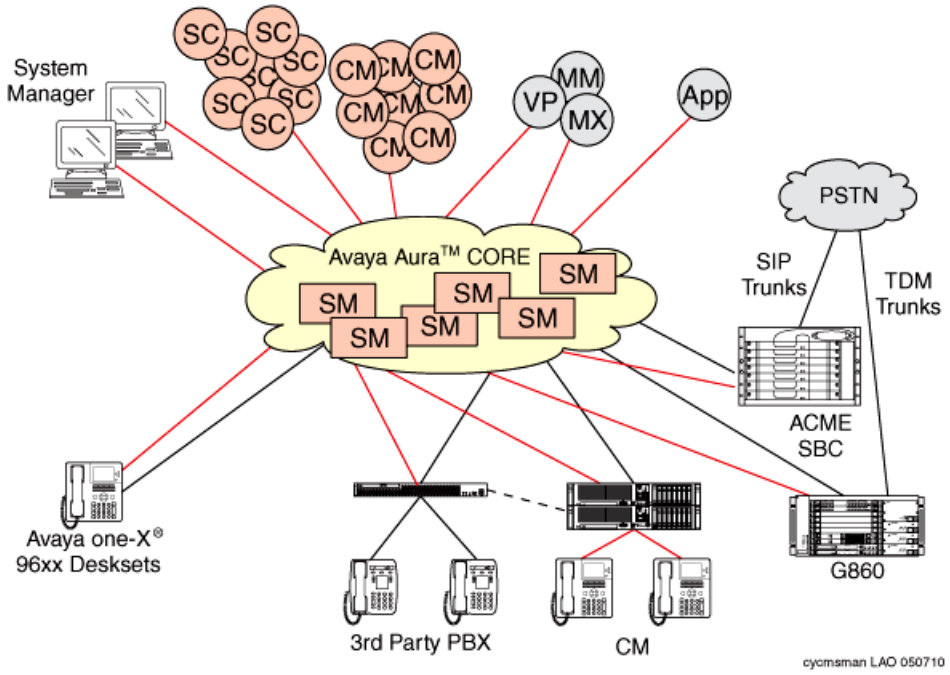
- Billing Service
- Voice Monitor
- Communication Manager Feature Server
- Call Blocker
- Personal assistant
- Meeting Coordinator.

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 a 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.



SM	Avaya Aura™ Session Manager
VP	Avaya Voice Portal 5.1 and 6.0
MM	Avaya Modular Messaging Release 6.0, 5.2 and 5.1.
MX	Avaya Meeting Exchange 6.0 and 5.1
G860	Avaya G860 High Density Trunk Gateway R2
SC	Survivable Core
App	other SIP applications
CM	Communication Manager
ACME SBC	Acme Packets Session Border Controller 2900/3800/4500

A Session Manager instance consists of one server supporting up to 50,000 SIP entities. An enterprise network can support up to six Session Manager 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.

SIP entities are all the network entities that are a part of the SIP System. Session Manager supports the following SIP entities which form part of the overall enterprise setup:

- Avaya Aura™ Session Manager
- Avaya Aura™ System Manager
- Private branch exchanges
- Avaya Aura™ Communication Manager Feature Server
- Public switched telephone network service providers
- SIP-enabled adjuncts that work with PBXs to provide services
- Desksets
    - Avaya one–X desksets
    - 3rd Party desksets
- Avaya Aura™ one-X Communicator
- Avaya G860 High Density Trunk Gateway R2 that work with non-SIP service provider networks
- Communication Manager with Branch Session Manager
- Branch Gateway
- Acme Packets Session Border Controller 2900/3800/4500

Session Manager is the software component for all enterprise SIP sessions. System Manager is the single, centralized management point of control. It runs on a separate server, and only one is required for the entire network, not per instance.

Related topics:

SIP entities on page 14
Secure Access Link on page 16
Survivable Core on page 16
Survivable Remote on page 17

SIP entities

Session Manager, Release 6.0, supports several PBXs, gateways, telephones, and other SIP entities and SIP-enabled adjuncts.

Communication Manager Feature servers

Communication Manager as a feature server provides Communication Manager features to SIP endpoints using the IP Multimedia Subsystem (IMS) half call model that allows full application sequencing.

The feature server only supports SIP endpoints that are registered to Avaya Aura™ Session Manager. The Communication Manager server is connected to Session Manager via a SIP-ISC interface which uses an IMS-enabled SIP signaling group and associated SIP trunk group. Communication Manager is administered as a feature server by enabling the **IMS-enabled?** field on the signaling group form.

Communication Manager as a feature server has the following constraints:

- The dial plan for IMS users must route all PSTN calls back to Session Manager over the IMS trunk group. Routing of such calls directly to ISDN trunks is not supported.
- IPSI port networks are not supported.
- Traditional phones such as DCP, H.323, ISDN, and analog are not supported.

Communication Manager Evolution Server

Communication Manager as an evolution server provides Communication Manager features to both SIP and non-SIP endpoints. It uses the full call model with Communication Manager as the only supported application.

With an evolution server:

- H.323, digital, and analog endpoints register with Communication Manager
- SIP endpoints register with Session Manager (URE user)
- All endpoints receive service from Communication Manager

Communication Manager is connected to the Session Manager via a SIP—ISC interface. The Session Manager routes calls from and to SIP endpoints. The SIP endpoints can then communicate with all other endpoints that are connected to the Communication Manager.

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 High Density Trunk Gateway R2.

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 5.1 and 6.0, Avaya Modular Messaging Release 6.0, 5.2 and 5.1, Avaya Meeting Exchange 6.0 and 5.1.

SIP devices

SIP devices, particularly the Avaya 96XX handsets R2.6, may register to the Session Manager core. Session Manager can support up to 50,000 Avaya SIP devices. Session Manager provides SIP proxy, registrar, location services, and more to this initial set of devices.

Secure Access Link

Secure Access Link (SAL) enables monitoring 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
- Operating system
- System Manager platform, including Routing
- Session Manager solution.

Survivable Core

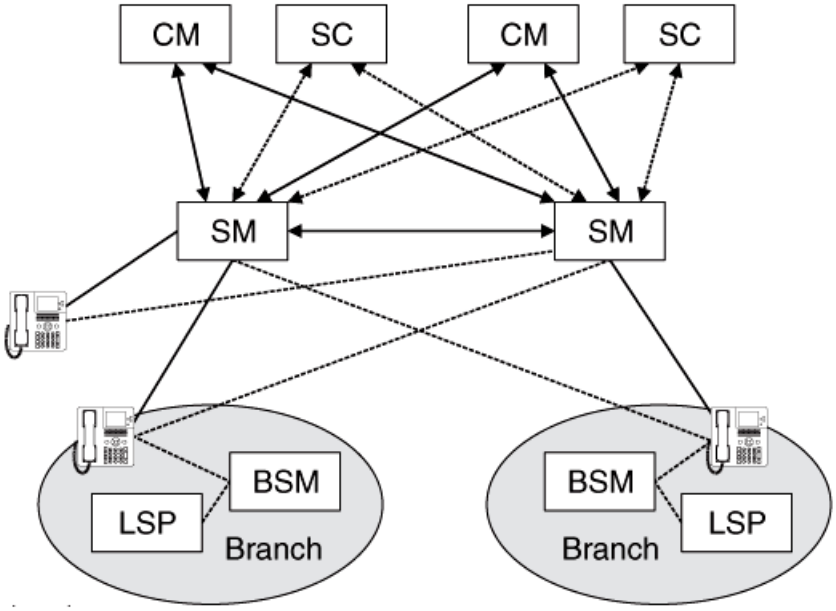
Survivable Core provides geo-redundant Feature Server redundancy and supports multiple Data Centers for a failed or unreachable main Communication Manager. The Survivable Core works as per following conditions:

- Session Manager monitors entity links to the Core Communication Managers via OPTIONs.
- Once Core Communication Manager goes down, the Session Manager starts sending SIP messages to the Survivable Core.

- When connectivity to the main Communication Manager is restored, Gateways re-register with the main Communication Manager automatically via Media Gateway Recovery Rules.
- When the main Communication Manager recovers, Session Manager again starts sending SIP messages to the Communication Manager instead of the Survivable Core.

Survivable Remote

Survivable Remote Sites include a local Branch Session Manager and local Communication Manager (either a Feature Server or an Evolution Server). SIP Phones simultaneously register to the main Session Manager, a backup main Session Manager and the Local Branch Session Manager. During a WAN outage, the phones failover to the Branch Survivable Session Manager and the local Communication Manager server (LSP) provides feature functionality.



BSM	Branch Session Manager
CM	Communication Manager (Feature Server and Evolution Server)
LSP	Local Survivable Processor
SC	Survivable Core

SM	Session Manager

Survivable Remote provides the following features:

- Intelligently works around various individual elements and connectivity outages:
  - with Communication Manager at the core
  - with Session Manager at the core
  - WAN outages
- Active-Active geo-redundancy support
- SIP phones support for simultaneous registration to multiple controllers for fast failover and failback

High availability

Session Manager provides redundancy by supporting up to six Session Manager instances in an enterprise and are implemented in the same data center or in data centers that are separated geographically, even around the world. These instances need not exist 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 important 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 using System Manager Trust Management functionality
- Whitelisting and blacklisting 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.
- Routing: Allows for the administration of routing policies 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.
- Enterprise Licensing Management Service

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 Central Data Distribution Service detects changes to the System Manager central database and distribute these changes to the Session Manager instances. All communication between System Manager and Session Manager instances is done over secure links.

Licensing

Session Manager requires a concurrent user license. When Communication Manager 6.0 licenses are ordered through Avaya Solution Designer (ASD), these licenses can be included in a Session Manager license file on the Avaya Product Licensing and Delivery System Web site. If an enterprise uses application sequencing capabilities of Session Manager for users registered to Session Manager but do not have Communication Manager 6.0.1 licenses, additional licenses for these types of users may also be obtained from Avaya Solution Designer.

Application sequencing is also possible for some of the following endpoints that are not registered to Session Manager:

- DCP
- Analog
- H.323 endpoints on Communication Manager Evolution Server
- Users on third party PBXs where those PBXs are SIP-connected to Session Manager
- Dialed Number Identification Service (DNIS) or Direct Inward Dial (DID) numbers on incoming trunks to Session Manager

Related 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.
- *Installing and Configuring Avaya Aura™ Session Manager* (03–603473) — Provides information for installing Session Manager and the Avaya S8800 server, and provides initial administration for Session Manager.
- *Administering Avaya Aura™ Session Manager* (03–603324) — Provides information on administering Session Manager through System Manager.
- *Administering Avaya Aura™ Communication Manager Server Options* (03–603479) — Provides information on administering a feature server, evolution server, trunk gateway as SIP entities.

- *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (03–603325) — Provides information on maintaining and troubleshooting Session Manager, including logging and alarming.
- *Security Design for Avaya Aura™ Session Manager* — Provides information on making Session Manager secure on the network.

Index

A

applications
- centralized 12
- sequenced 12

availability 18

C

central management 19
centralized
- applications 12
- dial plan 9
- routing 9
- SIP trunking 11

D

dial plan 9
documentation set 20

F

features 8

G

global routing 9

L

legal notice 2
licensing 20
load balancing 9

N

normalized network 9

P

policy-based routing 9

R

routing
- alternate 9
- global 9
- policy-based 9

S

SAL, see Secure Access Link 16
Secure Access Link 16
security 19
sequenced applications 12
Session Manager architecture 13
SIP entities
- SIP-enabled adjuncts 14
- feature servers 14
- PBX 14
- service providers 14
- SIP gateways 14
- SIP telephones 14

SM100 19
survivable Core 16
survivable Remote 17
System Manager 19

T

Tail end hop off 11