Avaya Aura® Session Manager Case Studies

Release 7.1.1
Issue 2
August 2017

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if 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.

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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.

Virtualization

The following applies if the product is deployed on a virtual machine. 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.

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: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, 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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or 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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

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

Avaya is a registered trademark of Avaya 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

Purpose

This document provides different scenarios of Avaya Aura® Session Manager to provide a practical understanding of administration and configuration procedures. This should be read in conjunction with the book *Administering Avaya Aura® Session Manager*.

The book covers the following case studies:

1. Setting up a network
2. Setting up a new user
3. Call Handling
4. Emergency Call handling
5. Setting up a survivable remote branch office

To understand the different roles of the Communication Server in the Session Manager environment, see *Administering Avaya Aura® Communication Manager Server Options*.

This document is intended for anyone who is involved in understanding, administering and troubleshooting Session Manager.

Change history

Issue	Date	Summary of changes
2	August 2017	• Added IPv6 case study. • Added case study on deploying Session Manager on Amazon Web Services.

Chapter 2: Network case study

Overview

This case study describes a network that provides the following solutions through Session Manager:

- Manage signaling messages between disparate PBXs, which includes translation of signaling messages of PBXs with different extension lengths and brands.
- VoIP connections to SIP service providers.
- Tail-end hop-off (TEHO) to maintain calls on the internal network of an enterprise for as long as possible and transmit the calls to PSTN where the calls incur the least cost.
- Access to network systems, including Avaya Aura® Messaging.

The solutions described in this case study use the following Session Manager features:

- Geographically redundant network session control.
- Least- cost routing.
- Alternate routing based on active SIP network monitoring to mitigate network faults.
- Network bandwidth usage limitation based on call admission control.
- Load balancing.
- Session or call detail recording.

Network

The network in this case study consists of:

- Two Session Manager instances in the core network for redundancy.
- Communication Manager instances in Westminster, Highlands Ranch, the New Jersey headquarters, and Avaya Labs in New Jersey with dial plans of different lengths of three, four, and five digits.
- Cisco Call Manager in San Jose with a 5-digit dial plan.
- A SIP trunk to the AT&T SIP service provider.
- A Session Border Controller (SBC) that connects trunks to the Verizon and the Hypothetical SIP service providers.

- Avaya Aura® Messaging that supports all the users in the enterprise.
- Experience Portal Service for 1-866-GO-Avaya at different locations in the network.
- CS1000 PBX at the Belleville location.

Before you administer Session Manager, you need to determine:

- Domains for routing. You will administer Session Manager as the authoritative session management network element for the avaya.com domain and the avayalabs.com domain. The avayalabs.com domain is used for calls that originate from the Communication Manager instance at Avaya Labs in New Jersey.
- The enterprise-wide dial plan and the domain-specific dial plans. Each user on a PBX must be able to dial another user, in the local area or a remote area, using a unique 7-digit enterprise-canonical number.
- The locations defined for call admission control and the location-specific dial plans.

Note the following fundamental rules of administering adaptation rules and the dial plan:

- The Session Manager dial plan determines the routes of internal enterprise-wide numbers and E.164 numbers, which includes E.164 formats of internal numbers.
- The local PBX sends the calling party numbers in the enterprise-canonical format. Session Manager converts these numbers to the E.164 format during the ingress adaptation process.
- Session Manager converts the calling party numbers in the enterprise-canonical format to a format required by a service provider during the egress adaptation process.

After the initial, core provisioning for each solution, configure the following elements in the order listed in routing:

1. Domains
2. Locations
3. Adaptations
4. SIP Entities
5. Entity Links
6. Time Ranges
7. Routing Policies
8. Dial Patterns
9. Regular Expressions
10. Defaults

Core provisioning

Core provisioning includes administering:

- The domains for which Session Manager is the authoritative session management network element.
- The SIP entities for the Session Manager instances.
- The locations that you can use to group entities with different dial plans and to manage bandwidth.

Note:

You can add the domains and the locations to the network after the initial configuration. You can add and link the SIP entities to the network later.

Related links

Domains on page 11
SIP entities for Session Manager instances on page 11
SIP entity for the Session Manager instance in Westminster on page 12
SIP entity for the Session Manager instance in New Jersey on page 12

Domains

Add the domains in request-URI of the INVITE messages that the Communication Manager instances send.

The Cisco PBX, the CS1000 PBX, and the service providers send the IP address of Session Manager in request-URI. Administer an adaptation rule for Session Manager to convert this IP address into the avaya.com domain so that Session Manager can determine the routes for the calls from these entities.

Related links

Core provisioning on page 11

SIP entities for Session Manager instances

Provision the locations and the adaptations before you provision SIP entities. Session Manager-type SIP entities are not associated with a location or an adaptation. Alternatively, instead of provisioning all the locations and the adaptations, provision the location, the adaptation, and the SIP entity details for each SIP entity.

Related links

Core provisioning on page 11

SIP entity for the Session Manager instance in Westminster

You do not need to provision adaptations and locations to Session Manager instances that are located in the core network.

Session Manager monitors the connections on the ports specified in the Entity Links and Port table. If a port is specified in the SIP Entity table, Session Manager replaces the IP address of Session Manager in request-URI of the SIP messages with the domain specified for the port in the Port table. The Cisco PBX and other service providers might send a call request that contains the IP address of Session Manager in request-URI of the SIP message. To monitor connectivity among the Session Manager instances, define entries in the Entity Link and Port table.

Related links

Core provisioning on page 11

SIP entity for the Session Manager instance in New Jersey

Each SIP entity in a network with two Session Manager instances is connected to both the Session Manager instances for redundancy.

If connectivity between a non-Session Manager SIP entity and a Session Manager instance fails, the Session Manager instance determines an alternate route for the call request through another Session Manager instance. To ensure that a particular Session Manager instance can determine an alternate for call requests, all Session Manager instances must be interconnected through SIP entity links.

Session Manager implements cryptographic algorithms and methodologies that are generally accepted in the INFOSEC community. Cryptographic functions are selected based on an assessment of obtaining approval under a FIPS-140-2 or Common Criteria certification assessment.

Session Manager supports Transport Layer Security (TLS) 1.2 for media encryption to:

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

All entity links must be marked as **Trusted** for the entity links to function. Unless there are restrictions against the use of the TLS protocol, set the **Protocol** of the entity links between Session Manager instances as `TLS`. If other SIP entities use the TLS protocol, you must define the TLS protocol for the entity links. The TLS protocol is used to process information securely, such as media encryption keys. If one of the inter-proxy connections does not use the TLS protocol, the non-TLS links are not secure.

If there are three Session Manager instances in this case study, you need to set an entity link between each pair.

The pairs available in case of the three Session Manager instances have good interconnectivity through the entity links. So, if one of Session Manager instances is not available, there can be an alternative for the call requests.

Related links

Core provisioning on page 11

Locations

Administering SIP entities to different locations ensures you can:

- Use different dial plans. Calls that originate from SIP entities at different locations can match different dial patterns and use different routes, even though the location where the call terminates is the same.
- Limit the bandwidth usage between the core network and the location from where a call originates.

In this case study, each SIP entity on the edge of the network is given a separate location. You can create locations and assign these locations to SIP entities any time.

Locations with Managed Bandwidth

In this case study, you can manage the bandwidth usage at the Westminster location by setting the **Total Bandwidth** limit to ensure that audio and multimedia calls can establish simultaneously. You can manage the bandwidth usage of multimedia calls by setting the **Multimedia Bandwidth** limit. This multimedia bandwidth usage limit ensures that multimedia calls do not consume excess bandwidth from the total bandwidth available at a location, which affects establishment of audio calls. For example, to limit the bandwidth usage of multimedia calls to 30% of the total bandwidth usage at a location, administer the **Multimedia Bandwidth** limit with a value that is 30% of the **Total Bandwidth** limit value. If multimedia calls exceed the multimedia bandwidth usage limit, CAC rejects call requests for multimedia calls.

You can also specify the bandwidth usage limit of each call by setting the **Maximum Multimedia Bandwidth (Intra-Location)** limit or the **Maximum Multimedia Bandwidth (Inter-Location)** limit. Set the **Default Audio Bandwidth** limit to 83 Kbps because Avaya endpoints, along with other popular endpoints, use the G.711-Mu code as the primary audio codec.

A G.711 codec produces audio uncompressed to 64 kbps. G.711 is used within LANs because bandwidth is abundant and inexpensive.

A G.729 codec produces audio compressed to 8 kbps. G.729 is generally recommended for transport over limited bandwidth WAN links.

Session Manager modifies the SDP in a call request to reduce the bandwidth requested for the call and enforce the bandwidth usage limits. When Session Manager reduces the bandwidth requested by a call, the call participants might experience a reduction in video call quality. Alternatively,

Session Manager modifies the SDP in a call request to enforce the location-wide multimedia bandwidth usage limits and determines a different route for the call. If Session Manager cannot establish a call by reducing the bandwidth usage of the call, Session Manager denies establishment of the call.

Incoming call requests are associated with SIP entities in different ways. If a call request is associated with a particular SIP entity, Session Manager processes the call request as if the request is sent from a location that is assigned to the SIP entity. If a call request contains the location pattern IP address, Session Manager overrides the location if the IP address determined for the request matches an IP location pattern. If the IP address of the SIP entity is listed in the IP address patterns, then Session Manager routes the call using the location that the request has been associated with.

Enable the CAC SDP functionality by disabling the **Ignore SDP for Call Admission Control** Global Settings option in the Session Manager Administration page.

Note:

1. Select the **Ignore SDP for Call Admission Control** Global Settings option to change the CAC mode to “Ignore SDP”. The “Ignore SDP” mode is similar to the CAC mode setting in Session Manager releases earlier than Release 6.1.
2. Disable the **Ignore SDP for Call Admission Control** Global Settings option to change the CAC mode to “Use SDP”. The “Use SDP” mode is the new CAC mode setting for Session Manager Release 6.1 and later. This case study describes this CAC mode.

Locations without Managed Bandwidth

The Session Manager instance in Avaya Labs at New Jersey does not have bandwidth management. This does not mean that this location has availability of unlimited bandwidth between the location and Avaya Aura® core. Other limits, such as a limit for the maximum number of calls for a SIP entity, might enforce limits to ensure that calls do not use excessive bandwidth. If you do not set a value for the **Multimedia Bandwidth** limit, Session Manager does not manage bandwidth or enforce bandwidth usage limits.

It is better to administer Session Manager for bandwidth management because Session Manager determines the bandwidth usage at a location before forwarding a call request to the location. During bandwidth exhaustion, Session Manager alternate routes the call and prevents the call rejection by the destination entity. Session Manager associates multiple SIP entities with a location and manages the bandwidth of the entire location.

CAC sharing between Communication Manager and Session Manager

Communication Manager can establish VoIP media for H.323 stations and trunks, for inter Port Network, gateway or Avaya Aura® Media Server IP connections and for non-Session Manager

routed SIP trunks. These IP media connections are not visible to Session Manager. In Communication Manager 7.1, Session Manager can be configured as a central authority for bandwidth management. With this setting, Communication Manager requires bandwidth for voice and multimedia IP connections from Session Manager. You can set the bandwidth limits applicable for various locations through System Manager. For more information about setting bandwidth limits, see *Administering Avaya Aura® Session Manager*.

Time ranges

Session Manager refers to time ranges to determine an alternate route for a call request, even though the administration of routing is not based on time ranges.

Time ranges are not associated with a particular SIP entity. Time ranges determine the ranking of routes, with the least-cost option at a particular time period taking precedence over all the other possible routes. Ensure that you at least define the range for the All Day time range.

Non-Session Manager SIP entities

The provisioning details of the non-Session Manager SIP entities are described as solutions that correspond to each SIP entity in this case study. These SIP entities are listed in the SIP Entities table. For the purposes of routing, the Session Manager **Type** of the entity is important.

In this case study, the non-Session Manager SIP entities are:

- PBXs and PSTN trunks

  OR

- SIP service providers that are essentially the front PSTN trunks. Even though they might route some calls entirely within their SIP network it is assumed all or a known subset of PSTN numbers can be reached through them.

  OR

- Systems such as Avaya Aura® Messaging, Experience Portal, or any other server that uses SIP to establish communication sessions.

Harmonize disparate PBXs

This case study describes the following three brands of PBXs:

- Communication Manager

- CS1000
- Cisco Call Manager

The extensions and dial plans of these PBXs are different. Session Manager must convert the SIP messages from these PBXs to the standard SIP message format, the E.164 format, and the Enterprise Canonical dial plan that is described in this case study.

Adaptations for PBXs

Adaptation rules must be defined for all the PBXs that connect to Session Manager. Define adaptation rules for SIP messages of PBXs before you create SIP entities so that you can assign these adaptation rules to PBXs that are similar. Alternatively, create SIP entities with blank adaptation and assign the adaptation rules to these SIP entities later.

For the Westminster Communication Manager instance, you can assign a dial plan of five digits starting with 8, for example, 8xxxx.

Assign a local dial plan of four digits for the Communication Manager instance at New Jersey.

For Avaya Labs Communication Manager instance, assign a three-digit dial plan.

Assign two five digit dial plans for the PBX at San Jose and PBX at Belleville.

Defining rules for the digit conversion in adaptation rules is a complex task. Ensure that you plan adequately for the deployment in this case study.

Adaptation for the PBX located at Westminster

The Westminster Communication Manager instance has a local 5-digit dial plan. For example, 8xxxx. You can dial an extension through the 7-digit enterprise canonical number, 538-xxxx. This PBX also has DID numbers assigned. A user calling from PSTN can dial +1303538xxxx to directly call an extension.

This adaptation uses `DigitConversionAdapter`.

- The Westminster PBX is the authoritative session management network element for the dr.avaya.com domain. INVITE messages from Session Manager to the PBX must have the dr.avaya.com domain in the host part of the request-URI. Specify the odstd parameter to override the destination domain in the **Module Parameter Type** field.
- The PBX also uses the dr.avaya.com domain as the far-end domain on the signaling group of Session Manager. The P-Asserted-Identity header of incoming INVITE messages must be converted to the dr.avaya.com domain. Specify the osrcd parameter to override the source domain in **Module Parameter Type**.
- In the **Module Name** field, enter `DigitConversionAdapter` in the **Module Parameter Type** field, and enter `odstd=dr.avaya.com osrcd=dr.avaya.com` based on your digit conversion table.

Adaptation for the Communication Manager instance located at the New Jersey headquarters

The Communication Manager instance located at the New Jersey headquarters has a local 4-digit dial plan. For example, xxxx. You can dial an extension through the 7–digit enterprise canonical number, 953-xxxx. This PBX also has DID numbers assigned. A user calling from PSTN can dial +1908953xxxx to directly call an extension.

This adaptation uses the `DigitConversionAdapter`. The PBX in the New Jersey headquarters is the authoritative session management network element for the nj.avaya.com domain. The PBX also uses the nj.avaya.com domain as the far-end domain in the signaling group to Session Manager. These domain conversions are specified as parameters in the adaptation module.

- In the **Module Name** field, enter `DigitConversionAdapter`.

  In the **Module Parameter Type** field, enter `odstd=nj.avaya.com osrcd=nj.avaya.com` based on your digit conversion table.

Adaptation for the PBX located at Avaya Labs in New Jersey

The Avaya Labs Communication Manager instance has a local 3-digit dial plan. For example, xxx. You can dial an extension through the 7-digit enterprise canonical number, 696-5xxx. The PBX also has DID numbers assigned. A user calling from PSTN can dial +19086965xxx to directly call an extension.

This adaptation uses `DigitConversionAdapter`. Communication Manager is the authoritative session management network element for the avayalabs.com domain. This PBX also uses the avayalabs.com domain as the far-end domain on the signaling group to Session Manager. The P-Asserted-Identity header of incoming INVITE messages must be changed to the avayalabs.com domain.

- In the **Module Name** field, enter `DigitConversionAdapter`.
- In the **Module Parameter Type** field, enter `odstd=avayalabs.com osrcd=avayalabs.com` based on your digit conversion table.

Adaptation for the PBX located at San Jose

The PBX at San Jose has a local 5-digit dial plan. For example, 1xxxx. Users of the extensions connected to this PBX dial the 5-digit extension number to call other extensions. You can dial an extension through the 7-digit enterprise canonical number, 661-xxxx. The PBX also has DID numbers assigned. A user calling from PSTN can dial +1408661xxxx to directly call an extension.

For calls made by local users, the adaptation process converts:

- Numbers dialed by local users into enterprise canonical numbers. For example, a San Jose user calls another San Jose user through Session Manager.
- Local calling party numbers into enterprise canonical numbers. For example, when a user in San Jose calls a user in Westminster. The calling party number displayed in Westminster is the enterprise canonical number.

- The numbers of international calls to the E.164 format. For example, when you make an international call with the number 011+<digits>.
- The number of calls made to North American numbers to the E.164 format.

For calls made to the San Jose PBX, the adaptation process must convert:

- The called party enterprise canonical number into a local extension number. For example, 661-xxxx to a 1xxxx.
- The E.164 number into a local extension number for calls from a service provider. For example, +1408661xxxx into 1xxxx.

This adaptation uses the Cisco adapter to convert the proprietary headers that Cisco uses to convey the display and the diversion information to the standard headers that the Avaya products use. The Cisco Adapter can also perform digit conversion. In the Cisco PBX, specify:

- The IP address as the host part of request-URI.
- The parameter as `odstd` to override the destination domain.

During the ingress adaptation process in Session Manager, this adapter performs the following digit conversions:

- The numbers of international calls to the E.164 format. For example, 011+<digits>.
- The numbers of calls within North America. For example, 1+<10 digits> to the E.164 format.

During the egress adaptation process in Session Manager, this adapter performs the following digit conversions:

- The E.164 format number to the local number.
- The enterprise canonical number to the local number.

Adaptation for the PBX located at Belleville

The PBX at Belleville has a local 5-digit dial plan. For example, 8xxxx. You can dial an extension through the 7-digit enterprise canonical number, 538-xxxx. A user calling from PSTN can dial + 1613-538-xxxx to directly call an extension.

This adaptation uses the CS1000 adapter. Enter identical common phone-context strings in the ingress adaptation rules and the egress adaptation rules forms. If these strings are not identical, the CS1000 adapter might cause errors.

- In the **Module Name** field, enter `CS1000Adapter`.
- In the **Module Parameter Type** field, enter `odstd=avaya.com osrcd=avaya.com` based on your digit conversion table

Example:

The request `R-URI 5385335; phone context=Belleville@avaya.com; user=phone` matches the three rules of this adapter. However, the CS1000 adapter determines Rule 2 to apply the adaptation process because the call request matches four fields of Rule 2 compared to the three fields of Rule 3.

SIP entities for PBXs

The PBXs in this case study are listed in the SIP entity table as the Communication Manager type or the Other type. However, all SIP entities of the Other type are not PBXs located on the edge of a network.

Each of these PBXs is administered similarly, except for the FQDN or the IP address of PBX.

The IP address identifies sessions originating from the PBX. Session Manager determines to terminate a session through the IP address of a PBX.

The PBX location determines how the adaptation process modifies signaling messages, unless there are other factors overriding the process of routing and adaptation.

Single Interface

The Westminster Communication Manager is an example of a PBX with a single interface where an IP address is specified.

In the General section, specify the **Name** field with a unique name that represents the name of the SIP entity. Setting a unique name that also represents the name of the SIP entity is not mandatory, but a unique name that identifies a SIP entity makes administering easier. Set the **Call Detail Recording** field to `none` because you do not need to create CDRs for each call in a PBX.

In the SIP Link Monitoring section, set the **SIP Link Monitoring** field to `Use Session Manager Configuration`. This setting applies the administered monitoring parameters of each Session Manager to this SIP entity. Enable SIP monitoring for all the SIP entities that support this feature. Most PBXs support the SIP monitoring feature.

In the Entity Links section, set the **Port** field to `5060` for both the links because this port is used for two-way communications. Set the **Connection Policy** field to `Trusted`. If you do not set the **Connection Policy** field to `Trusted`, the link does not work.

Multiple interfaces

The Communication Manager located in Highlands Ranch is a SIP entity with multiple interfaces. This SIP entity is an example of a large Communication Manager instance setup with more than one C-LAN. With multiple interfaces, SIP entities can determine alternate routes for redundancy and have a higher level of fault tolerance. Routing to the Communication Manager is handled by specifying an FQDN, which resolves to multiple IP addresses.

This particular SIP entity supports TLS, so the entity link protocol and port are administered accordingly.

The FQDN in this case can either be resolved by DNS or through a locally provisioned FQDN-to-IP address mapping. The FQDN-to-IP address mapping is specified in the Local Host Name Resolution table of Session Manager Element Manager.

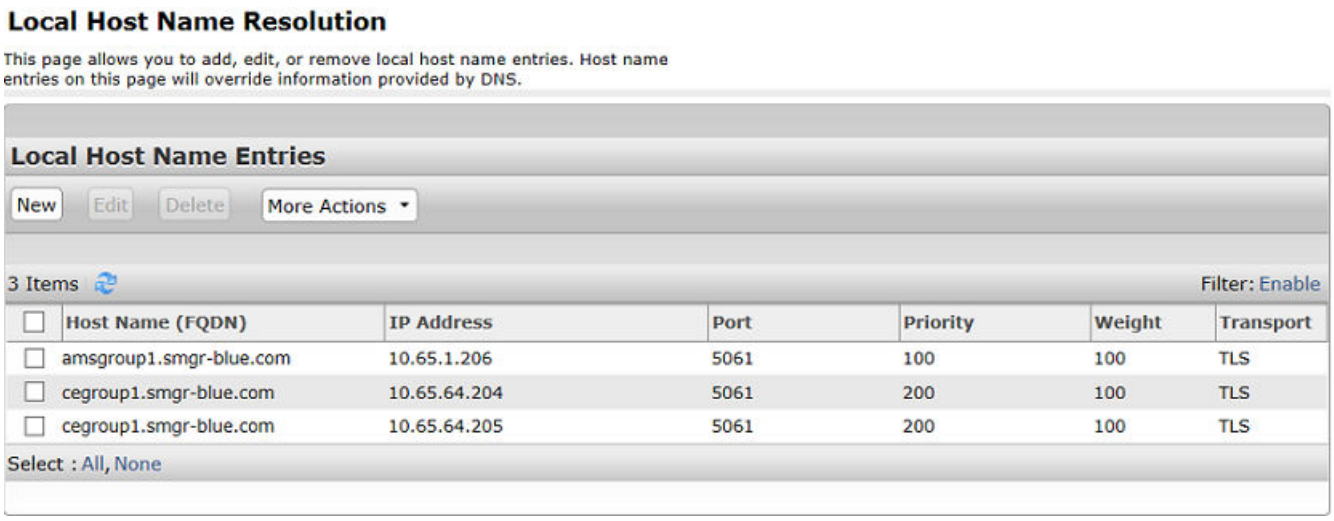
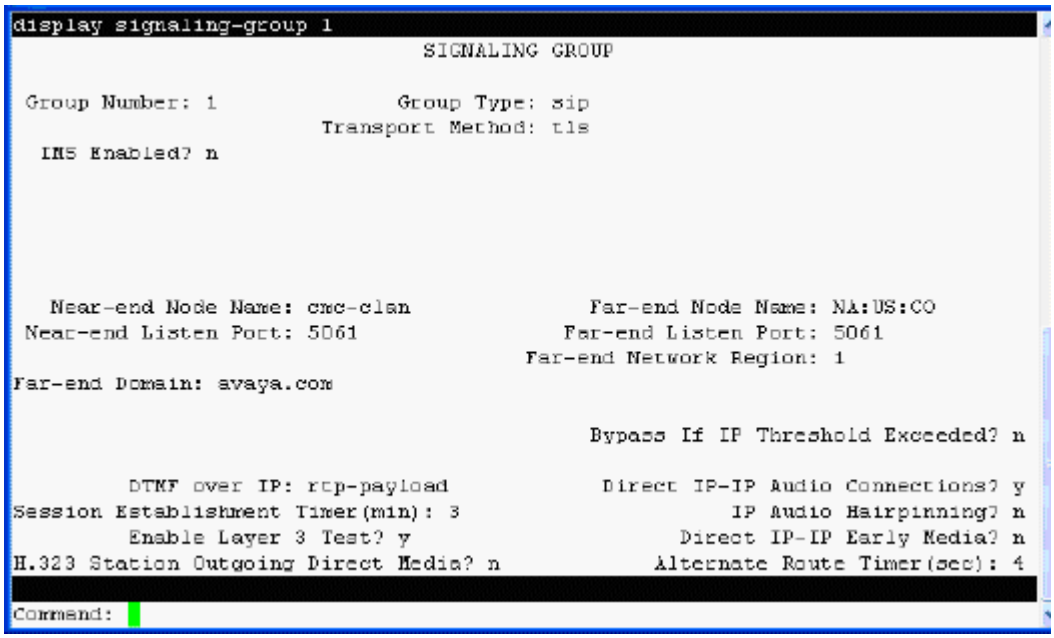


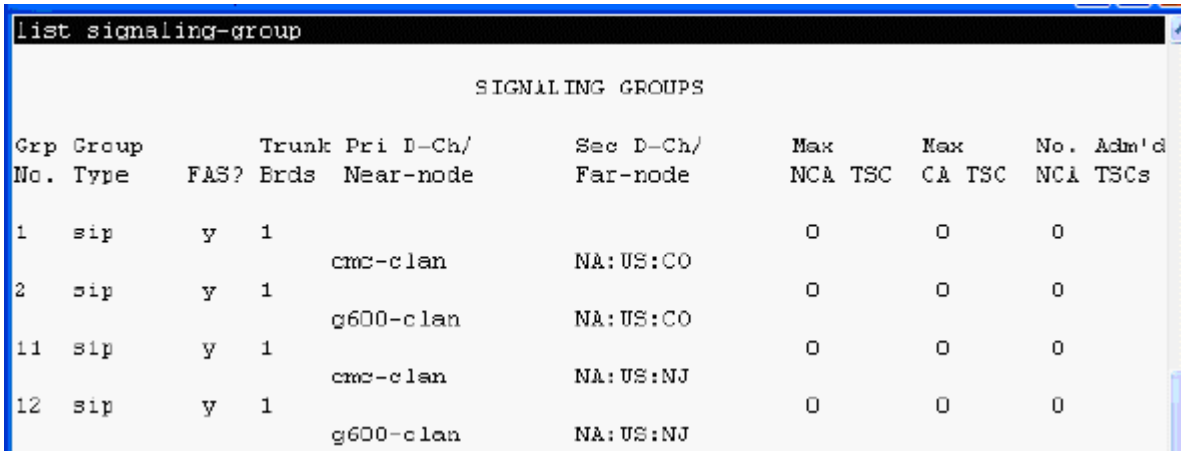
Figure 1: Local Host Name Resolution

The Local Host Name Resolution table is used for simple FQDN-to-IP address mapping and to specify the port and the transport protocol, as shown in the figure *Local Host Name Resolution*. For the simple case, Session Manager ignores the values of the **Port** and the **Transport** fields because these values are specified in the Entity Link table. To indicate that the values of these fields are specified in the Entity Link table, set the **Port** field to `5061`. If **Override DNS/SRV** is selected in the **SIP Entity** these ports are used instead of the Entity Link ports. The **Priority** field defines the priority for the host name resolution. A lower value has a higher priority. If the host name resolution fails with the first entry, the second entry is used to resolve the host name.

The Highlands Ranch Communication Manager instance requires four signaling groups and four trunk groups, one from each C-LAN to each of the Session Manager instances. The following figure illustrates the first signaling group:



The transport method and port match those specified in the entity link from each Session Manager to the Communication Manager instance. The **IMS Enabled** field must not be set for standard SIP scenarios. With the Level 3 tests enabled, Communication Manager perform OPTIONS monitoring of the Session Manager instances. The Bypass request must not be enabled. Communication Manager tests if the network characteristics between the media processors and Session Manager are suitable for media and Communication Manager must not send media to the Session Manager instance. The following figure lists the four signaling groups:



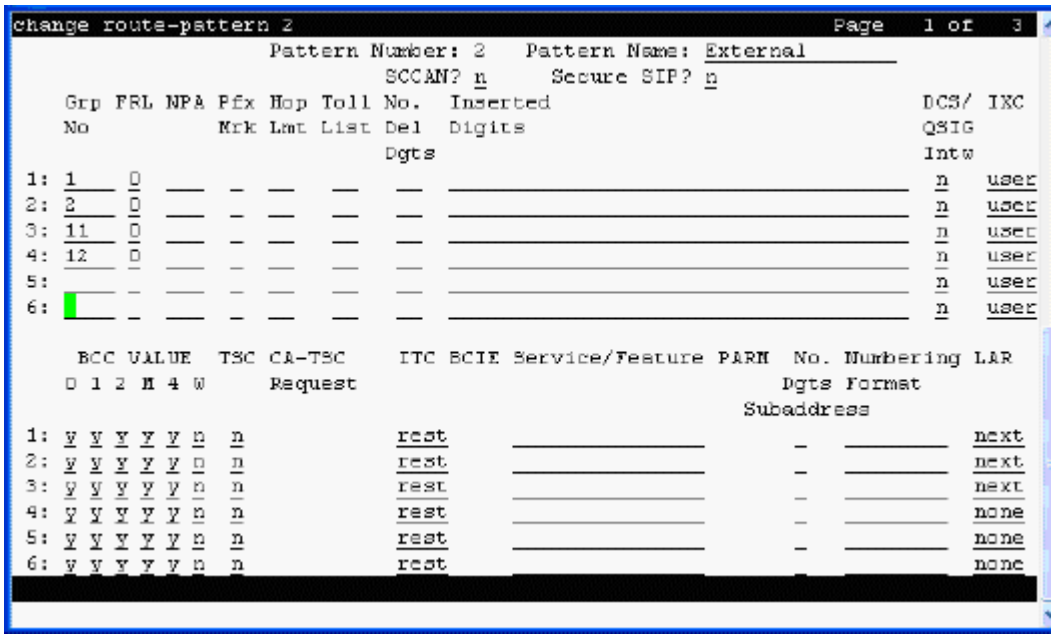
```
list signaling-group

                               SIGNALING GROUPS

Grp Group        Trunk Pri D-Ch/       Sec D-Ch/       Max      Max      No. Adm'd
No. Type    FAS? Brds  Near-node       Far-node        NCA TSC  CA TSC   NCA TSCs

1   sip      y   1                                     0        0        0
                     cmc-clan          NA:US:CO
2   sip      y   1                                     0        0        0
                     g600-clan         NA:US:CO
11  sip      y   1                                     0        0        0
                     cmc-clan          NA:US:NJ
12  sip      y   1                                     0        0        0
                     g600-clan         NA:US:NJ
```

The following figure illustrates an outgoing routing pattern, where all SIP trunk groups associated with the signaling groups use the same group number:



```
change route-pattern 2                                          Page   1 of   3
                  Pattern Number: 2   Pattern Name: External
                                SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                          QSIG
                                  Dgts                            Intw
 1: 1   0                                                         n    user
 2: 2   0                                                         n    user
 3: 11  0                                                         n    user
 4: 12  0                                                         n    user
 5:                                                               n    user
 6:                                                               n    user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
     0 1 2 M 4 W    Request                              Dgts Format
                                                      Subaddress
 1: y y y y y n  n           rest                                      next
 2: y y y y y n  n           rest                                      next
 3: y y y y y n  n           rest                                      next
 4: y y y y y n  n           rest                                      none
 5: y y y y y n  n           rest                                      none
 6: y y y y y n  n           rest                                      none
```

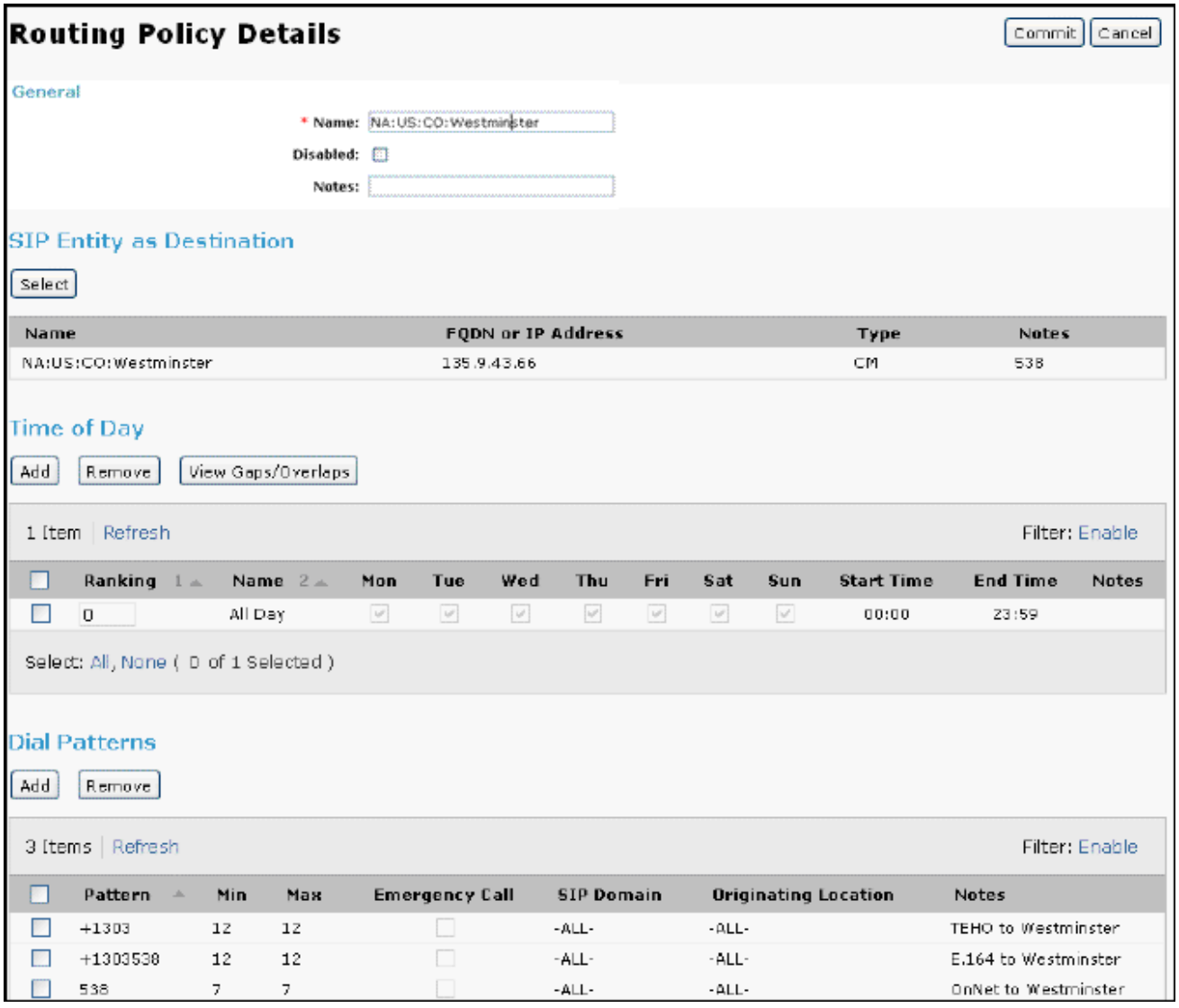
The Communication Manager instance attempts every connection to that local Session Manager instance — PBX and the NA:US:CO Session Manager instance are in Colorado — before trying the remote NA:US:NJ Session Manager instance in New Jersey. The **look-ahead routing (LAR)** field must be next on every preference that needs to skip to the next route when an error occurs.

Routing policies for PBXs

Routing policies indicate the rank of a particular SIP entity to determine routes. Multiple routing policies can be associated with a dial pattern for alternate routing. Additionally, the rank of a routing policy can be changed based on the time of day. For simple PBX routing, specific dial patterns are associated with one PBX and these dial patterns do not vary based on the time of day. For these types of routing policies, the name of the routing policy is identical to the name of the SIP entity.

The routing policy detail allows the association of the routing policy with the SIP entity. There is no time-of-day routing associated with this policy so only the All Day time range is added to the Time of Day section. Also this is a part of an alternate route so the rank is set to 0. The dial patterns are displayed here, but the patterns are defined on another form.

Figure 2: Routing Policy Details



Dial patterns for PBXs enterprise canonical numbering

The dial patterns defined in this solution enables the on-net 7-digit dialing feature between disparate PBXs.

In the details for the dial pattern, when you set the **SIP Domain** to `-ALL-`, the pattern matches with any domain. The originating location and routing policy associated with this dial pattern are `-ALL-` and the Westminster PBX SIP entity, respectively. This means a session created from anywhere with a user part of 538xxxx terminates at this particular PBX. The system denies the access to this dial pattern for calls originating from specific locations.

Network Routing Service

Network Routing Service (NRS) provides routing services to VoIP solutions based on CS1000. Apart from the SIP proxy support, NRS also acts as an H.323 gatekeeper and supports the mobility feature of the UNISTIM heritage Nortel IP phones. NRS consists of the following three servers:

- SIP Proxy Server (NRS-SPS) provides SIP proxy or registrar functions for SIP endpoints.
- Network Connect Server (NRS-NCS) supports the centralized CS1000 solution for IP clients and the UNISTIM phones.
- H.323 Gatekeeper (NRS-GK) provides H.323 gatekeeper functions to H.323 endpoints.

The NCS provides the following information to each endpoint:

- Primary CS1000
- Secondary CS1000
- Survivable CS1000

The NCS communicates to each CS1000 through a component named Terminal Proxy Server (TPS). The endpoints register to the TPS and the TPS requests the information from the NCS. The NCS locates the primary, the secondary, and the survivable servers for each NRS proxy user when the user logs in. You can define NCS user patterns and associate user patterns with up to three TPS servers along with the priority. Since a large number of users share the same server set, you can administer a range for the user pattern in order to match a large set of users.

CS1000 elements connect with Session Manager using SIP Trunks. CS1000 supports the SIP and non-SIP users directly. SIP endpoints connect with SIP Line Gateway (SLG), UNISTIM phones connect with TPS, and analog phones connect with the Media Gateway (MGW) element of CS1000.

Session Manager provides the SIP routing function for interconnecting CS1000 and Communication Manager instances in a star– based network topology.

While CS1000 and Session Manager or Communication Manager follow standard SIP, there are differences in the SIP dialect that these elements follow. The CS1000 adapter normalizes the SIP dialect to address the signaling difference and interconnect CS1000 and Communication Manager.

Configuring NRS

Before you begin

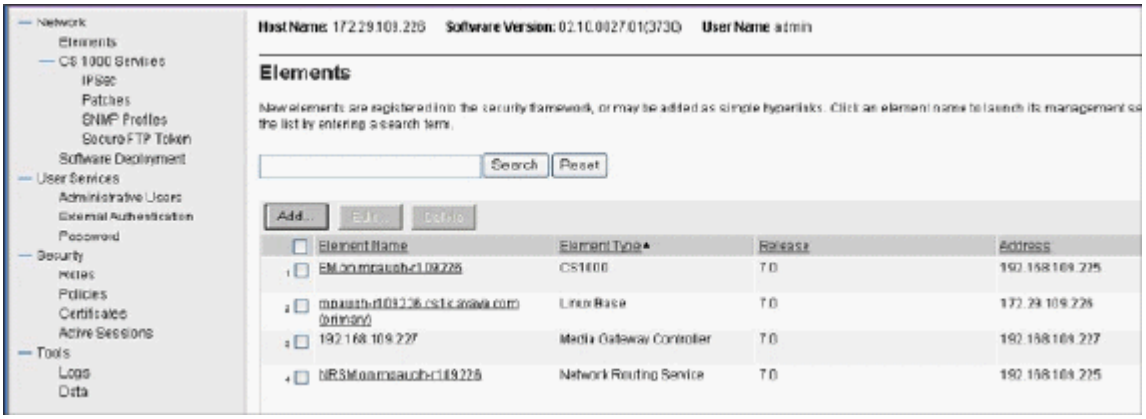
To ensure that all the SPS routing data is migrated to System Manager before you administer the connection of the gateways to Session Managers, convert the NRS data and import the data to System Manager using CS1000 NRS Data Conversion Tool on all SPS in the network.

About this task

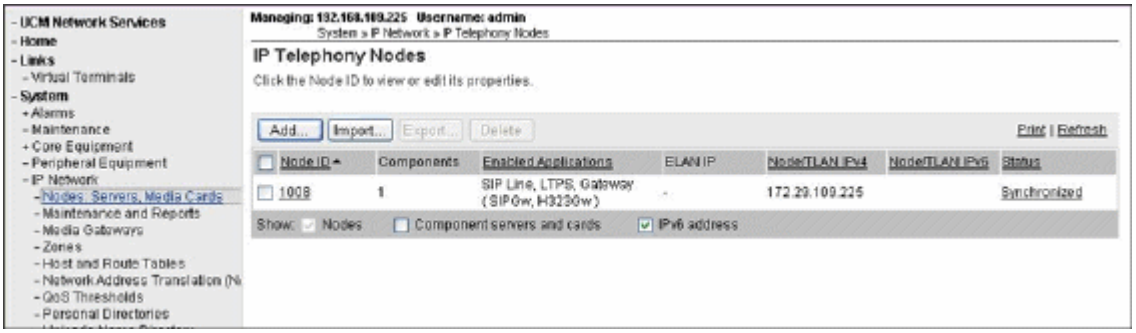
This section describes the NRS configurations on CS1000 with Network Connection Service (NCS).

Procedure

1. In Element Manager, click an element of **Element Type** “CS1000”.

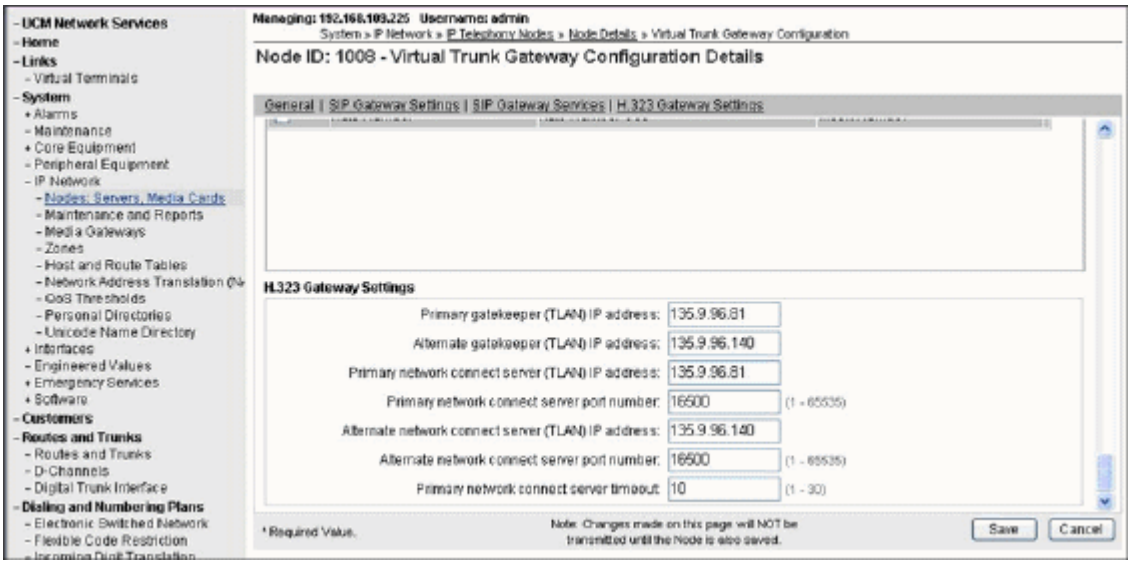


2. In the System Overview page, click **System** > **IP Network** > **Nodes: Servers, Media Cards**.



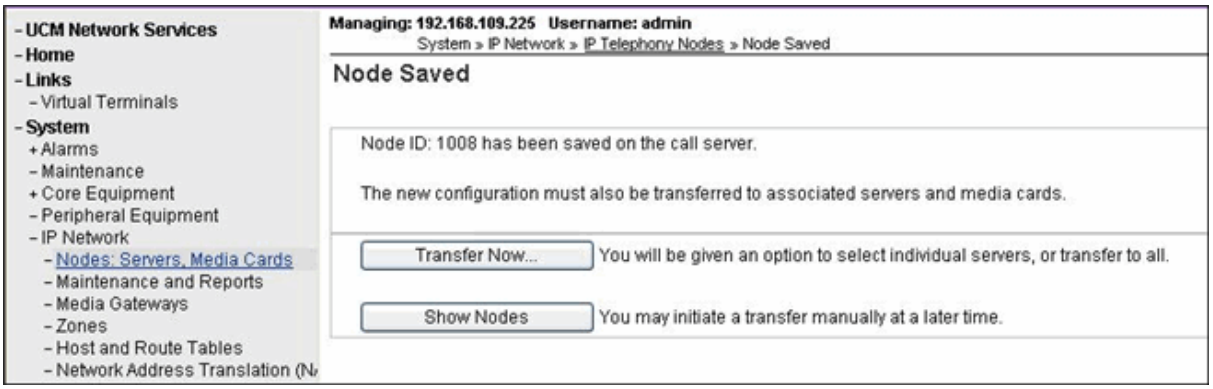
3. Click **Node ID** of the node that you want to configure.
4. Navigate to **Applications** and click to edit configuration section.

5. Click **Gateway (SIPGw & H323Gw)** and navigate to the **Network Connect Server** section.



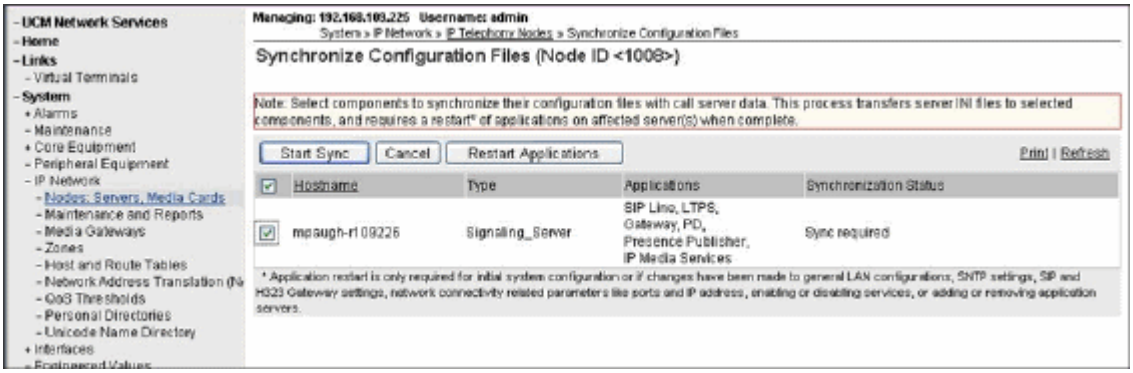
6. Enter the IP address of the Session Manager SIP entity in **Primary network connect server (TLAN) IP address**.
7. If required, enter a value for **Alternate network connect server (TLAN) IP address**.
8. Click **Save** to save your changes, and return to the Node Details page.
9. In the Node Details page, click **Save**.

   System Manager displays the Node Saved page.



10. In the Node Saved screen, click **Transfer Now...**

11. Select **Signaling Server(s)** in the Node ID column, and click **Start Sync** to synchronize the data with the signaling servers.



12. Click **Restart Applications** to restart the applications on the Signaling Server.

Next steps

Repeat the steps for the all NCS in the network.

NCS Integration

Adding a Terminal Proxy Server

Procedure

1. On the System Manager console, in **Elements**, click **Inventory** > **Manage Element**.
2. On the Manage Elements page, click **New**, and select type as **CS 1000 Terminal Proxy Server**.
3. On the New CS 1000 Terminal Proxy Server page, enter the name of the main or the primary call server, and the node IP address.
4. Click **Commit** to create the new instance.

Creating NRS Proxy User Rule

Procedure

1. On the System Manager Web console, click **Elements** > **Session Manager**.
2. Click **Application Configuration** > **NRS Proxy Users** to open NRS Proxy Users page.
3. Click **New** and enter the appropriate information for the new NRS Proxy User Rule.
4. Click **Commit**.

SIP service providers

In this case study, the network consists of three SIP service providers, such as AT&T, Verizon, and Hypothetical, connected through one Session Border Controller (SBC). These service providers can be connected directly. Verizon and Hypothetical are connected through a different, shared SBC.

For connections to SIP service providers to manage outgoing and incoming call traffic, each PBX must send the on-net 7-digit calls and the PSTN calls to Session Manager. Session Manager sends the 7-digit calls to other PBXs and converts the PSTN call signals to send the PSTN calls to the SIP service providers.

SIP service provider adaptations

SIP service providers send call requests that contain digit strings in the format of the network area of these service providers where the calls terminate.

In North America, the called party and the calling party numbers are 10-digit or 7-digit numbers. For outgoing calls (relative to the Session Manager network), SIP service provider may allow only calling party numbers from a block of purchased ones (that is, those they route into the Session Manager network over the SIP facility). Adaptation can be used for the necessary conversions.

AT&T adaptation

A call request from the AT&T network contains the calling party and the called party numbers in the 10–digit format for calls from North America and in the E.164 format for international calls. Session Manager converts the called party numbers in these calls to the E.164 format.

Session Manager converts the calling party and the called party number in the call requests to the AT&T network. For the AT&T network, the host part of request-URI in the call request is the IP address. For example, 135.9.43.69. Session Manager inserts the calling party number in request-URI in the 10–digit format for calls to North America and in the <011+digits> format for international calls. Session Manager sends the calling party number in the 10–digit format.

This adaptation uses the AttAdapter, which converts the digits and strips the History-Info header from call requests. The *AT&T* network is not compatible with this header that Communication Manager uses. The IP address that *AT&T* sends must be specified as a parameter to convert the host part of request-URI. Specify:

- **Module Name**: `AttAdapter`
- **Module Parameter Type**: `odstd=135.9.43.69`

Verizon Adaptation

A call request from the Verizon network contains the calling party and the called party numbers in the 10–digit format for calls from North America and in the E.164 format for international calls. Session Manager converts the called party numbers in these calls to the E.164 format.

Session Manager converts the calling party and the called party number in the call requests to the Verizon network. For the Verizon network, the host part of request-URI in the call request is the IP address. For example. 135.9.43.69. Session Manager inserts the calling party number in request-URI in the 10–digit format for calls to North America and in the <011+digits> format for international calls. Session Manager sends the calling party number in the 10–digit format.

This adaptation uses the *VerizonAdaptation* module. This module converts the digits and replaces the History-Info header to a Diversion header during the egress adaptation process and replaces the Diversion header with the History-Info header during the ingress adaptation process.

In this case study, the Verizon network and the Hypothetical network are connected through a common SBC. The SBC converts the domain in the SIP message request-URI to the IP address of the gateway.

Hypothetical Adaptation

The DigitConversionAdapter module supports the adaptation for other SIP service providers. Alternatively, an external SBC provides adaptation functions along with the DigitConversionAdapter module, which converts the digits in the SIP message.

A call request from the Hypothetical service provider contains the calling party and the called party number in the 10–digit format for calls from North America and in the E.164 format for international calls. Session Manager converts the called party number in this call to the E.164 format.

Session Manager converts the calling party and the called party number in the call requests to the Hypothetical network. For the Hypothetical network, the host part of request-URI in the call request is *hyposp.com*. Session Manager uses DNS to locate the correct server. Session Manager inserts the calling party number in request-URI in the <1+10 digits> format for calls to North America and in the <011+digits> format for international calls. Session Manager sends the calling party number in the 10–digit format.

A call request from PBX contains the calling party number in the enterprise-canonical format. During the egress adaptation process to the Hypothetical network, Session Manager converts these numbers to the 10–digit format through the Digit Conversion for Outgoing Calls table. Specifying:

- The origination address in the Address to modify column ensures that Session Manager only modifies the calling party numbers in the P-Asserted-Identity header of the call request.
- The destination address in the rule that converts the number from the E.164 format to the format for calls to North America ensures that Session Manager modifies only request-URI.

This adaptation uses the DigitConversionAdapte module. The *hyposp.com* domain parameter modifies host part of request-URI Specify:

Egress URI Parameters: `user=phone` because the Hypothetical network requires this value in request-URI.

Note:

The **Adaptation Name** and **Egress URI Parameters** fields support free format text. These fields scroll horizontally so their complete values may not show on the form without active selection and scrolling. The system does not validate the values in these fields, so ensure that you enter the correct values.

SIP entities for SIP service providers

The SIP service provider connections are different from the PBX connections. The SIP service providers connect through SBC and log CDRs.

In this case study, the AT&T network is connected through a dedicated SBC, while the Hypothetical and the Verizon networks connect through one SBC.

Single SIP entity connected to Session Border Controller

A single SIP entity connected to Session Border Controller (SBC) ensures that SBC represents only one SIP entity. Session Manager does not need to determine the SIP entity that sends call requests through this SBC instance that connects to a single SIP entity. The SIP entity configuration is similar to other SIP entities.

In this example:

- The **FQDN or IP Address** is the IP address of SBC.
- The **Type** is `SIP Trunk`.
- The **Call Details Recording** is `egress` to record only outgoing call requests. Session Manager logs CDRs of incoming calls only for a SIP entity where **Call Details Recording** is `egress` or `both`.

An entity link is created for each Session Manager to this SIP entity. In this case, set:

- The protocol to `UDP`. Session Border Controller can also be used to translates UDP that the TCP protocol of AT&T supports.
- Session Border Controller to accept messages from all the Session Manager instances and transmit messages to all Session Manager instances for resiliency.

Multiple SIP entities connected to Session Border Controller

In this example, the service providers *Verizon* and *Hypothetical* connect to Session Border Controller (SBC) through an IP address that FQDN specifies. There is no entry in the Local Host

Name Resolution table. The Session Manager resolves the IP address through the DNS server of the network.

The entity links specified for this SIP entity uses standard ports for TCP.

The gateway of the Hypothetical service provider connected to Session Border Controller is located in the same location as the gateway of the Verizon service providers. The bandwidth management limits apply to both these SIP entities, but the time zone for the time-of-day routing differs. The service providers connect to Session Border Controller with the same physical link, but the gateways are located in different time zones and contain different tariffs based on the time zone of these gateways. The Hypothetical service provider does not support SIP monitoring.

Administer this configuration as a special entity link. The ports are nonstandard on both sides of the entity link. Administer Session Border Controller to send messages from the Hypothetical service provider gateway to port 5062 using the TLS protocol and accept connections through port 5062 to forward these call requests to the Hypothetical service provider, which might have different ports. Different ports for the service provider ensures that Session Manager can distinguish call traffic between the SBC IP address and SIP entities.

Routing policies for SIP service providers

The routing polices *Alternate-AT & T*, *Alternate-Verizon*, and *HypotheticalSP* are the primary policies that determine the routes to the SIP service providers. The *Alternate-BaskingRidge* polices are for tail-end hop-off, and the *Ap800* polices are for some systems.

Simple routing policy for SIP service providers

The *HypotheticalSP* is a simple routing policy. There is no alternate routing, so the rank of the routing policy is set to `0`. A unique dial pattern references to only this policy.

Alternate routing policy for SIP service providers

The *Alternate-AT&T* and *Alternate-Verizon* routing policies work together. The names of such routing policies have a prefix “Alternate” and contain the relative ranking of these routing policies in the **Notes** field. In this example, the rank of *Alternate-AT&T* is set to 10 and the rank of *Alternate-Verizon* is set to 20, so any dial pattern that references both these routing policies prefers *Alternate-AT&T*.

Rank policies in increments of 10 at the start so that you can intermediately rank the other policies that you add later without renumbering.

When routing sessions, Session Manager chooses the lower ranked or the higher numbered routing policy if :

- SIP monitoring has marked all the endpoints identified by the higher ranked or lower numbered routing policies as down, or
- The call fails to establish due to a bad return code or TimerB expiration, or
- The call fails to establish because the managed bandwidth at the destination location is exhausted.

Dial patterns for SIP service providers

The E.164 dial patterns determine routes for calls from PSTN through the SIP service providers. These dial patterns are marked in the **Notes** field as:

- `APP` to send call requests directly to a SIP foundation server. These are marked.
- `TEHO` for Tail-End Hop-Off.
- `E.164` to send DID numbers from the SIP service provider to the relevant PBX. These entries are relatively low because PBXs own the full bank of DID numbers. For example, the Westminster PBX owns all numbers from +13035380000 to +13035389999. If this PBX does not own these range of numbers, the discrepancy can be solved with more entries:
  - either with a larger set of more explicit ones to send fewer numbers to the given PBX.
  - or with more explicit ones that send call requests with exceptions elsewhere, like the +13035389077 entry.
- `PSTN` for the entries that start with a plus sign (+) are generic patterns that match any E.164 number which does not match a more explicit entry.

As shown in all the adaptations, all PBXs and incoming service provider calls have their destination addresses converted to E.164. For example, a plus sign (+) is prefixed, so that matching dial patterns is more uniform and predictable.

The first entry in the table with a plus sign (+) is distinct from the second, because it only applies if the destination domain is avayalabs.com. The second pattern matches any other domain.

Simple routing policy for dial patterns of SIP service providers

The simple routing policy involves sending a call request to an address in the E.164 format and the avayalabs.com domain only through the HypotheticalSP routing policy.

In this case study, the BaskingRidge:Research SIP entity uses the avayalabs.com domain. Session Manager sends all the numbers in the E.164 format that do not match other dial patterns through the HypotheticalSP SIP service provider.

Alternate routing policy for dial patterns of SIP service providers

The alternate routing policy for dial patterns entry selects two distinct routes for all the numbers in the E.164 format except those numbers that terminate at the avayalabs.com domain.

If a call request originates from San Jose, the dial pattern selects the HypotheticalSP service provider. If a call request originates from other locations, the dial pattern selects the Alternate-AT&T or the Alternate-Verizon service providers.

Dial Plan Ranges

Note:

Before enabling the Dial Plan Range feature in an enterprise system, ensure that all Session Manager installations are of version 6.3.4 or later.

Using a Dial Plan Range, you can specify number ranges in the Session Manager Dial Plan.

A valid range has the following characteristics:

- Two integers separated by a colon (:)
- (Optional) A plus sign (+) can precede the numbers. If one number begins with a (+) sign, then the other number must also begin with a (+) sign.
- The number to the left of the colon must be numerically less than the number to the right. These numbers cannot be equal.
- The numbers on the left and right of the colon must be of the same length.

Note:

The Global Settings **Dial Plan Ranges** must be enabled on the Session Manager Administration page.

The valid pattern format is [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23}. For example, +493420479242000:+493420479242999.

You can enter a range that is a subset or superset of an existing range or pattern. The smaller range is a sub-range. Sub-ranges have the following limitations within the same location and domain:

- Two sub-ranges must not match each other.
- A sub-range must not match a pattern.
- A sub-range must not cross the starting or end of another range.

Dial Plan Range Example

If the Dial Plan Range is 5000:5499, you can specify the sub-ranges as:

- 5002:5011
- 5000:5499 and 5492:5499, where the end of sub-range and range match.

- 5000 (single entry) and 5000:5009, where the beginning of sub-range and range match.

The sub-range 5300:5555 is not valid because the sub-range crosses the end of the range.

Note:

When routing, Session Manager performs more efficiently using a smaller range rather than a larger range or longer pattern.

Multilocation Dial Plan

The Communication Manager location of a user is determined from the Communication Manager station form or from the *ip-address* of the endpoint if this address is administered on the Communication Manager *ip-network-map* form. If a user has a specific location other than the administered global location, then both the global and location specific dial plan entries are sent to the endpoint. If the user is not administered with a Communication Manager location, then only the global dial plan entries are sent to the endpoint. This information is used by the endpoint to determine the permitted dial sequences for a user.

Note:

For Session Manager releases earlier than 6.2, upon user login, endpoints receive all the administered Communication Manager dial plan entries.

Creating Dial Patterns

Use the Dial Patterns page to create Dial Patterns and to associate the Dial Patterns to a Routing Policy and Locations.

Note:

You cannot save a dial pattern unless you add at least a routing policy or a denied location.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Dial Patterns**.
2. Click **New**.
3. Enter the Dial Pattern General information in the General section.

   Note:

   You can provide a Domain to restrict the Dial Pattern to the specified Domain.
4. Under the Originating Locations and Routing Policies section, click **Add**.
5. Select all the required Locations and Routing Policies that you want to associate with the Dial Pattern.
6. When you have finished making your selections, click **Select**.
7. To deny calls from the specified locations:
   a. Click **Add** under the Denied Locations section.

b. Select all the Locations that are to be denied.

c. When you have finished making your selections, click **Select**.

8. Click **Commit**.

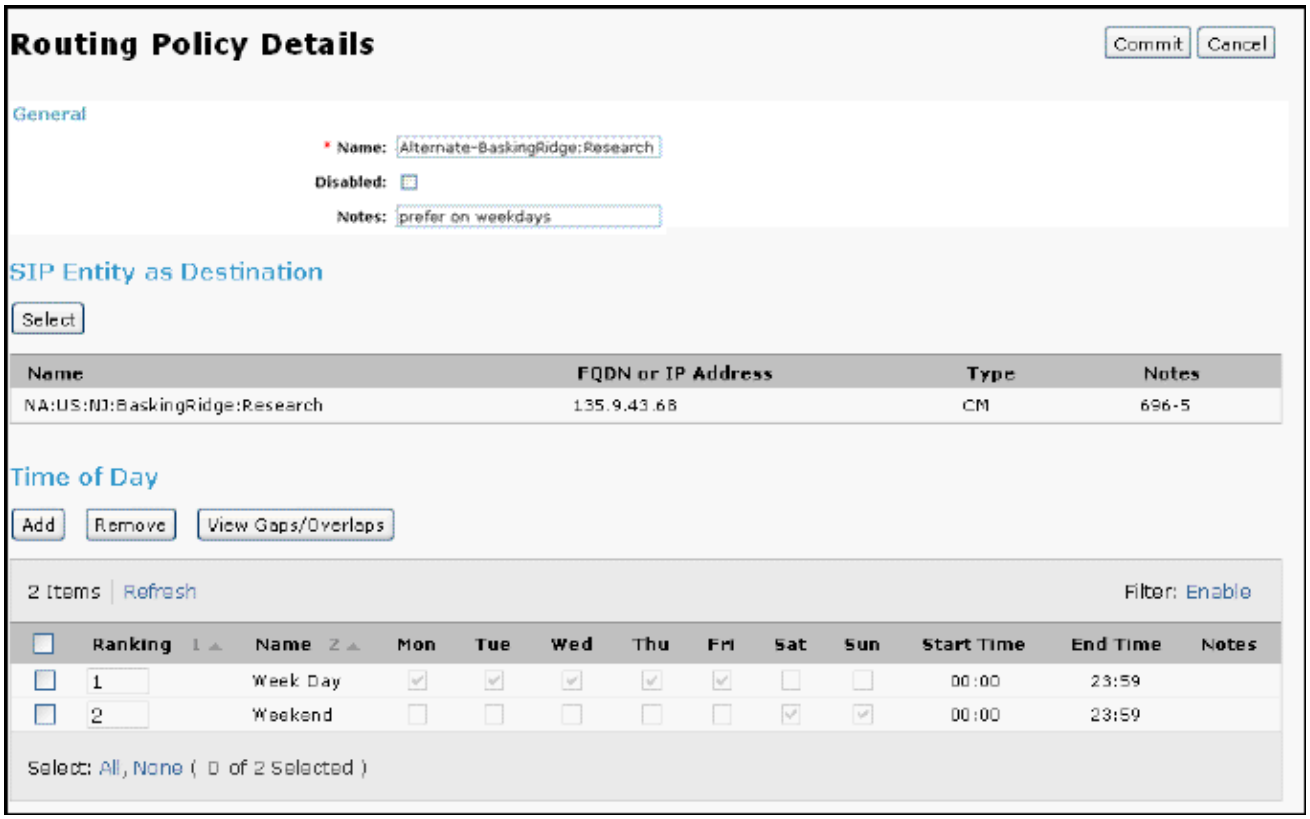
Tail-end hop-off

Tail-end hop-off (TEHO) supports the routing of call requests that contains numbers in the E.164 format. TEHO processes these calls as if PBXs send all calls from PSTN to Session Manager.

Session Manager sends certain call requests that contain numbers in the E.164 format to PBX that has a dedicated PSTN trunk. In this case study, the Basking Ridge PBXs process call requests to the 908 area code. The dial pattern entry identifies one of four routing policies.

Set the *Alternate-AT&T* and the *Alternate-Verizon* entries as shown earlier. These entries are ranked as 10 and 20, respectively. The ranks of the other *Alternate-BaskingRidge:Research* and *Alternate-BaskingRidge:HQ* entries vary according to the time of day.

Figure 3: Routing Policy Details



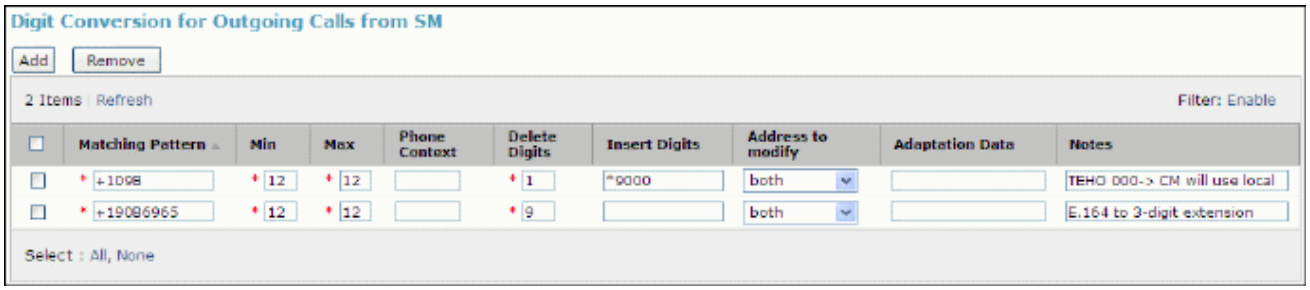
BaskingRidge:Research has a rank of 1 on weekdays and a rank of 2 on weekends, and BaskingRidge:HQ has a rank of 2 on weekdays and a rank of 1 on weekends.

Thus the routing policy and so SIP entity ordering is:

- Weekdays:
  - BaskingRidge:Research
  - BaskingRidge:HQ
  - AT&T
  - Verizon
- Weekends:
  - BaskingRidge:HQ
  - BaskingRidge:Research
  - AT&T
  - Verizon

The Basking Ridge PBXs must be set up to send call requests through the SIP service provider trunks if the PSTN trunks fail. To ensure this redundancy and to simplify routing, these PBXs send all PSTN calls to Session Manager. However, if a 908 area code call is sent back to these PBXs, the PBXs send this call to Session Manager again, which forms a loop. To mitigate this scenario, the adaptation process changes the destination address in call requests to ensure that the PBXs send the call request to the PSTN trunks rather than Session Manager.

Figure 4: Adaptation for BaskingRidge:Research



The +1908 dial pattern entry modifies all 908 area code numbers to be destined for *9-000-1-908-xxx-xxxx. The PBX must recognize this to be a specially-routed number. In this case, for Communication Manager, the *9 is the ARS access code and the 000 is a digit string that can be used for this unique identification.

Application systems

The two SIP application types in this case study are Avaya Aura® Messaging and Experience Portal.

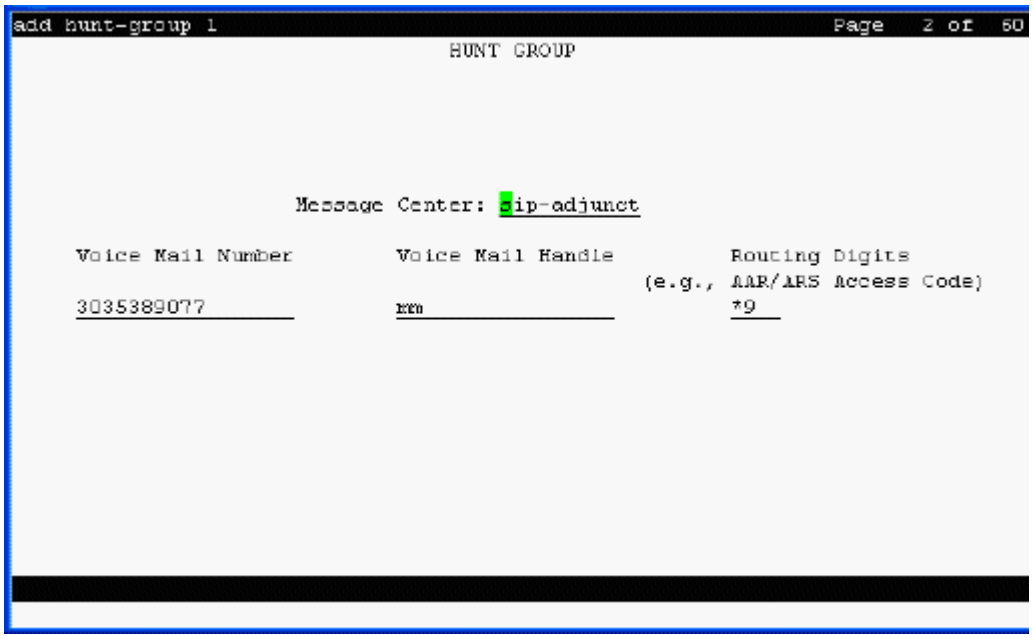
These applications process incoming and outgoing calls. Avaya Aura® Messaging primarily processes incoming calls. Like any SIP entity, you can use this adaptation for digit conversion, but that is needed primarily for existing Avaya Aura® Messaging or Experience Portal applications with

existing dial plans. New applications can be provisioned to use the full length E.164 numbers (save possibly to delete and add the +) internally.

Avaya Aura® Messaging

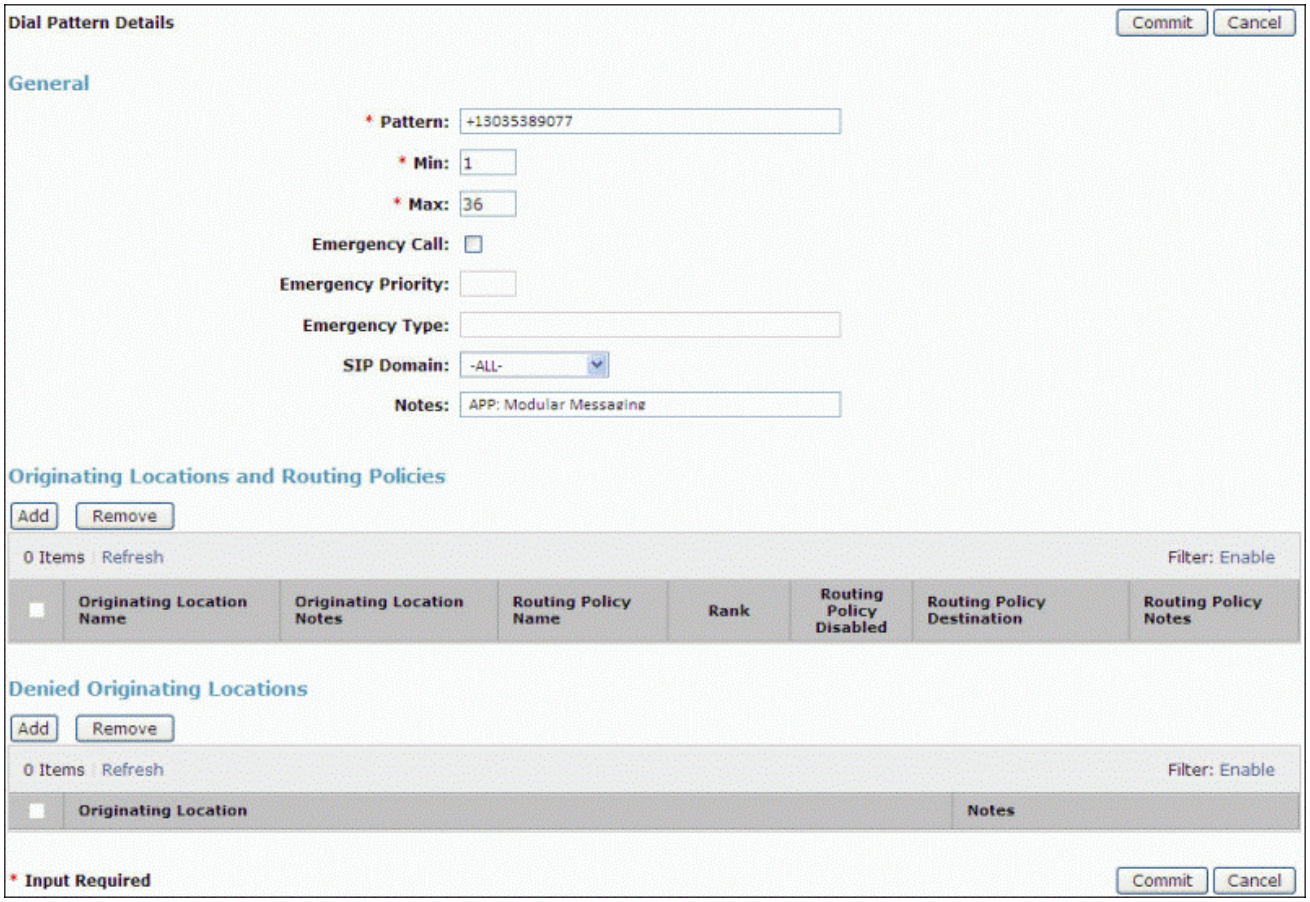
On each Communication Manager instance, Avaya Aura® Messaging is associated with a hunt group. Avaya Aura® Messaging is assigned a routing digit string to determine routes of covered and direct media sessions along with a Voice Mail handle for MWI subscriptions and notifications. Session Manager must send these media sessions from the Communication Manager instance to Avaya Aura® Messaging.

On the Communication Manager instances in this case study the hunt group data is:



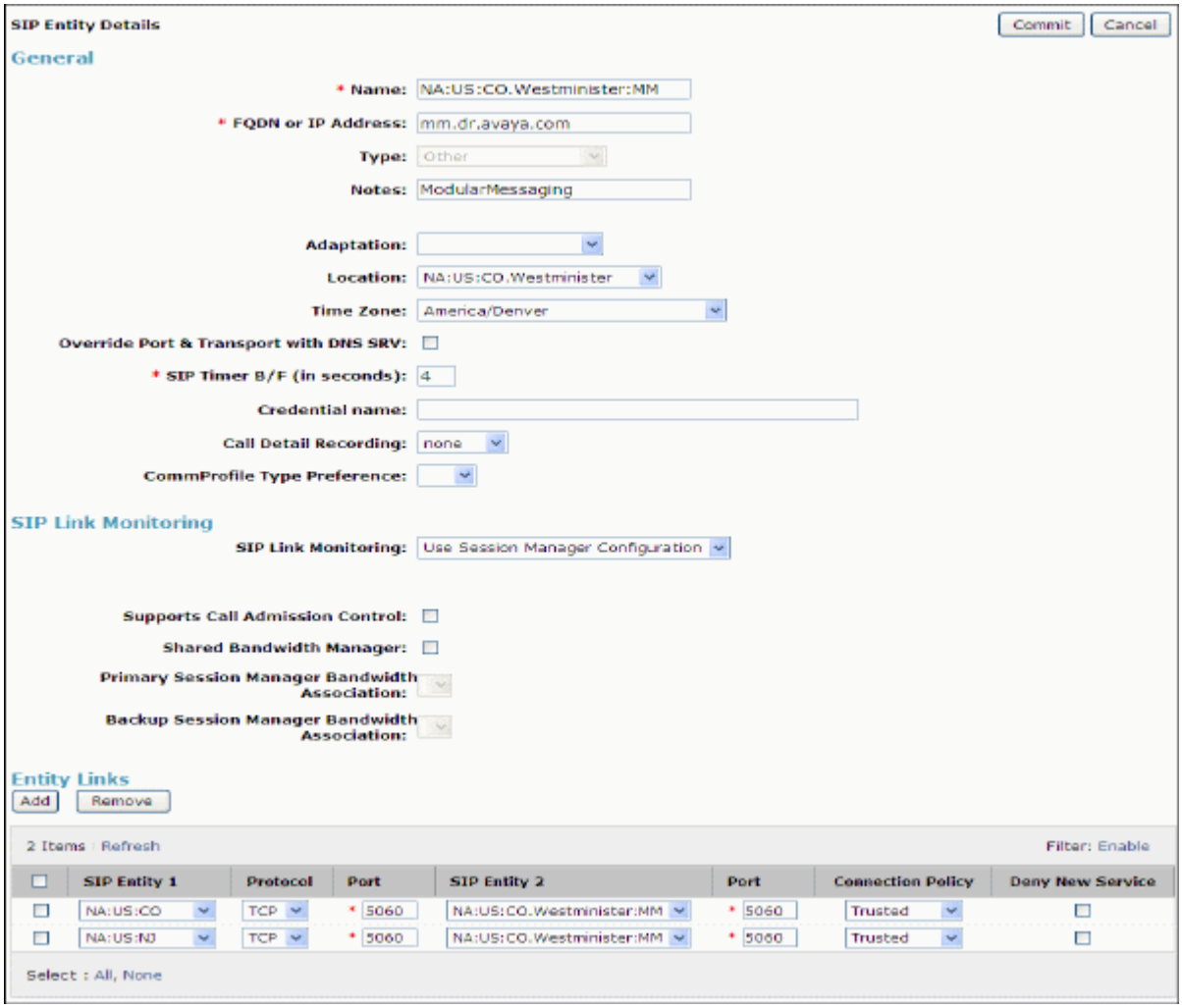
The number 3035389077 is routed through the dial pattern:

Figure 5: Dial Pattern Details



The dial pattern identifies a SIP entity. You can enable Call Detail Recording. Implementing bandwidth management on Avaya Aura® Messaging is useful in the local area. However, limited bandwidth may reduce the number of calls. The Local Host Name Resolution table provides multiple IP addresses along with the ports and transport protocol information.

Figure 6: SIP Entity Details



If you check **Override Port & Transport with DNS SRV**, the port or transport information administered for the entity link is overridden by information obtained from DNS and from LHNR entries.

SRV records within the DNS server accessed by the Session Managers provide the necessary overridden information, but it is much easier to include this information in the Local Host Name Resolution table.

In this particular case, TLS connections are made to port 5061 of both MASs with the IP addresses. Load balancing is done on a statistically weighted basis, because each MAS is at the same priority. About 10/30 or one-third of the calls are loaded to MAS at 135.9.43.34 while two-thirds of the calls go to the other MAS. This ratio is valid over many calls. There is a possibility that for any given small set of calls, more or less than 1/3 of the calls go to the first MAS.

The MWI subscribe and notify sessions are routed with the handle specified in Communication Manager, which is mm@avaya.com in this case. Handles are currently routed using the regular expressions table.

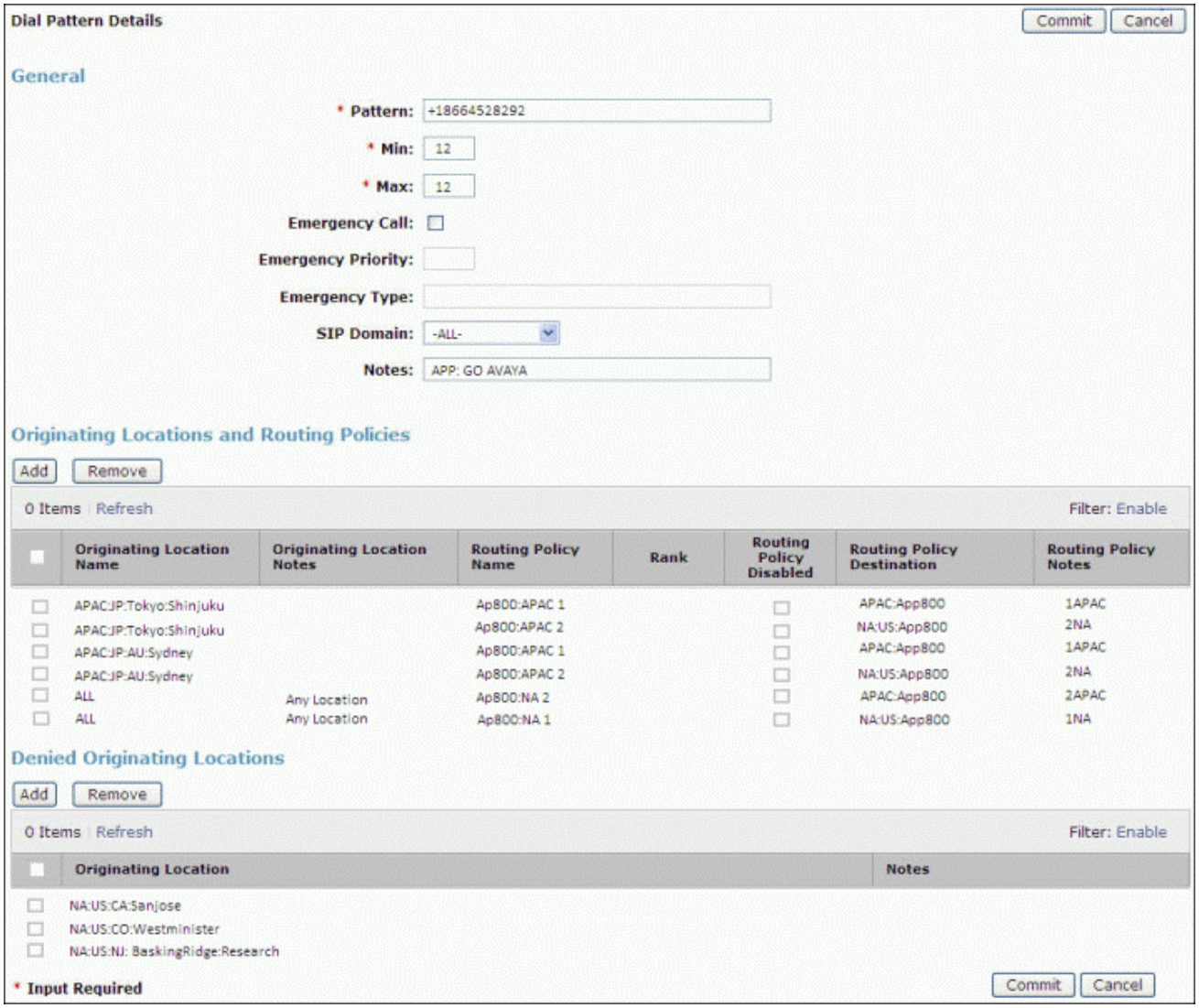
The pattern here is very precise with no meta character pattern matching symbols only because a specific handle needs to be matched. The fewer meta characters assure more efficient match. The routing policy selected is the same one selected by the dial pattern of the number associated with the Communication Manager hunt group, +13035389077.

Experience Portal-like SIP application service

The other SIP application service in this case study is similar to how calls are routed to the Experience Portal. The Experience Portal administration itself is not described nor is this application fully set up to make outgoing calls. Adaptation would most likely be necessary for this.

This Experience Portal-like application is reached when you dial 1-866-GO-AVAYA. The dial pattern is quite complex:

Figure 7: Dial Pattern Details



To paraphrase the routing policy selection, without actually listing the routing policies themselves:

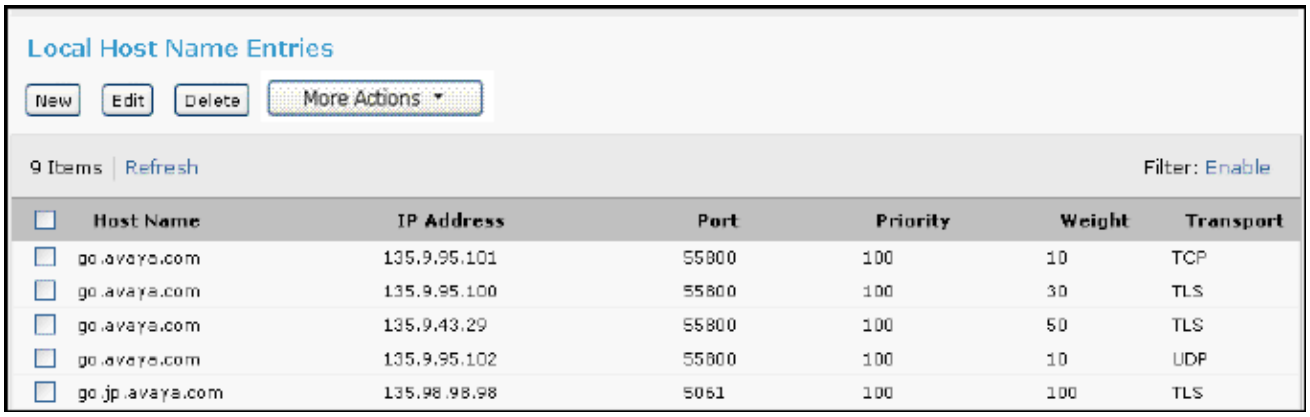
- SIP entities in the locations Tokyo and Sydney prefer the APAC:App800 foundation server, a SIP entity, and falls back to the NA:US:App800 server. There are, however, no SIP entities associated with these locations yet.
- All other SIP entities including the ones defined in this case study PBX and SIP service provider alike prefer the NA:US:App800 server.
- SIP entities in the SanJose, Westminster, and BaskingRidge:Research locations cannot route calls to this dial pattern. The calls are denied.

The SIP entities for the foundation servers are similar.

These SIP entities have different FQDNs, are in different locations and time zones, but both the entities override the port and transport specified in the entity link.

The Local Host Name Resolution table shows why this override is necessary at least in the case of the *NA:US:App800* SIP entity. The *APAC:App800* SIP entity just has one associated IP address that uses the standard TLS port.

Figure 8: Local Host Name Entries



The *NA:US:App800* entity selects one of four different server IP addresses based on a total weight of 100. Ten percent of the time it goes to 135.9.95.101 with TCP, 30% to 135.9.95.100 with TLS, 50% to 135.9.43.29 with TLS, and the remaining 10% to 135.9.95.102 with UDP.

IPv6

The Avaya Aura® Session Manager supports IPv6 addresses in addition to IPv4 addresses. Session Manager supports a dual stack architecture. Therefore, you can simultaneously connect Session Manager with endpoints and SIP entities that use IPv4 and IPv6 addresses. When one party in a call uses IPv4 addressing and the other party uses IPv6 addressing:

- Session Manager provides signaling interworking
- Communication Manager provides media interworking

A large variety of address combinations are possible in SIP signaling. For example, messages can have:

- Only IPv4 addresses
- Only IPv6 addresses
- A mixture of IPv4 and IPv6 addresses

In addition, the address family used in media stream negotiations is independent of the SIP signaling address family. Session Manager functions as the registrar and interconnecting agent to connect SIP entities of different types. Therefore, Session Manager must handle signaling interworking to ensure that a network comprising mixed address family elements works properly. Before forwarding a SIP message to the next SIP entity or endpoint, Session Manager uses the Address Family Interworking Function (AFIF) to adapt the SIP messages to meet the needs of the next hop. For example, consider that an incoming message has IPv4 addresses and the destination SIP entity supports only IPv6 addresses. Session Manager uses AFIF and replaces the IPv4 addresses with IPv6 addresses in the request. Similarly, after receiving a response, Session Manager uses AFIF to reverse the adaptation and converts the IPv6 messages to IPv4 messages.

Session Manager uses the address family of the SIP entity or endpoint and the type of the link to determine their address type and then uses AFIF.

Support for deployment on Amazon Web Services

You can deploy Session Manager on Amazon Web Services.

Amazon Web Services (AWS) is a cloud services platform that enables the enterprises to securely run the applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3). Supporting Avaya applications on the AWS Infrastructure as a service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to the operational expense (OPEX).
- Reduces the maintenance cost of running the data centers.
- Provides the common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

Chapter 3: New user setup case study

Overview

Fred Stevens just joined Avaya located in Highlands Ranch. He is the new Network Engineer and will be working in the Network Management group. The following case study describes the configuration of the Avaya 9600-Series IP telephone of Fred in the enterprise network using the Avaya Aura® Session Manager User Registration feature and Avaya Aura® Communication Manager Feature Server supports the Session Manager. To improve reliability of the configuration, the SIP telephones are registered to both Session Managers. The sample configuration includes Avaya Aura® Communication Manager Feature Server supporting IP Multimedia Subsystem (IMS)-SIP users registered to Avaya Aura® Session Manager. Communication Manager Feature Server is connected to both Session Managers through IMS-enabled SIP signaling groups and associated SIP trunk groups.

The overall configuration involves:

1. Administering of Communication Manager Feature Server using System Access Terminal (SAT) using the following steps:
    a. Verifying system capacities
    b. Configuring Trunk-to-trunk transfers
    c. Configuring IP Codec set
    d. Configuring IP Network region
    e. Configuring IP Node names and IP addresses
    f. Configuring SIP signaling groups and Trunk groups
    g. Configuring route pattern
    h. Administering numbering plan
    i. Administering AAR Analysis
    j. Configuring stations
2. Configuring Avaya Aura® Session Manager to support registrations of the telephone.

Before you set up the user, it is important to synchronize the CM Station Data to System Manager as shown in the section *Synchronize CM station data to the System Manager*. The various stages to setup the user are:

1. Adding two SIP entities for Session Manager with listen ports
2. Adding the Session Manager instances for both primary and secondary Session Manager
3. Adding SIP domains

4. Adding application sequences
5. Adding survivability server
6. Adding home location
7. Adding a user or SIP end-point

The setup includes the following configuration:

- Two Avaya Aura® Session Managers running on separate Avaya S8300E Servers are deployed as a pair of active-active redundant servers.
- Avaya Aura® Communication Manager Feature Server runs on an Avaya S8300D server with Avaya 450 Media Gateway.

Configuring Avaya Aura® Communication Manager Feature Server

Feature server

A feature server provides Communication Manager features to the SIP endpoints registered with Session Manager. The feature server uses the half-call model of IP Multimedia Subsystem (IMS). The feature server connects to Session Manager through an IMS-enabled SIP signaling group and an associated SIP trunk group.

The feature server supports full application sequencing.

The feature server has the following limitations:

- Does not support routing of PSTN calls directly to ISDN trunks for IMS users. You must administer the dial plan to route all PSTN calls to Session Manager over the IMS trunk group.
- Does not support traditional endpoints, such as DCP, H.323, ISDN, and analog.
- Does not support G650 Media Gateway.

Evolution server

An evolution server is similar to the traditional Communication Manager server. The evolution server provides Communication Manager features to both SIP and non-SIP endpoints. The evolution server uses the full-call model. The evolution server connects to Session Manager through a non-IMS Signaling group. Session Manager handles call routing for SIP endpoints and enables SIP endpoints to communicate with all other endpoints that are connected to the evolution server.

If you configure Communication Manager as an evolution server:

- H.323, digital, and analog endpoints register with Communication Manager.

- SIP endpoints register with Session Manager.
- All endpoints receive service from Communication Manager.

The evolution server supports a limited form of application sequencing.

Related links

Application sequencing in the evolution server on page 44

Application sequencing in the evolution server

The evolution server supports a limited form of application sequencing:

- Non-SIP users receive implicit application sequencing.
- SIP users receive explicit application sequencing with the following conditions:
  - Origination sequencing: The sequenced applications must be before Communication Manager in the sequence vector.
  - Termination sequencing: The sequenced applications must be after Communication Manager in the sequence vector.

Related links

Evolution server on page 43

Verifying System Capacities

Verifying Off-PBX telephone capacity

Procedure

Type **`display system-parameters customer-options`** command. On Page 1, verify the limit specified for the number of **Maximum Off-PBX Telephones - (OPS)**.

```
display system-parameters customer-options                  Page   1 of  11
                              OPTIONAL FEATURES
G3 Version: V16                              Software Package: Enterprise
       Location: 2                                System ID (SID): 1
                                                            USED
                              Platform Maximum Ports: 6400  55
…
                    Maximum Off-PBX Telephones - EC500: 9600  0
                    Maximum Off-PBX Telephones -   OPS: 9600  11
                    Maximum Off-PBX Telephones - PBFMC: 9600  0
…
```

Figure 9: Display system — parameters customer — options, Page 1

Verifying SIP trunk capacity

Procedure

Type **display system-parameters customer-options** command. On Page 2, verify that the limit specified for number of **Maximum Administered SIP Trunks** is sufficient.

Figure 10: Display system — parameters customer — options, Page 2

```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES
IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 500    0
           Maximum Concurrently Registered IP Stations: 18000  0
  Max Concur Registered Unauthenticated H.323 Stations: 100    0
…
                   Maximum Video Capable IP Softphones: 0      0
                       Maximum Administered SIP Trunks: 4000   40
…
```

Verifying AAR or ARS Routing feature

About this task

To simplify the dialing plan for calling stations on Communication Manager Evolution Server, you need to verify that the AAR or ARS features are enabled on the system.

Procedure

Type **display system-parameters customer-options** command. On Page 3, verify the following features are enabled:

- In ARS?, enter y.
- In ARS/AAR Partitioning?, enter y
- In ARS/AAR Dialing without FAC?, enter y.

```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

A/D Grp/Sys List Dialing Start at 01? n                            CAS Main? n
Answer Supervision by Call Classifier? n                  Change COR by FAC? n
                                   ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                        DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? n
…
```

Figure 11: Display system — parameters customer — options, Page 3

Verifying Private Networking

Procedure

Type **display system-parameters customer-options**. On Page 5, verify that the Private Networking is set to y.

```
display system-parameters customer-options                    Page   5 of  11
                              OPTIONAL FEATURES
                  Port Network Support? y              Time of Day Routing? n
                       Posted Messages? n      TN2501 VAL Maximum Capacity? y
                                                   Uniform Dialing Plan? y
                     Private Networking? y    Usage Allocation Enhancements? y
               Processor and System MSP? y
                     Processor Ethernet? y               Wideband Switching? n
...
```

Figure 12: Display system — parameters customer — options, Page 5

Configuring Trunk to Trunk transfers

About this task

If you enable this feature it poses significant security risk by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, define a COS to allow trunk-to-trunk transfers for specific trunk groups. For more information about how to configure Communication Manager to minimize toll fraud, see *Avaya Toll Fraud Security Guide*, available at http://support.avaya.com.

Procedure

Type **`change system-parameters features`** to enable trunk-to-trunk transfers.

This feature is needed when an incoming call to a SIP station is transferred to a station on Communication Manager Evolution Server. For simplicity, set the Trunk-to-Trunk Transfer on Page 1 to `all` to enable all trunk-to-trunk transfers on a system wide basis.

Configuring IP codec set

Procedure

1. Type the command **change ip-codec-set *n***, where *n* is the number used to identify the codec set.
2. In the **Audio Codec** field, enter `G.711MU` and `G.729` as supported types.
3. In the **Silence Suppression** field, retain the default value `n`.
4. In the **Frames Per Pkt** field, verify that the value is set as `2`.
5. In the **Packet Size (ms)** field, verify that the value is set as `20`.
6. In the **Media Encryption** field, enter the value based on the system requirement. In this sample configuration, it is set as `none`.
7. Save the changes.

Configuring IP network region

Procedure

1. Type `change ip-network-region x`, where *x* is an IP network region number.
2. In the **Authoritative Domain** field, enter the appropriate SIP domain name for example, `MyCompany.com`.
3. In the **Name** field, enter a descriptive name.
4. In the **Codec Set** field, enter the number of the IP codec set that you configured.
5. In the **Intra-region IP-IP Direct Audio** field, type `yes`.
6. In the **Inter-region IP-IP Direct Audio** field, type `yes`.
7. Save the changes.

Adding node names

About this task

Add the node-names and IP addresses for the procr interface on Communication Manager and the virtual Security Module interface of the Session Manager.

Procedure

1. Type **`change node-names ip`**.
2. In the **Name** field, enter the name associated with the IP address of the first Session Manager Security Module as `ASM1-R6` and the name associated with the IP address of the second Session Manager Security Module as `ASM2-R6`.
3. In the **IP Address** field, enter the IP address of the first Session Manager Security Module as `10.80.120.28` and the IP address of the second Session Manager Security Module as `10.80.120.30`.
4. Save the changes.

Adding signaling group

Procedure

1. Type **`add signaling-group n`**, where *n* is an available signaling group number to create SIP signaling group. In the sample configuration, trunk groups 10 and 11 and signaling groups 10 and 11 are used for connecting to both Session Managers.
2. In the **Group Type** field, type `sip`.
3. Set **IMS Enabled** to `y`.

Note:

Set IMS Enabled to `y` for a Feature Server. It should be left as `n` for an Evolution Server.

4. Set the **Transport Method** to `tcp`.

Note:

TCP is used in this sample configuration. However, TLS is usually used in production environments.

5. Set **Peer Detection Enabled** to `y`.
6. Use default value for **Peer Server**.

Note:

Replace the default value with SM after you establish a SIP trunk to Session Manager.

7. Set **Near-end Node Name** to `procr`
8. Set **Far-end Node Name** to the name of the Session Manager Security Module.
9. Verify that **Near-end Listen Port** is set as `5060`.
10. Verify that **Far-end Listen Port** is set as `5060`.
11. Set the **Far-end Network Region** value as the value that you set in the entered in the **change ip-network-region** form.
12. Set **Far-end Domain** to the same domain name that you entered as the **Authoritative Domain** on the **change ip-network-region** form.
13. Verify that **DTMF over IP** is set to `rtp-payload`.
14. Save the changes.

Repeat these steps to define a second signaling group to connect to the second Session Manager.

Adding a SIP trunk group

About this task

Add a SIP trunk group to the SIP signaling group for call routing from the Communication Manager server to Session Manager.

Procedure

1. Type **add trunk-group n** where *n* is an available trunk group number.
2. In the **Group Type** field, type `sip`.
3. In the **Group Name** field, type the name of the Session Manager Security Module.
4. In the **TAC** field, type an available trunk access code.

5. Set **Direction** to `two-way`.
6. Set **Service Type** to `tie`.
7. In the **Signaling Group**, type the SIP signaling group number that you added earlier.
8. In the **Number of Members** field, type the number of members in the SIP trunk.

   After the add trunk-group command is completed, trunk members are automatically generated based on the value in the **Number of Members** field.

Figure 13: Add trunk — group n, Page 1

```
add trunk-group 10                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 10                      Group Type: sip           CDR Reports: y
  Group Name: SIP-IMS to ASM 1              COR: 1        TN: 1        TAC: #10
Direction: two-way         Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n

                                                     Signaling Group: 10
                                                   Number of Members: 20
```

9. In page 2, set the **Preferred Minimum Session Refresh Interval** field to `1200`.

   Note:

   To avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of `1200`.

Figure 14: Add trunk — group n, Page 2

```
add trunk-group 10                                          Page   2 of  21
                                Group Type: sip
TRUNK PARAMETERS

     Unicode Name: auto
                                          Redirect On OPTIM Failure: 5000

           SCCAN? n                                  Digital Loss Group: 18
                    Preferred Minimum Session Refresh Interval(sec): 1200
```

10. In page 3, set the indicated fields as shown in the figure. Use the default values for the remaining fields.
    - For **Numbering Format**, type `private`.
    - For **Show ANSWERED BY on Display**, type `y`.

Figure 15: Add trunk — group n, Page 3

```
add trunk-group 10                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y

                     Numbering Format: private
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

 Show ANSWERED BY on Display? y
```

11. In page 4, set the indicated fields as shown in the figure. Use the default values for the remaining fields.
    - For **Support Request History**, type `y`.
    - For **Telephone Event Payload Type**, type `120`.

Figure 16: Add trunk — group n, Page 4

```
add trunk-group 10                                          Page   4 of  21
                                   PROTOCOL VARIATIONS

                      Mark Users as Phone? y
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                  Network Call Redirection? n
                     Send Diversion Header? n
                   Support Request History? y
              Telephone Event Payload Type: 120
```

Configuring route pattern

Procedure

1. In Communication Manager, enter **change route-pattern *x*** where *x* is an available route pattern.
2. In the **Pattern Name** field, enter a name for identification.
3. In the **Grp No** field, enter the newly added trunk group.
4. In the **FRL** field, enter the number `0`.
5. In the **Numbering Format** field, enter `lev0-pvt`.
6. In the **LAR** field, enter `next` for first row. Use default value for second row.
7. Save the changes.

   In this sample configuration, route pattern 10 is created.

Administering numbering plan

About this task

Extension numbers used for SIP users registered to Session Manager must be added to either the private or public numbering table on Communication Manager Feature Server. In this sample configuration, private numbering is used and all extension numbers are unique within the private network.

Procedure

1. Enter **`change private-numbering n`**, where *n* is the length of the extension.
2. In the **Ext Len** field, enter the length of extension numbers. In this sample configuration, the length of the extension is `7`.
3. In the **Ext Code** field, enter the leading digit from extension number. In this sample configuration, it is set as `666`.
4. In the **Trk Grp(s)** field, enter the trunk groups entered in the earlier step.

   If trunk group numbers are contiguous, use a single row. Else, it might be necessary to add two rows.
5. For **Private Prefix** field, leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.
6. In the **Total Length** field, enter the `7` because a private prefix is not defined.

Administering AAR digit analysis

About this task

This section provides configuration details of the AAR pattern used in this sample configuration for routing calls between SIP users supported by Communication Manager Feature Server. In this sample configuration, extension numbers starting with digits 666-3xxx are assigned to SIP stations supported by Communication Manager Feature Server.

Procedure

1. Enter **`change aar analysis n`** command, where *n* is the first digit of the extension numbers used in the system.
2. In **Dialed String** field, enter leading digit of extension numbers.
3. In **Min** field, enter the minimum number of digits that must be dialed.
4. In **Max** field, enter the maximum number of digits that may be dialed.
5. In **Route Pattern** field, enter the Route Pattern as defined earlier.
6. In **Call Type** field, enter `unkn`.

Configuring stations

About this task

For each SIP user defined in Session Manager, add a corresponding station on the Feature Server. The extension number defined for the SIP station is the number that the SIP user enters to register to Session Manager.

Note:

Instead of manually defining each station using the Communication Manager SAT interface, an alternative option is to automatically generate the SIP station when adding a new SIP user using System Manager.

Procedure

1. Enter **add station n** command, where *n* is a valid extension number defined in the system.
2. In **Type** field, enter `96xxSIP` corresponding to the specific device.
3. In **Port** field, do not set any values. After the command is submitted, a virtual port is assigned. For example, S0000.
4. In **Name** field, enter the display name for user.
5. In **Security Code** field, enter the number the user logs into station with [optional].

   Note:

   If number is entered, it should match the **Shared Communication Profile Password** field defined when adding this user in System Manager.

Figure 17: Add station n, Page 1

```
add station 6663000                                    Page   1 of  6

                              STATION

Extension: 666-3000                  Lock Messages? n             BCC: 0
     Type: 9630SIP                   Security Code: 123456         TN: 1
     Port:                         Coverage Path 1: 1              COR: 1
     Name: SIP Station User        Coverage Path 2:                COS: 1
                                   Hunt-to Station:

STATION OPTIONS
                                      Time of Day Lock Table:
             Loss Group: 19
                                            Message Lamp Ext: 666-3000
        Display Language: english             Button Modules: 0
          Survivable COR: internal
   Survivable Trunk Dest? y                     IP SoftPhone? n

                                                IP Video? n
```

6. In Page 6, you can set the **SIP Trunk** field, as `aar`, `ars`, or `route pattern` to use Route Pattern defined in the earlier section so that calls are routed over the secondary route in case the primary Session Manager is not available.

Figure 18: Add station n, Page 6

```
add station 6663000                                          Page   6 of  6

                                STATION
SIP FEATURE OPTIONS
          Type of 3PCC Enabled: None
                      SIP Trunk: aar
```

Verify off-PBX-telephone station-mapping

Procedure

1. Use the **change off-pbx-telephone station-mapping xxx** command, where *xxx* is an extension assigned to a 9600-Series SIP telephone to verify that an Off-PBX station mapping is automatically created for the SIP station as a result of the **add station** command.
2. In Page 1, verify the following fields are correctly populated.
   - Verify that the **Application**, is assigned as `OPS`.
   - Verify that the **Trunk Selection**, is assigned as `aar`.

Figure 19: Change off — pbx — telephone station — mapping xxx, Page 1

```
change off-pbx-telephone station-mapping 6663000              Page   1 of  3

                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station        Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                  Prefix                    Selection   Set     Mode
 6663000          OPS           -      6663000          aar          1
                                -
                                -
```

3. In Page 2, verify the following fields were correctly populated.
   - Verify that the **Mapping Mode**, is assigned as `both`.
   - Verify that the **Calls Allowed**, is assigned as `all`.

Figure 20: Change off — pbx — telephone station — mapping xxx, Page 2

```
change off-pbx-telephone station-mapping 6663000              Page   2 of  3

                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION


 Station        Appl    Call        Mapping    Calls      Bridged     Location
 Extension      Name    Limit       Mode       Allowed    Calls
 6663000        OPS      3          both       all         none
                                 -
```

Save translations

After configuration of Communication Manager Feature Server is complete. Use the save translation command to save these changes.

Note:

After making a change on Communication Manager Feature Server which alters the dial plan or numbering plan, synchronization between Communication Manager Feature Server and System Manager needs to be completed and SIP telephones must be re-registered.

Configuring Avaya Aura® Session Manager

Synchronizing Communication Manager station data to the System Manager

Use the System Manager interface to synchronize Communication Manager station data to the System Manager database. After a Communication Manager has been added as an entity, the Communication Manager is automatically scheduled for an initial and subsequent incremental daily data synchronization.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Click **New**.
3. In the **Type** field, select **Communication Manager** from the drop-down menu and wait for the screen to refresh.
4. On the Add Communication Manager page, under the **General Attributes** section, enter the required information for the Name and IP address.
5. Select an **Authentication Type**.
6. Enter and confirm the SAT password.
7. Click the **SNMP Attributes** tab.
8. Set the **Version** as **None**.
9. Click **Commit**.
10. To view the synchronization status for each Communication Manager, go to the home page and select **Services** > **Inventory** > **Synchronization** > **Communication System**.

Each Communication Manager is displayed in the table. The **Last Sync Time** column indicates when the last data sync completed or the phase of synchronization for the current sync job in progress.

Adding SIP entity for Communication Manager

About this task

A SIP entity must be added for the Communication Manager Feature Server connected to the Session Managers using SIP trunks.

Procedure

1. To create a SIP entity select **Routing** > **SIP Entities**.

   Depending on the IP Address Family that you select, the system displays:

   - For IPv4 IP address family: **FQDN or IPv4 Address** field.
   - For IPv6 IP address family: **FQDN or IPv6 Address** field.
   - For Both address family: **FQDN or IPv4 Address** and **FQDN or IPv6 Address** fields.

2. In the **FQDN or IPv4 Address** or **FQDN or IPv6 Address** fields, enter IP address used for the *PROCR IP* interface.
3. In the **Type** field, select **CM** for Communication Manager.
4. Click **Commit** to save the SIP entity.

Adding a SIP entity for Session Manager

About this task

A SIP entity must be added for each Session Manager and the Communication Manager connected to Session Manager using SIP trunks.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **FQDN or IP Address** field, enter IP address of IP signaling interface for virtual SM100 interface on Session Manager.
4. In the **Type** field, select **Session Manager** from the drop-down menu.
5. Select the **Securable** check box.
6. In the **SIP Link Monitoring** box, select **Use Session Manager Configuration**.
7. Create an Entity Link between Session Manager and Communication Manager.

8. Click **Commit**.

Creating Entity Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Entity Links**.
2. Click **New**.
3. Type the name in the **Name** field.
4. Enter the SIP entity 1 by selecting the required **Session Manager** SIP entity from the drop-down list and provide the required port.

   SIP entity 1 must always be a Session Manager instance.

   The default port for TCP and UDP is 5060. The default port for TLS is 5061.
5. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list and provide the required port.

   The port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
6. In the **IP Address Family** field, select the IP address family.
7. From the **Connection Policy** drop-down menu, select **Trusted**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
8.
9. Click **Commit**.

Adding a Session Manager instance

You can add a Session Manager instance using either the:

- Session Manager Administration pages.
- Manage Elements pages.

Note:

If a Version 7 license is installed and the Session Manager server instance count has been reached, the following error message appears after clicking the **New** button: `Cannot add Session Manager instance, maximum instance count reached for license.` You cannot administer a new Session Manager beyond the license limit until you install a Version 7 license with a higher limit.

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Use the Session Manager Administration page:
     a. Under **Elements**, click **Session Manager** > **Session Manager Administration**.
     b. Click the **Session Manager Instances** tab.
     c. Click **New**.
   - Use the Manage Elements page:
     a. Under **Services**, click **Inventory** > **Manage Elements**.
     b. Click **New**.
     c. From the **Type** field, select **Session Manager**.
     d. When the screen refreshes, from **Select type of Session Manager to add:**, select **Core Session Manager**.
     e. Click **Continue**.
2. On the Add Session Manager page, in the General section, perform the following:
   a. In the **SIP Entity Name** field, type the name of the Session Manager instance.
   b. In the **Description** field, type a description for this entity.

      This field is optional.
   c. In the **Management Access Point Host Name/IP** field, type the IP address of the management interface of the Session Manager server.

      The **Management Access Point Host Name/IP** field accepts only IPv4 addresses even when you create Session Manager instances for entities supporting IPv6 or Both address families.
   d. From the **Direct Routing to Endpoints** drop-down list, select Enable for direct routing to endpoints.
   e. From the **Data Center** drop-down list, select a data center.
   f. From the **Avaya Aura Device Services Server Pairing** drop-down list, select an AADS server.

      AADS is available with Avaya Equinox™ 3.0.

      When an AADS server is already paired with a Session Manager instance, the system does not display that AADS Server.
   g. **Maintenance Mode** is enabled by default. Deselect **Maintenance Mode** if you are not:
      - Staging a non-operational Session Manager or Branch Session Manager.
      - Pre-administering Session Manager or Branch Session Manager on System Manager prior to host installation.

3. Specify the appropriate information in the remaining required fields.

   For information about the fields, see Add Session Manager Administration page field descriptions.

4. Click **Commit**.

Adding domains

About this task

The phone number of Fred is captured as a SIP handle 6663008@avaya.com where part of the SIP handle is a domain (avaya.com).

Procedure

1. To add and administer a domain, click **Elements** > **Routing** > **Domains** > **New**.
2. Enter the name of the domain and select **Type** as **sip**. Click **Commit**.

Adding application sequences

About this task

You can set an origination application Sequence and a termination application sequence as preferred way of handling calls for Fred. When Fred receives a call from the user, Session Manager routes the call through the terminating sequence. Whereas when Fred calls a user, Session Manager routes the call through the originating sequence. For creating an application and application sequence refer to next topic. For details on configuring an application sequence, refer to the Call Handling Case Study.

Related links

Creating an application on page 58

Creating an Application Sequence on page 59

Creating an application

Before you begin

You must first administer a non-Session Manager SIP entity before you can create a new application entry.

Procedure

1. Verify the non-Session Manager SIP entity exists.
2. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Applications**.
3. Click **New**.
4. Enter the appropriate information for the new application.

5. Click **Commit**.

Related links

Adding application sequences on page 58

Creating an Application Sequence

An Application Sequence can contain a maximum of 10 applications.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Application Sequences**.
2. Click **New**.
3. Enter the appropriate information.
4. Click **Commit**.

Related links

Adding application sequences on page 58

Adding a home location

About this task

When you dial the numbers that are not associated with an administered user, the dial-plan rules are applied to complete the call based on this home location. If the physical location of the SIP device cannot be determined by matching the IP address to an administered location in the System Manager.

Note:

To apply dial plan rules select **Routing** > **Dial Patterns**.

Procedure

1. To add a home location element in the communication profile of Fred, click **Routing** > **Locations** > **New**.
2. Enter the name of the location and other information. Click **Commit**.

   You can specify a home location to support mobility for the currently displayed user. It is mandatory that you make this selection.

Adding the survivability server

Before you begin

To set a Branch Session Manager as a survivability server, you need to add a SIP entity of type Session Manager.

About this task

For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. This is optional and is required only for survivability.

Procedure

To administer a Branch Session Manager as a survivability server, go to **Elements** > **Session Manager** > **Session Manager Administration** and click **New** on the Branch Session Manager Instances section of Session Manager Administration screen.

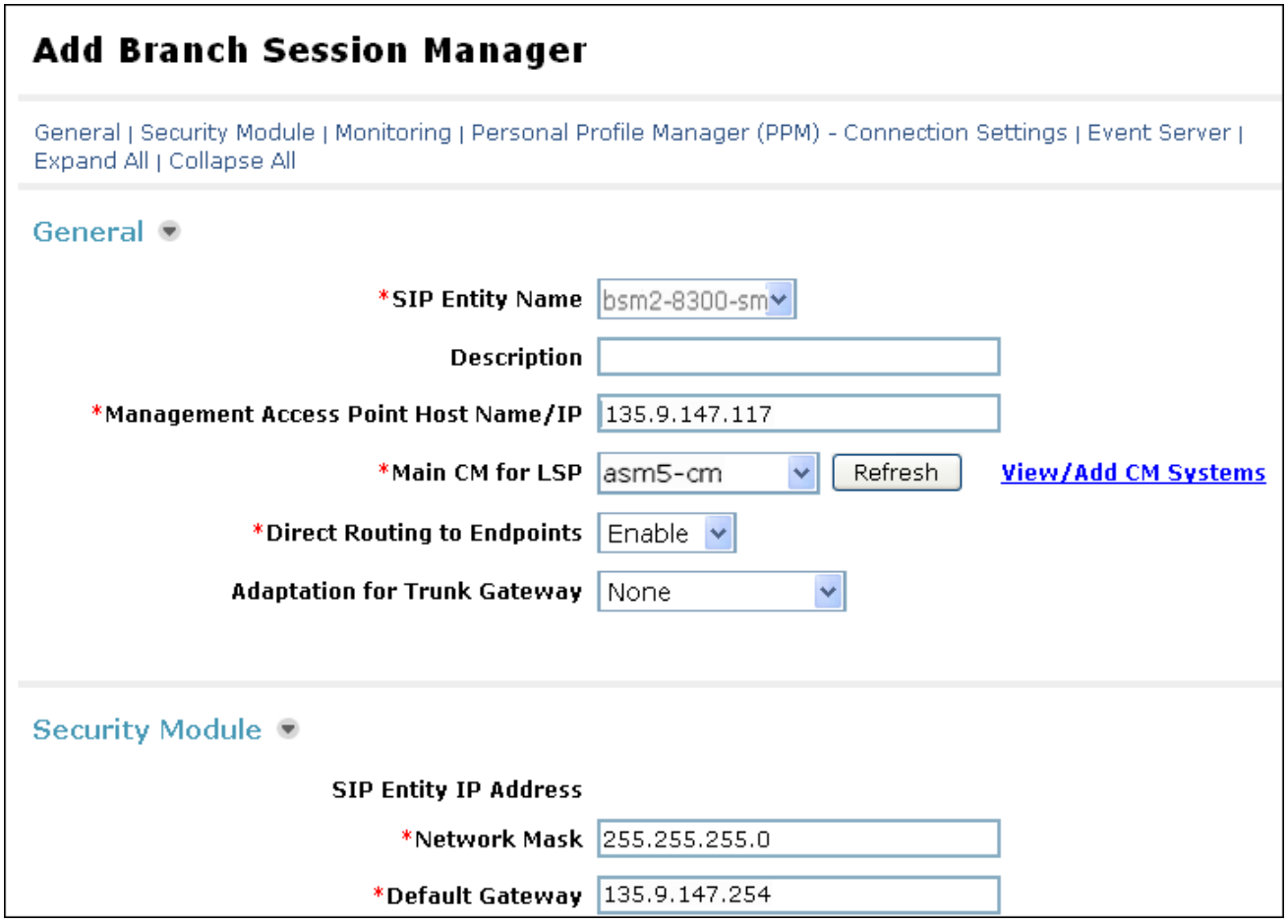


Figure 21: Add Branch Session Manager

Adding a SIP endpoint user

For basic setup of user profile for Fred, you need to complete the following sections in the User Management application.

1. Identity

2. Communication Profile
3. Membership
4. Contacts

Procedure

1. Navigate to **Users** > **User Management** > **Manage Users**, and click **New**.
2. In the Identity section, enter the last name and the first name of Fred.
3. Enter a description in the **Description** field. This field is optional.
4. Enter the **Login Name** for Fred. This is the unique system login name given to Fred and takes the form of *username@domain* (enterprise canonical number).
5. Select the **Authentication Type** as *Basic*.
6. Enter the System Manager Login Password in **Password** and confirm it. The password must start with an alpha (lower or upper case) character.

   Note:

   This step is for creating a System Manager login and not required for creating a SIP User.
7. Enter the **Localized Display Name** of the Fred. This is the name that is displayed as the calling party.
8. Enter the full text name of the user for **Endpoint Display Name**.
9. In the Address section, add mailing address details of Fred in the Address section.

   Fred may have one or more communication profiles for registering one or more SIP user handles (phone extensions) to the Session Manager. This enables Fred to define (optional) an origination and termination application sequence as his preferred call routing method.

   To register a SIP phone with Session Manager, at least one communication profile must be administered containing the Session Manager related details. You must have defined at least one SIP communication address. The handles may also be associated with a Communication Manager station and/or messaging subscriber.

   A communication address can be used to communicate with the contact. This can be a phone number, E-mail address, SIP or IM of the contact. One or more communication addresses for Fred is defined in relation to handle and domain in the format userinfo@domainpart when routing a communication interaction to Fred.
10. In Communication Address section, set **Type** as **Avaya SIP**.
11. Enter the phone extension in the **Fully Qualified Address** field and finally select the correct domain from the drop-down menu.

    Handle is a unique communication address for Fred which is set as 6663008. The name of the domain with which the handle is registered is avaya.com.

    In the Session Manager Profile section, you can associate Fred with a primary and secondary Session Manager, specify origination and termination application sequences, a

Survivability Server for example, a Branch Session Manager, and also specify a **Home Location** for this user. The phones of Fred register with the selected Session Manager. Calls from or to the phone of Fred are routed through the selected origination or termination applications sequences respectively.

12. Home Location is a mandatory input field to support mobile users. To administer locations select **Routing** > **Locations**.

    In the Station Profile section, specify the Communication Manager station association for Fred as per the following cases:

    - associate Fred with an existing station.
    - add a new station on the Communication Manager for Fred.

13. In case of existing station, select the previously administered Communication Manager entity in the **System** drop-down menu.
14. Enable **Use Existing Endpoints**.
15. Enter (or select when prompted) the extension for the station.
16. Optionally, the template for the station, you can change the security code and/or port values for this station.
17. In case of new station, select the previously administered Communication Manager entity in the **System** drop-down menu.
18. Enter or select when the system prompts for the extension of the station.
19. Select a phone template for the phone.
20. Enter or select when the system prompts for a value in the **Port**.
21. Optionally, enter a value in the **Security Code**.
22. In the Messaging Profile section, specify the association of a subscriber mailbox for Fred. Add messaging system on which you need to add Fred.
23. Add a system defined and user defined template that you want to associate with Fred. Templates are defined in the Communication System Management module.
24. Add a mailbox number for Fred.

    Fred can optionally be given a default Contact List by expanding the Contact List section at the bottom of the page.

25. Click **Add** to select already administered users as contacts.

    Note:

    These contacts are transferred to Fred’s phone if the phone supports contacts feature.

Administering 96xx SIP deskphones

About this task

A deskphone can use settings from a file server if you set up the environment for the deskphone.

Procedure

1. To go to the **Configuration** menu, perform one of the following steps:
   - On the physical deskphone, press the **Mute** button, and type `CRAFT#` by using the keypad.
   - On the soft telephone, type `admin options`, and press `Enter`.
2. In the **SIP Global Settings** section, perform the following steps:
   a. In the **SIP Domain** field, type the domain name of the Session Manager server.
   b. In the **Avaya Environment** field, select **auto**.
   c. In the **Reg. Policy** field, select **simultaneous**.
   d. Leave the **Avaya Config Server:** field blank.
3. In the **SIP Proxy Settings** section, perform the following steps:
   a. In the **SIP Proxy Server** field, type the IP address of the primary Session Manager server.
   b. If applicable, type the IP address of the secondary Session Manager server.
   c. In the **Transport** field, select **TCP** or **TLS**.
   d. In the **SIP Port** field, type the port number defined in the Session Manager SIP entity.

      For example, type `5060` for TCP.
4. In the **SSON** field, type the appropriate SSON number for the deskphone to gain access to the file server.

Note:

For more information on administering 96xx SIP deskphones, see *Administering Avaya 9601/9608/ 9608G/9611G/9621G/9641G IP Deskphones SIP*.

Chapter 4: Call Handling case study

Overview

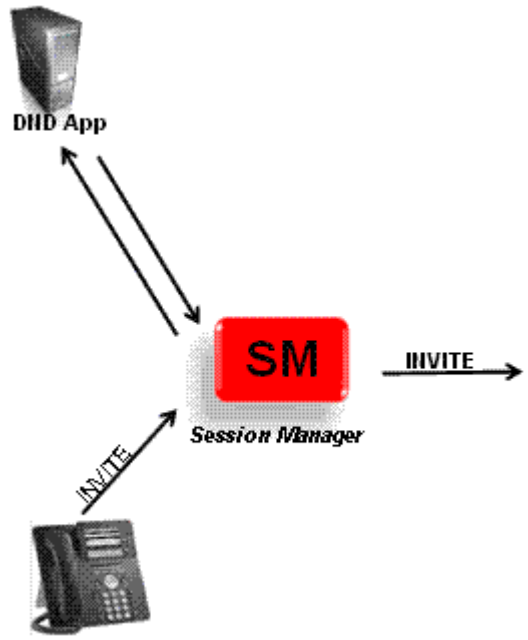
This case study shows call handling as per the preferred set of applications using application sequence functionality or as per some enterprise dial pattern using implicit user functionality. Some examples of such applications are as follows:

- Do-not call and selective call lists
- Caller-ID manipulation — Outsourcers or partners calling “on behalf of” their customer
- Conference bridge selector — Use built in 6-party conferencing first, then automatically switch to an internal or a hosted conference bridge if greater capacity needed
- Call Screener — Could be activated if user is in a meeting or depending on their presence status
- Selective call recording
- Call transcription or archiving

Scenario definition

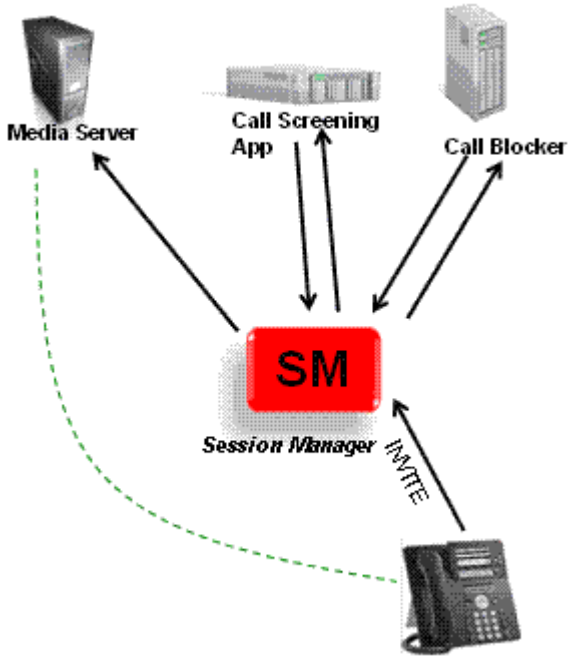
This scenario shows how a call from Barney for Fred is handled using application sequencing defined in the communication profile of Fred at termination side.

Origination side sequencing



1. Barney makes an outbound call.
2. Session Manager signals the originating applications associated with Barney.
3. The Do Not Call (DND) application verifies that Fred is not listed in “Do Not Call” registry.
4. After verification, it forwards the call to Session Manager.
5. Session Manager sequences to the next application in the sequence.

Termination side sequencing



1. Session Manager gets INVITE from telephone.
2. Session Manager signals the terminating applications for Fred.
3. The Call Blocker application does not block call.
4. Session Manager signals the next application.
5. The call screening application checks the status of Fred.
6. If Fred is Busy, call screening application forwards request to Media Server.
7. The Media Server plays custom message accordingly.

Using application sequence

About this task

Application sequence functionality enables you to define and manage a set of applications for call sequencing as per the communication profile of the user. Some of the steps are outlined as follows:

Procedure

1. You should setup application sequences before users are assigned.
2. All applications must include Communication Manager.
3. To administer Communication Manager SIP entity beforehand select **Routing** > **SIP Entities**.

4. Associate the user with a particular Session Manager instance and an application sequence as the originating and terminating sets as shown in the *New User Setup Case Study*.

Adding Communication Manager Feature Server

Procedure

1. Add the Communication Manager Feature Server as a SIP Entity in the routing application. For more information about adding Communication Manager as a SIP entity, see *Adding SIP entity for the Communication Manager*.
2. To administer applications, select **Elements** > **Session Manager** > **Application Configuration** > **Applications**. The main page displays a list of currently administered applications.
3. Click **New** to add a new application.
4. Enter a name for the application as ACM and select the associated Communication Manager feature server for SIP Entity.

   Note:

   You need to add an entity of type CM previously using **Elements** > **Inventory** > **Manage Elements** for the data synchronization to System Manager.
5. **(Optional)** Enter an application handle and URI parameter, if required.
6. Set the media attributes for the application.
7. Click **Commit**.

   Note:

   - Add other applications that need to be added in the application sequence for Fred.
   - By itself, an application cannot be associated with a user. Only application sequences consisting of one or more applications assigned in an order can be associated with a user for call routing.

Creating an application sequence from existing applications

Procedure

1. The Application Sequences web page is located below the Applications page **Elements** > **Session Manager** > **Application Configuration** > **Application Sequences**. The main page displays all currently administered application sequences. Click **New** to add a new sequence.

2. Name the application sequence and click the + icon next to an available application such as the Communication Manager Feature Server — ACM. Now, the selected application gets added in the *Applications in this Sequence* table. This suggests that ACM is now a part of the application sequence.

Administering implicit users

About this task

The implicit user functionality allows routing calls to and/or from a specified dial pattern through application sequences. This is similar to specifying an origination and termination application sequence for a user, but it allows application sequencing to be applied to any dial pattern as opposed to a phone number for a registered phone of the user. However at first, a match on an explicit users dial pattern is attempted. If no match is found, then the system attempts to match an implicit user. Some of the important points about implicit users are:

- Implicit users are not registered users.
- Users can be on third party PBX.
- Also includes DCP, Analog or H.323 CM users.
- Identified by phone numbers or extensions.
- Can have origination and termination application sequences.

Procedure

1. To open the Implicit Users screen, on the System Manager Web Console, click **Elements** > **Session Manager** > **Application Configuration** > **Implicit Users**.
2. Click **New**. The Implicit User Rule Editor screen appears. The pattern, min and max input fields are similar to those on the Dial Pattern web page and are used to specify a dial pattern. The *SIP Domain* field allows restricting the origination and termination application sequencing to calls from or to a matching phone number on the specified domain only.
3. In the Implicit User Rule Editor screen, enter the appropriate information and click **Commit**.

Chapter 5: Emergency Calling case study

Overview

E911 service such as the ELIN server enables emergency location looks up for emergency calls and helps in identifying the physical location of the emergency caller who is a registered user on Session Manager in the event of an emergency call. The ELIN (Emergency Location Identification Number) is a 10 digit number which provides specific details about the location of the caller. This enables emergency services to:

- call back the emergency caller in case of need for additional information after ending the emergency call
- re-establish the emergency call if it gets disconnected for some reason

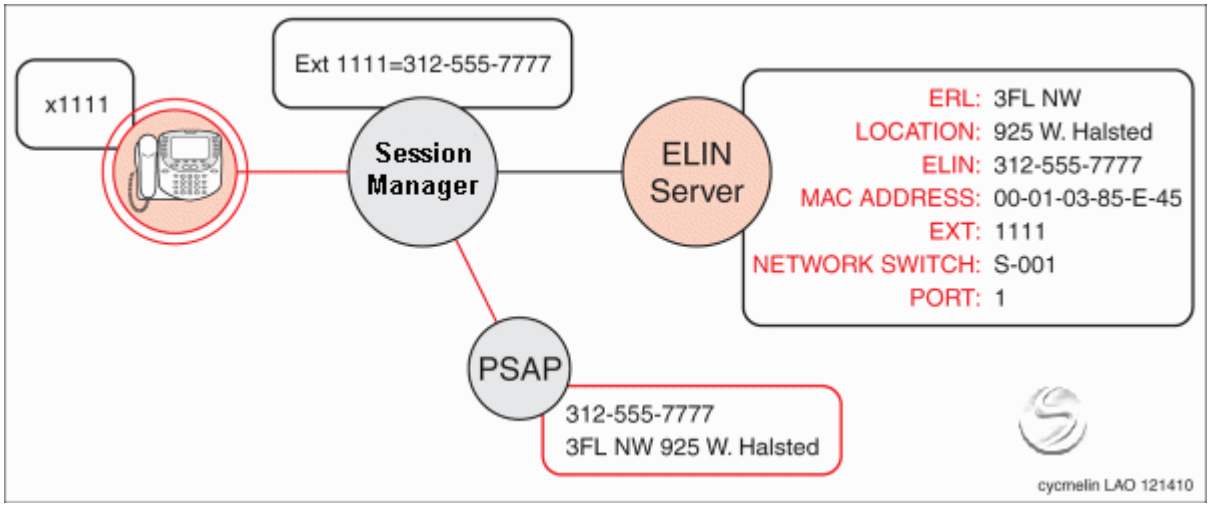
This case study provides the basic concepts, scenario definition and some administration related details regarding emergency calling.

Case definition

The following is a case study of an emergency call of 911 from Ellen using her extension 1111 and shows how emergency services such as Public Safety Answering Point (PSAP) or the Communication Manager (CM) is able to view the location details of Ellen:

1. The Extension 1111 registers to the Session Manager (SM).
2. The Session Manager sends a `PUBLISH` message to the ELIN server.
3. The ELIN Server looks up the information provided and determines the ELIN number (312-555-7777).
4. The ELIN server sends ELIN to Session Manager in a PUBLISH message.
5. Ellen at extension 1111 places an emergency call which is routed to Session Manager.
6. The Session Manager looks up the ELIN record, includes it in the INVITE (AP-Loc header) and forwards it on to the PSAP (CM).
7. The PSAP does a look up based on the ELIN number and determines the physical address of the caller.

Figure 22: Emergency calling



In case of an emergency call when the ELIN is stored for the user:

1. The call is identified as an emergency call based on the provisioned Dial Pattern match such as 911.
2. Based on a lookup on the user, Session Manager provides the required ELIN and includes it in the INVITE under the AP-Loc header.
3. The INVITE is then either passed directly to the Public Safety Answering Point (PSAP) or to Communication Manager, then to the PSAP.

In case of an emergency call either when the ELIN is not stored for the user or when the ELIN server is unavailable:

1. The call is identified as an emergency call based on the provisioned Dial Pattern match such as 911.
2. Based on a lookup on the user, if the Session Manager cannot find associated ELIN, the INVITE is sent without an AP-Loc header either to the Communication Manager or directly to the Public Safety Answering Point (PSAP), depending on the configuration.
3. In cases when the call is routed to the Communication Manager without an ELIN, Communication Manager uses the ip-network-region mapping to determine an ELIN based on the IP address of the user. If it can map the calling user to an ELIN, Communication Manager uses digit conversion to assign the user to some station. After it finds the station, it reapplies the digit conversion to set the ELIN back to 10 digits format before forwarding it to the PSAP.
4. In case when the Communication Manager finds no match for the IP address to an ELIN, it includes the extension number of the calling station as the calling party for the PSAP.

Registration based events

Initially Session Manager synchronizes with the ELIN Server through the bulk PUBLISH messaging. Later Session Manager starts sending individual PUBLISH message for each registration events, such as when a user registers, unregisters, or the registration expires.

When the SIP phone registers with Session Manager the following registration based events occurs:

1. Session Manager sends a PUBLISH message to the ELIN servers. The PUBLISH message contains the registration information including the terminal ID and the IP address of the SIP phone. A sample PUBLISH message format for reference is:

```
PUBLISH sip:rs1.redskye911.com
Via: SIP/2.0/TLS sm1.avaya.com;branch=z9hG4bKl21
Max-Forwards: 70
To: <sip:rs1.redskye911.com>
From: <sip:sm1.avaya.com>;tag=3212
Call-ID: 8dj2983s
CSeq: 387 PUBLISH
Contact: <sip:sm1.avaya.com>
Event: reg
Content-Type: application/reginfo+xml
Content-Length: ...

<registration aor="">
    <contact id="">
        <uri>sip:5551414@lab.avaya.com</uri>
   </contact>
</registration>
</sip:sm1.avaya.com></sip:sm1.avaya.com></sip:rs1.redskye911.com>
```

2. The ELIN Server uses this information to discover the ELIN as administered per detailed location.

   Note:

   ELIN provisioning is done on the E911 server and not in the Session Manager.

3. The ELIN server sends PUBLISH messages only to those Session Managers to which a station is registered. If an endpoint is dual-registered to a primary and a secondary Session Manager then the ELIN server sends ELINs to both Session Managers. A sample PUBLISH message format for reference is:

```
PUBLISH sip:sm1.avaya.com
Via: SIP/2.0/TLS rs1.redskye911.com;branch=z9hG4bKu8j21
Max-Forwards: 70
To: <sip:sm1.avaya.com>
From: <sip:rs1.redskye911.com>;tag=182341
Call-ID: 67fk2dw
CSeq: 53 PUBLISH
Contact: <sip:rs1.redskye911.com>
Event: reg
Content-Type: application/reginfo+xml
Content-Length: ...

<registration aor=”17325551414” id=”edfisw” state=”init”>
    <contact id=”hr” state=”active” event=”registered”
        Duration registered=”3600”>
        <uri>sip:5551414@lab.avaya.com</uri>
        <elin>sip:5551112222</elin>
    </contact>
```

```
</registration>
...
<registration aor="17325551415" id="edfisw" state="init">
    <contact id="hr" state="active" event="registered"
        Duration registered="3600">
        <uri>sip:5551415@lab.avaya.com</uri>
        <elin>sip:5551112222</elin>
    </contact>
</registration>
```

Note:

If an ELIN for an endpoint is changed, the ELIN Server sends a new PUBLISH to Session Manager with the new ELIN. Session Manager replaces the previous ELIN with the new one.

OPTIONS monitoring is automatically activated between Session Manager and the ELIN server in order to determine the operational state of the ELIN server to determine when the ELIN server connection goes down or is restored. Session Manager sends OPTIONS messages at administered intervals to an ELIN server and determines the response to OPTIONS queries.

When the ELIN server resumes service after network outage or malfunctioning of the ELIN server, Session Manager sends a bulk PUBLISH to the ELIN server for all users with missing ELINs.

Note:

Bulk PUBLISH also occurs when the ELIN server is administered for the first time in System Manager or when the entity links are added, and other instances. Session Manager sends a bulk PUBLISH and waits for a bulk PUBLISH from the ELIN server.

OPTIONS monitoring also enables Session Manager to detect the following:

- The ELIN server initialization events.
- When the ELIN server is provisioned for the first time, Session Manager sends a bulk/batch PUBLISH message for all the registered contacts on Session Manager with ELIN information.
- Administration related changes carried out on the ELIN server during a network outage. The ELIN server retains the failed updates to Session Manager and eventually ensure that Session Manager receives these updates when the link is restored.

Emergency call notification by Session Manager

With Multiple Device Access (MDA) feature, users can register for multiple devices. The multiple devices usage results in problem in establishing exact location of an emergency call.

Session Manager supports the tracking of an emergency caller in large campus settings. The advanced communication applications guide the emergency crew to the exact location of the emergency call using LED display units near the main entrance of the site.

The applications use the capabilities of the following Avaya Aura® components:

- Session Manager shares the IP address of the caller's SIP device.
- Communication Manager shares the identity of the emergency caller from the database.

Session Manager adds an Emergency Call (EC) Alert to the existing Adjunct Emergency Location Server (AELS) interface for the SIP users. The AELS establishes the exact location of the emergency caller.

The caller may be a SIP user registered through System Manager or an unregistered/unknown user.

The notification is in form of a PUBLISH message.

A sample PUBLISH message format for reference is:

```
PUBLISH sip:aels.AELSe911.com
Via: SIP/2.0/TLS sm1.avaya.com;branch=z9hG4bKu8j21
Max-Forwards: 70
To: sip:aels.AELSe911.com
From: sip:sm1.avaya.com;tag=1823
Call-ID: 67fk2dw
CSeq: 53 PUBLISH
Contact:  sip:sm1.avaya.com
Event: av-ecalert
      Content-Type: application/reginfo+xml
      Content-Length: ...

       ?xml version="1.0"?
 reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
version="408" state="partial"
 registration aor="sip:6000006@avaya.com" id="a42505" state="active"
   contact id="c42505-534151170--1680203528-1" state="active" event="registered" duration-
registered="2500" q="1.0"
     uri sip:6000006@135.9.211.65:1044;transport=tls;avaya-sc-enabled /uri
     unknown-param name="+sip.instance"  "<urn:uuid:
00000000-0000-1000-8000-001b4f7344b4>"  /unknown-param
    ec-alert
       r-uri sip:911@avaya.com /r-uri
       user type=”sip” administered=”true”/
    /ec-alert
    elin 5757528728 /elin
   /contact
/registration

/reginfo
```

Administering ELIN server

About this task

The basic steps of ELIN server administration using System Manager web console are as follows:

Procedure

1. In Local Host Name Resolution (LHNR) page, administer the FQDN for the ELIN Server to have a primary and a backup IP addresses with different priorities.
2. Add a SIP entity of type ELIN server using the above FQDN.
3. In the Session Manager Administration page under Global Settings section, select the administered ELIN Server for **ELIN SIP Entity** field.
4. Create the entity links from the ELIN server to all Session Manager SIP entities.
5. Import certificates for entity link between Session Manager and the ELIN server if the link is of type TLS.

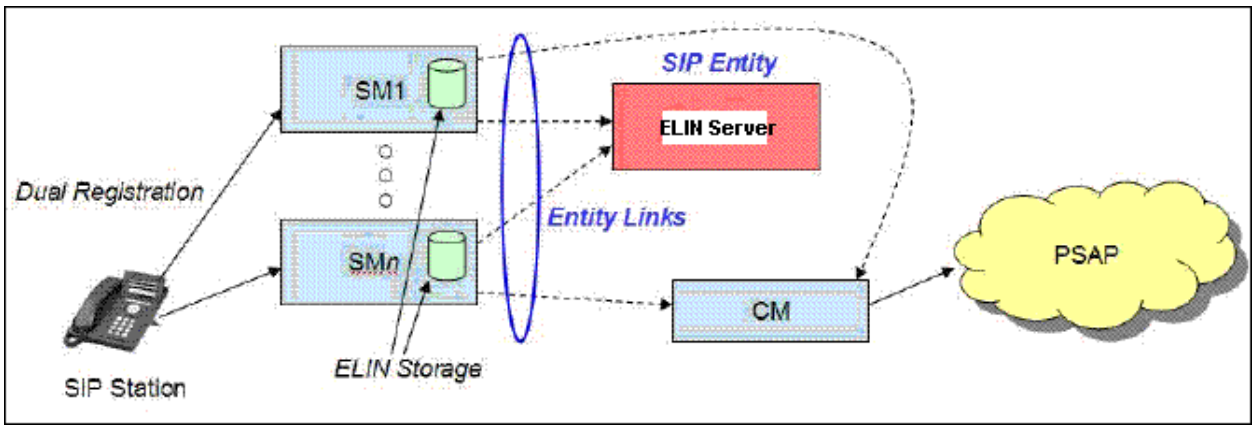
Note:

TLS certificates are required only if the links are of TLS type.

Example

Note:

Session Manager supports ELIN server or server pairs as trusted hosts. ELIN servers can be on different subnets or the same subnet that is, geo-redundancy is supported in ELIN server when the two servers are either on the same subnet or between two different subnets. A primary or secondary pair of ELIN servers can be administered as one SIP Entity with up to two IP addresses. You cannot administer a pair of ELIN servers as two separate SIP entities.



- SM 1…n - Session Manager instances
- ELIN - Emergency Location Identification Number
- CM – Communication Manager as Evolution Server (mandatory)
- PSAP - Public Safety Answering Point

Configuring Communication Manager for ELIN server support

Communication Manager should be able to route “911” calls to the PSAP and the required SIP groups and trunks needs to be configured.

1. For incoming emergency calls to the Communication Manager, if the message signaling has the presence of an ELIN:
   a. ELIN needs to be mapped to an existing extension through an incoming call handling such as inc-call-handling-trmt of the SIP trunk group to get the extension number.
   b. Each shortened ELIN should be a valid station extension in order to enable callback for the phone making the emergency call. Similar is the case if an unregistered phone makes an emergency call.

In case an unregistered phone makes an emergency call the IP network map will be looked up to determine the emergency location extension (ELIN). An unregistered extension will not have an ELIN

c. ELIN must be converted back to 10 digits through public-numbering before being sent out to the public network (PSAP).

2. For incoming emergency calls to the Communication Manager, if the message signaling does not have the presence of an ELIN:

   a. Communication Manager uses the ip-network-region mapping to determine an ELIN based on the IP address of the user. If the Communication Manager maps the calling user to an ELIN, it uses digit conversion to assign it to some station. After the Communication Manager finds the station, it reapplies the digit conversion to set the ELIN back to 10 digits format before forwarding it to the PSAP.

   b. In case when the Communication Manager finds no match for the IP address to an ELIN, it includes the extension number of the calling station as the calling party for the PSAP.

About this task

Following are some of the essential steps to ensure proper coverage in case of emergency calls:

Procedure

1. Administer a paired station extension for every ELIN.
2. Define digit pattern conversion for incoming and outgoing ELIN to station extension mapping.
3. Assign an IP address to Communication Manager, mapping to ELIN in case of emergency calling from unregistered phones.

Creating a Dial Pattern for Emergency Numbers

Before you begin

Ensure that the routing policies have been created so that you can map these routing policies with originating locations.

For more details, see the section *Routing Policies* in the book *Administering Avaya Aura® Session Manager*.

About this task

System Manager supports administering of up to a maximum of 100 emergency numbers for each unique location. Emergency numbers can be administered in dial pattern pages. Before proceeding to create a dial pattern, it is very important to know about dial patterns and E911 services such as the ELIN server.

About Dial Patterns:

A dial pattern specifies which routing policies are used to route a call based on the digits dialed by a user, which match that pattern. Session Manager matches these dialed digits after applying any administered ingress adaptation.

The originating location of the call, the domain in the request-URI, and the Global Settings option of Prefer Longer Matching Dial Patterns in Location ALL to Shorter Matches the location in the Originator's Location in the Session Manager Administration page also determine how the call gets routed.

About E911 Services:

The E911 service enables identification of the physical location of a registered user in the event of an emergency call. The location is determined through the IP address and port level discovery as per E911 administration. Session Manager interacts with E911 service upon user registrations to obtain an Emergency Location Identification Number (ELIN). Each Session Manager synchronizes with the E911 services server, stores ELIN records for its registered users, and sends the ELIN to Communication Manager when an emergency call is made.

Session Manager synchronizes with the E911 services server when any of the following events occurs:

- The server is added to Session Manager in order to initialize or synchronize databases.
- The connection between Session Manager and the server is lost and later restored.
- User registration and un-registration causes Session Manager to synchronize with the E911 service.

E911 services operate in a primary and secondary server mode, in which one server is active and the other is operating in a warm standby mode.

Procedure

1. In the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **Dial Patterns**.
3. Click **New**. The Dial Pattern Details screen is displayed.
4. Under **General** section:
   a. Enter a dial pattern in **Pattern** field. A valid pattern can have between 1 and 36 characters.
   b. Ensure that the minimum and maximum number of digits are matching the valid pattern.
   c. Select the **Emergency Call** check box.

      Note:

      Some of the important constraints on the use of this feature are as follows:

      - You can assign multiple emergency numbers per location.
      - Since it is possible to have more than one emergency number for a location, the Priority 1 emergency number must match the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.

The **Min** and **Max** fields are grayed out with the values in those fields being auto-generated based on the length of the emergency number specified in the **Pattern** field.

d. In **Emergency Priority** field, mention the emergency priority.

   Based on the IP address of the endpoint, up to 100 emergency numbers are downloaded to the endpoint based on location, each assigned with a separate priority.

e. In **Emergency Type** field, enter a type of emergency number for example, medical, fire, and others.

f. In **SIP Domain** field, select a SIP Domain for which you want to restrict the dial pattern.

5. Under **Originating Locations and Routing Policies** section:

   a. Click **Add** to map Originating Locations and Routing Policies for this Dial Pattern.

   b. Select the Originating Locations and Routing Policies, and click **Select**.

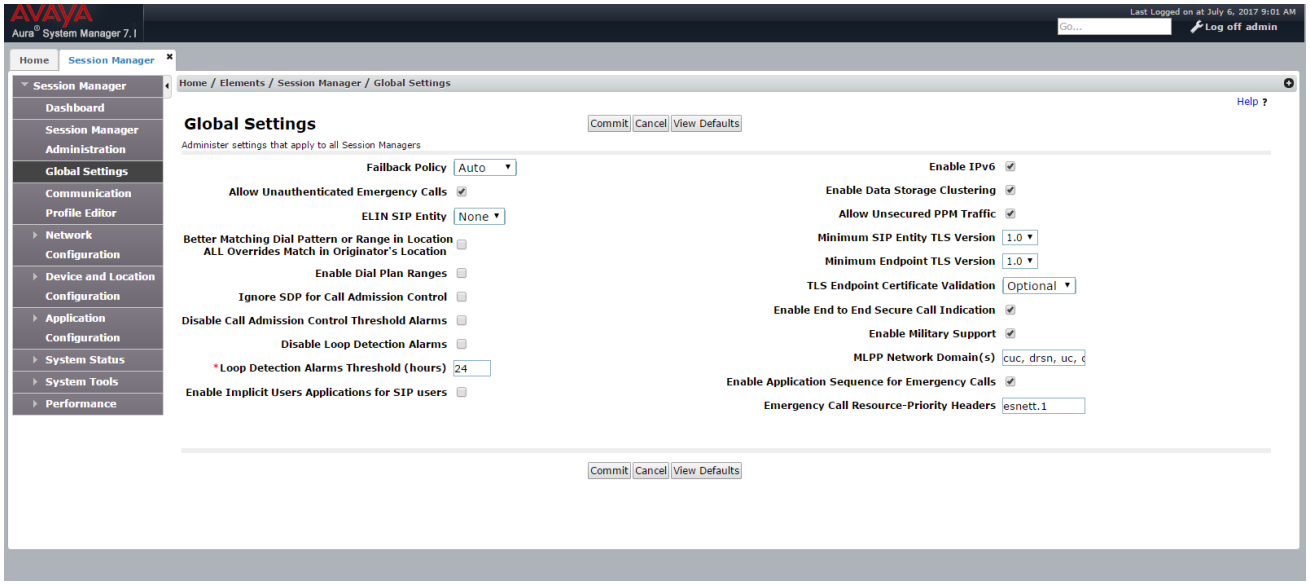
6. In the Dial Pattern Details page, click **Commit**.

Allowing unauthenticated emergency calls

While administrating a Session Manager instance, you can configure a parameter to allow or restrict the unauthenticated emergency calls.

You can allow users using unregistered telephones and unauthenticated users to make emergency calls based on dial pattern by enabling the **Unauthenticated Emergency Calls** in the Session Manager Administration page as shown in the following figure.

Figure 23: Session Manager Administration



Chapter 6: 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		
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 7.1 Release Notes	Contains enhancements, fixes, and workarounds for the Session Manager 7.1 release.	System administrators Services and support personnel
Implementation		
Deploying Avaya Aura® applications from System Manager	Describes how to deploy the Avaya Aura® virtual applications using the System Manager Solution Deployment Manager.	Services and support personnel
Deploying Avaya Aura® Session Manager	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager in a virtualized environment.	Services and support personnel
Routing Web Service API Programming Reference	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel

Table continues…

Title	Description	Audience
Upgrading and Migrating Avaya Aura® applications from System Manager	Describes how to upgrade and migrate the Avaya Aura® virtual applications using System Manager Solution Deployment Manager.	Services and support personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches for Avaya Aura applications.	System administrators
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 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™ R620 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R630 Server	Describes the installation procedures for the Dell™ PowerEdge™ R630 server.	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
Installing the HP ProLiant DL360 G9 Server	Describes the installation procedures for the HP ProLiant DL360 G9 server.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Migrating and Installing Avaya Appliance Virtualization Platform	Describes the migration and installation procedures for Appliance Virtualization Platform.	Services and support personnel
Using the Solution Deployment Manager client	Describes the patch deployment and installation procedure for Avaya Aura® applications.	Services and support personnel
Maintaining and Troubleshooting		
Maintaining Avaya Aura® Session Manager	Contains the procedures for maintaining Session Manager.	Services and support personnel

Table continues…

Title	Description	Audience
Troubleshooting Avaya Aura® Session Manager	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Related links

Finding documents on the Avaya Support website on page 80

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Related links

Documentation on page 78

Training

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

New training courses are added periodically. Enter **Session Manager** in the **Search** field to display the inclusive list of courses related to Session Manager.

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

Table continues…

Course code	Course title
5U00081V	Session Manager Administration
5U00082I	Session Manager and System Manager Administration
5U00082R	Session Manager and System Manager Administration
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
5U00105W	Avaya Aura® Session Manager Overview
ATC01840OEN	Survivable Remote Session Manager Administration
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
2011V	What is new in Avaya Aura® System Manager 7.0 and Avaya Aura® Session Manager 7.0

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.

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

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

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

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

Numerics

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W