Installing and Administering Avaya Aura™ Session Manager

03-603324
Issue 1.1
Release 1.1
June 2009

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full support information, please see the complete documents, *Avaya Support Notices for Software Documentation*, document number 03-600758 and *Avaya Support Notices for Hardware Documentation*, document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

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

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

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

Contents

Chapter 1: Introduction

This book provides information on setting up Avaya Aura™ Session Manager instances. It includes procedures for

- Installing the Avaya Aura™ System Manager management system
- installing, configuring, and monitoring Session Manager instances
- Using the System Manager Common Console
- Creating administrator accounts
- Managing security
- Administering network routing for Session Manager and various SIP entities

Intended audience

This book is intended primarily for those individuals who are responsible for installing and configuring Session Manager and installing System Manager. It is also intended for administrators who configure Network Routing Policy (NRP), Session Manager instances, and network and SIP firewalls.

This book is also useful for those who are interested in information about specific features, and the Avaya personnel responsible for configuring and supporting Session Manager.

Required skills and knowledge

The audience is expected to have some experience installing Avaya products and be able to perform installation and administration procedures. They must also have a basic understanding and working knowledge of the following areas:

Operating systems in general	TCP/IP	SSH	SIP
Graphical and command line interfaces such as Windows and Linux	FTP and SFTP	LAN/WAN	Hostname/DNS

Contents

This document includes the following chapters:

Chapter 2: Obtaining licenses and login accounts

This chapter provides information about obtaining product licenses and product IDs necessary to use the product, creating login accounts necessary to install and use the product, and registering the product.

Downloading product software and licenses

The Avaya Product Licensing and Delivery System (PLDS) provides customers, business partners, distributors, and Avaya Associates with easy-to-use tools for managing asset entitlements and electronic delivery of software and related licenses. Using PLDS, you can perform activities such as license activation, license de-activation, license re-host, and software downloads.

Session Manager and System Manager installation software is available as ISO files on PLDS. After activating the license entitlements, installation administrators must download the ISO images to a PC, and choose to either burn a DVD for installation or transfer the ISO file to the target server for installation.

Session Manager is currently provided as an appliance offer. The Session Manager server arrives with an install file (.iso) already loaded on the server hard drive. System Manager is a software-only offer and requires customer installation prior to administering Session Manager.

Always review the PLDS to determine if a later service pack or release is available. If updates do exist, you should refer to the appropriate upgrade procedures, contact Avaya, or contact the Avaya Business Partner Service representative.

Obtaining licenses

You should have a license code with you before you install Session Manager and System Manager. Using Avaya Product Licensing and Delivery System (PLDS), you can activate the license entitlements and download the products.

After you buy a product, you can create license entitlements in the form of License Activation Codes (LACs). The LAC will help you identify the product among other Avaya products you hold licenses for, keep track of the number of downloads, and automatically download patches and upgrades - all the while keeping the required groups and coordinators informed, through e-mail messages. The LAC e-mail recipients should be identified during the order placement process by providing their e-mail addresses.

Prerequisites

To activate a license entitlement, you need the following:

- License Activation Codes (LACs): These are system generated codes which provide you with entitlement details linked to the code.
- License Host: The “machine” on which the license entitlements are activated. This is not a reference to where the application instance is installed.

Both these fields together uniquely identify the entitlement. All licenses provide the name of the company, the entitlements under that license for different versions of the product, the groups or customer locations that have access to each entitlement, if the product has been downloaded, and the number of downloads still available for that entitlement.

With the LACs in hand, you can use the Quick Activation screen to activate the LACs and download the product.

Activating license entitlement

To install a license for Session Manager using PLDS:

1. Log in to the Avaya PLDS Web site https://www.plds.avaya.com
2. Search for Session Manager Entitlements:
   - From the home page, click **View Entitlements** in the left navigation pane.
   - In the **Application** field, select **Session Manager**.
   - The **Status** field should be **Available or Active**.
   - Click **Search Entitlements >>**
3. Select **Options > Activate >>** on the appropriate entry.
4. Select the **Entitlement** checkbox on the Session Manager record and click **Activate >>**
5. Enter a System Name if one has not already been entered for the System Manager server that will hold the license. Enter the hostname or select it if it is already in the system.
6. Move the entitlement to a specific sold-to. Select the appropriate sold-to from the drop-down list and click **Next >>**
7. Enter the WebLM host server’s MAC address or host ID. The host ID can be found by logging into System Manager and selecting **Asset Management > Licenses (WebLM) > Server Properties**. The host ID is the Primary Host ID. Enter the host ID into PLDS for this license and click **Next >>**
8. Accept the Avaya End User License Agreement
9. In the **Email to:** field, enter the e-mail addresses to whom the license file(s) should be sent.
10. Add comments and notes if desired.

11. Complete the form and click **Finish >>**. The license XML file will be mailed as an e-mail attachment to the e-mail addresses previously specified.
12. Save the file to the local disk (laptop or PC connected to the same network) and then upload it to the WebLM server on the System Manager using the **Asset Management > Licenses (WebLM) > Install License** screen. Enter the path to the file or select the path using the **Browse** button.
13. If the license file installation was successful, the License File Installed Successfully message will be displayed, and there will now be a Session Manager section in the WebLM system.

    If the license file did not install successfully, verify that the HostID is correct and try the process again. If the license installation attempt fails again, contact Avaya Support.

Obtaining product IDs

Note:
Only Avaya Services logins have permission to run the product ID tools. These tools cannot be run with the cust or craft logins.

At the time of installation, the new system must be registered using the Functional Location (FL) and product type. Product IDs are provided for each managed element for alarm reporting.

The various managed elements have Product IDs which are used as part of the identification source of the alarm for each installed server. You can use the **`setProductID`** and **`getProductID`** commands to set and read the Product ID for the managed elements. The command **`spiritAgentCLI`** assigns the resident SAL agent Product ID.

setProductID

`setProductID ASM | ASMAS | ASM100 | ASMPLT | SM | SMELEM` ***`productid`***

Use setProductID to set the Product ID for alarming managed elements.

setProductID command managed elements

command	managed element	description
For Session Manager only		
`setProductID`	**`ASM`** ***`productid`***	Sets the Session Manager Product ID to productID. The Product ID is a 10-digit number that starts with "8"
	`ASMAS` ***`productid`***	Sets the SIP Foundation Server Product ID to productID. The Product ID is a 10-digit number that starts with "8"

	ASM100 ***productid***	Sets the Security Module Product ID to productID. The Product ID is a 10-digit number that starts with "8"
	ASMPLT ***productid***	Sets the OS/Platform/ThirdParty Product ID to productID. The Product ID is a 10-digit number that starts with "8"
For System Manager only		
setProductID	**SM** ***productid***	Sets the System Manager Product ID to productID. The Product ID is a 10-digit number that starts with "8"
	SMELEM ***productid***	Sets the Session Manager Element Manager Product ID to productID. The Product ID is a 10-digit number that starts with "8"

getProductID

getProductID ASM | ASMAS | ASM100 | ASMPLT | SM | SMELEM

Use getProductID to view the product ID for alarming managed elements.

getProductID command managed elements

command	managed element	description
For Session Manager only		
getProductID	**ASM**	Gets the Session Manager product ID. The Product ID is a 10-digit number that starts with "8"
	ASMAS	Gets the SIP Foundation Server product ID. The Product ID is a 10-digit number that starts with "8"
	ASM100	Gets the Security Module Product ID. The Product ID is a 10-digit number that starts with "8"
	ASMPLT	Gets the OS/Platform/ThirdParty product ID. The Product ID is a 10-digit number that starts with "8"
For System Manager only		
getProductID	**SM**	Gets the System Manager product ID. The Product ID is a 10-digit number that starts with "8"
	SMELEM	Gets the Session Manager Element Manager product ID. The Product ID is a 10-digit number that starts with "8"

spiritAgentCLI

`spiritAgentCLI alarmId` ***`productid`***

Use **`spiritAgentCLI`** to set and view the product ID for alarming managed elements.

spiritAgentCLI command managed elements

command	managed element	description
For System Manager and Session Manager		
`spiritAgentCLI`	**`alarmId`** ***`productid`***	Sets the SAL Agent Product ID to productID. The Product ID is a 10-digit number that starts with "5"
`spiritAgentCLI`		Gets the SAL Agent Product ID by bringing up a menu; the Product ID is on line 1.

Installed logins

This section provides details of the login accounts that are created and installed for Session Manager, System Manager, and the System Manager Common Console login accounts.

Installed OS-level logins for Session Manager

For security purposes, the **root** login has been disabled on the Session Manager. The following is a list of logins which are created during the Session Manager software installation:

- **craft** —This is an Avaya services login which accesses the system remotely for troubleshooting purposes. The Avaya Password Change System changes the password associated with this login to a random value every 82 days.
- **sroot** —This is an Avaya services root permission login which accesses the system remotely for troubleshooting purposes. The sroot login cannot be accessed directly from a login prompt except at the server console. The Avaya Password Change System changes the password associated with this login to a random value every 82 days.
- **customer** —This customer login is created by the SMnetSetup script. During execution of the SMnetSetup script, the customer access login defaults to **cust**. It is your responsibility to ensure the security of this login account. The customer login has permissions to run tools on the Session Manager server that do not require root access.
- **CDR_User** —This login is a restricted shell login that collects Call Detail Recording (CDR) data from the Session Manager server. This login is restricted to sftp access only.

Administration of the password associated with this login is performed on the System Manager Common Console by clicking **Session Manager** > **Session Manager Administration** from the left navigation pane, then editing the specific Session Manager instance.

- **asset** —This login is created during the SM100 Security Module software installation. Access to the system using this login is disabled by default.
- **spirit**—This login is created by the Secure Access Link remote alarming and remote access module for Avaya services.
- **postgres**—This login is created by the installation of the Session Manager software's PostgresSQL database system. Access to the system using this login is disabled.

Installed OS-level logins for System Manager

The System Manager installation does not create Avaya services logins on the server. OS-level administration on the System Manager server is the responsibility of the customer. You may be asked to create a login for Avaya services access to the system in the event that troubleshooting must be done. The following two logins are created by the System Manager installation for use by the System Manager:

- **spirit**—This login is created by the Secure Access Link remote alarming and remote access module for Avaya services.
- **postgres**—This login is created by the installation of the Session Manager software's PostgresSQL database system. Access to the system using this login is disabled.

Installed System Manager Common Console logins

The System Manager Common Console has two default logins that are created during installation. Individual general-purpose logins should be created for each administrative user of the System Manager Common Console. The following two logins are created during the System Manager installation:

- **admin**—This login is the default login used for administration within the System Manager Common Console.
- **system**—This is an internal login that is used for internal system purposes.

Chapter 3: Installation

To use Session Manager, you must install two different software packages on two different servers. All install files require Red Hat Enterprise Linux (RHEL) to be installed prior to their execution. System Manager requires RHEL 5.1 or 5.2, Session Manager requires RHEL 5.3.

- Avaya field technicians and partners install and configure Session Manager on one or more Avaya-provided servers. Session Manager performs the routing and other session processing functions of a Session Manager network. Currently, Avaya installs the operating system, Session Manager, and the security module on each server and ships it to the customer site.
- You install System Manager on a separate, customer-provided server. You also install and configure the RHEL 5.1 or 5.2 operating system.

Pre-installation checklist

Use this checklist to prepare yourself for the installation.

Table 1: List of pre-installation tasks

X	Tasks
	Ensure that all the equipment and cables for Session Manager are on site. Verify the contents against the list provided by the project manager.
	Verify that you have filled out the Installation Worksheets (see Appendix A: Installation and Administration Worksheets on page 99 for a blank form). The Installation Worksheets help you complete the configuration and administration fields.
	Ensure that you have the appropriate CAT5 cables.
	Obtain the product ID needed for alarming. For details, see Obtaining product IDs on page 13.
	Verify that you have the license file for Session Manager.
	Keep the DVDs handy with Session Manager and System Manager.
	Ensure that a server installed with the required OS is available for the System Manager installation.

High-level installation process

The installation process involves the following:

1. Installing System Manager on a customer-provided server
2. Installing the license file using the System Manager Common Console.
3. Installing the Avaya S8510 Server into the rack.
4. Configuring Session Manager with customer parameters.
5. Administering Session Manager.
6. Testing the installation.

System Manager Installation

You install System Manager at your site on a customer-provided server. Avaya does not provide any hardware. You can install System Manager in two ways:

- Install System Manager using a DVD.
- Install System Manager using an ISO Image of the installer file.

System requirements for the System Manager

Hardware requirements	Intel Xeon Dual Core 3-GHz processor 4-GB RAM NIC 100 MB Minimum disk space of 40 GB
Operating system	Red Hat Enterprise Linux 5.1 or 5.2 only
Sun Java software	Java Runtime Environment 1.6 or higher
Other	Server does not run any other software The firewall must be disabled SELinux must be disabled

Prerequisites

The installer file includes the System Manager software in ISO format. Ensure that you complete the following steps:

- Download the System Manager ISO image from the Avaya Product Licensing and Delivery System web site https://www.plds.avaya.com
- Verify that SELinux is disabled on the System Manager server. In the file **/etc/selinux/config** verify that the following option is set:

  ```
  SELINUX=disabled
  ```

- Verify that the System Manager server has only SDP products running on it.
- Verify that the correct time and locale are set.
- Verify that the firewall is disabled using the following commands:

  ```
  $ service iptables stop
  ```

  ```
  $ chkconfig --levels 2345 iptables off
  ```

- After installing the OS, you must check the **/etc/hosts** file. Verify that the **/etc/hosts** file on the System Manager server has the correct format, including the correct IP address and name of the System Manager. Here is an example:

  ```
  # Do not remove the following line, or various programs
  # that require network functionality will fail.

      127.0.0.1       localhost.localdomain     localhost
      ::1             localhost6.localdomain6   localhost6
      192.168.0.13    systemmgr.mycompany.com   systemmgr
  ```

Customer-provided equipment

You provide the following equipment:

- Server (see System requirements for the System Manager on page 18)
- Keyboard, monitor, and mouse (see Connecting using the keyboard, monitor, and mouse on page 24
- Blank DVDs of at least 4 GB each if using physical media
- CAT5 Ethernet straight-through cables
- NTP server (if using)

Installing System Manager using a DVD

Run the System Manager installer from the console or from a SSH session login with root privilege. The **install.sh** script is included in the downloaded *avmgmt-installer-<version>.zip* file. It will install the System Manager and the Avaya Session Manager Element Manager (SMEM).

To install System Manager software using a DVD:

1. Log in to a console on the System Manager server or SSH login with root privilege.
2. Insert the System Manager DVD in the CD tray and mount the DVD using the commands

   ```
   $ mount /dev/cdrom /mnt
   $ cd /mnt
   ```

3. Run the installer with the following command within the directory where the zip file has been expanded:

   ```
   $ ./install.sh
   ```

   The installation automatically continues for approximately 40 minutes without technician assistance. An indication is given when the installation is complete.

4. When the installation is complete, eject the DVD with the following commands:

   ```
   $ cd /
   $ eject
   ```

   This completes the installation of the System Manager.

Installing System Manager using the ISO image

If you download the ISO images of the installer files from PLDS and then copy them to the System Manager and Session Manager servers using scp or winscp, you can mount them without copying to physical media as follows:

1. Login to a console on the System Manager server or SSH login with root privilege.
2. Transfer the System Manager ISO image to the System Manager server.
3. Enter the following commands on the command line:

   ```
   $ mkdir /iso
   $ mount -o ro,loop /home/craft/avmgmt-1.1.1.1-18000.iso /iso
   $ cd /iso
   $ bash install.sh
   ```

4. When the installation is complete, enter the following commands:

   ```
   $ cd /
   $ umount /iso
   ```

   This completes the installation of the System Manager.

Setting product IDs

You need to set the product IDs to complete the configuration. See Obtaining product IDs on page 13 for information on obtaining the product IDs and the command formats.

To set the product ID:

1. Log in with a login that has root permissions.
2. Enter **`setProductID`** ***`mgdElem productID`***, where ***`mgdElem`*** is the managed element code (or SE code) and ***`productID`*** is the product ID number for one managed element.
3. Enter **`getProductID`** ***`mgdElem`*** to verify that the product ID was entered correctly.
4. Repeat the commands for each managed element.

System Manager is successfully installed.

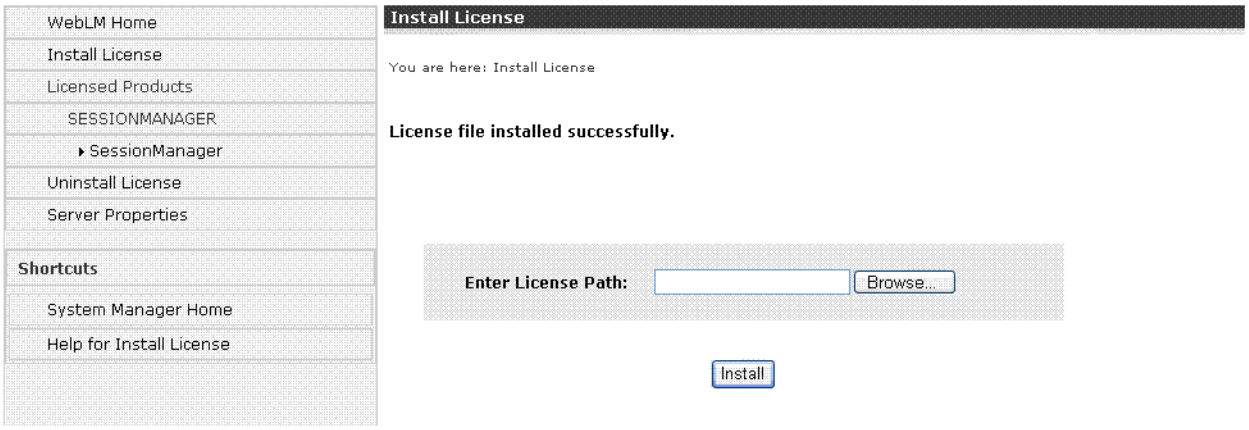
Installing the WebLM license file

To install WebLM license file on the server, complete the following steps using the System Manager Common Console.

1. Log on to the System Manager Common Console.
2. From the left navigation pane, click **ASSET Management**, then click **Licenses (WebLM)**.
3. Click **Install license**.
4. Enter the path for the license file or select **Browse** and navigate to the location where you saved the license file.

5. Click **Install**.

   The System Manager Common Console displays a message that the license file was installed successfully.



Enabling trust management

Before you install Session Manager software on a Session Manager server, you must set up an enrollment password in System Manager. For the procedures, see Enrolling a password on page 38.

Session Manager installation

At the customer site, field technicians install the Avaya S8510 Server in the rack, customize Session Manager, administer the network routing policy, verify the security settings, and test the total solution before leaving the customer site.

Session Manager Release 1.1 supports up to three Session Manager instances. The servers running Session Manager are in different locations and likely in different geographical regions. You can set up and administer the three Session Managers concurrently.

For Release 1.1, Session Manager runs on the Red Hat Enterprise Linux Version 5.3 operating system.

Avaya-provided equipment

For Session Manager installation, Avaya provides the following:

- Server belonging to the Avaya S8510 Server Family
- SM100 card installed on the above server
- Power cord for the server

The Session Manager server has the following configuration:

- RAID Level 1 mirroring for reliability - 250GB capacity
- System Name - avaya-asm
- Eth0 - 192.168.02/24
- Eth1 - 192.11.13.6/30 (reserved for service technician access)
- Eth2 and Eth3 - unused
- DNS Domain - localdomain
- DNS Server - 127.0.0.1

Customer-provided equipment

You provide the following equipment:

- Keyboard, monitor, and mouse
- Blank DVDs for burning the ISO images if necessary
- 2 CAT5 Ethernet straight-through cables
- Optional separate Ethernet switches for the SIP traffic and client management networks.

Session Manager software

The Session Manager software installs on top of the Red Hat Enterprise Linux Server 5.3 operating system. This software includes some additional RPMs that may or may not be part of the base Red Hat Linux OS, but Session Manager may require newer versions of these

packages. Below is a list of the additional RPM packages which are installed by the Session Manager installer:

Package Description	RPM Name
Java 1.6 Sun Compatibility Libraries	java-1.6.0-sun-compat
PostgreSQL Database System ver 8.2.6	postgresql
	postgresql-docs
	postgresql-libs
	postgresql-contrib
	postgresql-server
Java Development Kit & Runtime 1.6.0_11	jdk-1.6.0_11fcs
Security Module-100 Hardware Drivers & Software	asset-gefanuc
Core Services Watchdog (Process/Service Management)	cs_watchd
XML to C/C++ language binding for web services	gsoap

Session Manager software also contains the JBOSS Application Server and the Avaya SIP Application Server. Most of this software is installed in /opt/Avaya.

The *Avaya Aura Session Manager: Port Matrix* document identifies which network ports must be open in firewalls. This document is available to Avaya customers, associates, and business partners via SSO and the InSite Knowledge Management Database by logging in to http://support.avaya.com

Connecting using the keyboard, monitor, and mouse

Location of ports for connecting a keyboard, monitor, and mouse shows where to connect the keyboard, monitor, and mouse to the Avaya S8510 Server.

Figure 1: Location of ports for connecting a keyboard, monitor, and mouse

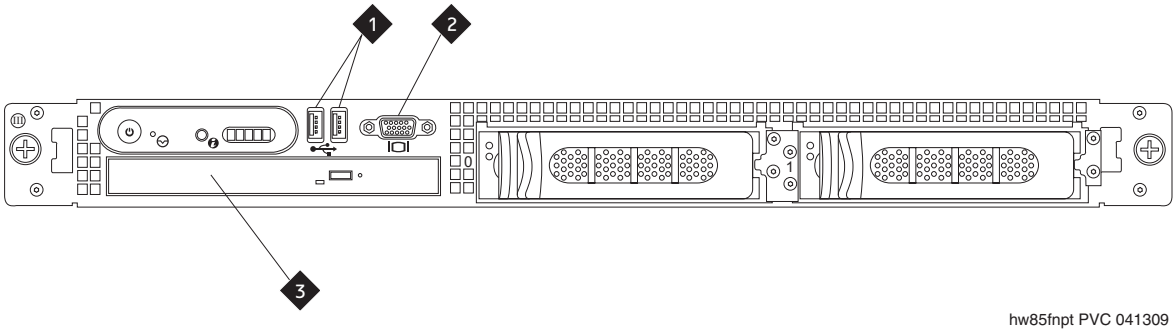


Figure notes:

1. **USB ports for connecting the keyboard and mouse (see Figure 2: Back view of the Avaya S8510 Server Family server showing the SM100 card**
2. **Video port for connecting the monitor**
3. **CD/DVD drawer**

Connecting to the server using the laptop

To access the server directly, use a computer with the following minimum specifications:

- A Windows XP operating system
- 32-MB of RAM
- 40-MB of available disk space
- A network interface card (NIC) with a 10/100BaseT Ethernet interface
- A 10/100 BaseT Ethernet category 5 or better cable with an RJ45 connector on each end (MDI to MDI-X)
- A CD-ROM drive.
- An X server program such as cygwin/X

6. Plug one end of the Ethernet cable into the Services access port on the back of the server. Plug the other end of the into the NIC on your computer.
7. Configure your network connection as follows:
   - IP address: 192.11.13.5
   - Subnet mask: 255.255.255.252

Setting up the S8510 Server

To set up the S8510 Server:

1. Install the Avaya S8510 Server in a rack. See *Installing the Avaya S8510 Server Family and its Components* (03-602918) for the step-by-step procedures.
2. Connect the Ethernet cables. See Figure 2: Back view of the Avaya S8510 Server Family server showing the SM100 card for the location of the Ethernet ports on the server.
   - One end of an Ethernet cable plugs into the back of the SM100 card (left-most port on the SM100). The other end connects to your network. Because this connection is for the client SIP traffic network infrastructure, make sure it connects to a separate Ethernet switch from the management network.
   - One end of the second CAT5 Ethernet cable plugs into the native NIC port (GB1) on the S8510 server. The other end connects to your network. Because this connection is for the client management network infrastructure, make sure it connects to a separate Ethernet switch from the SIP traffic network.

Figure 2: Back view of the Avaya S8510 Server Family server showing the SM100 card

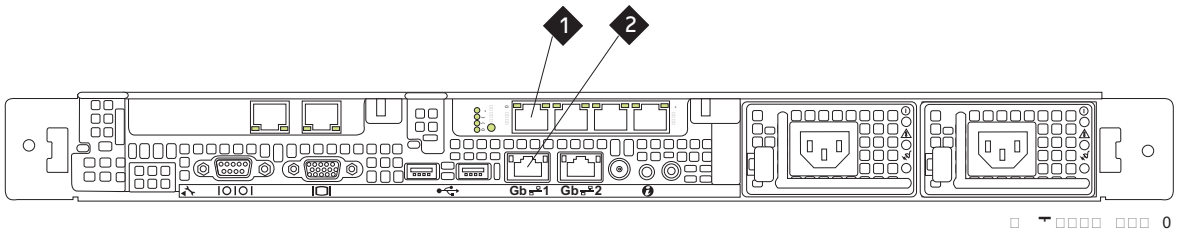


Figure notes:

1. **Ethernet port on the SM100 card for the SIP traffic network**
2. **Ethernet port on the server NIC for the client management network (Eth0)**

Configuring Session Manager

This section provides the steps to add the IP addresses and domain names specific to the customer site. Before running the network configuration script, ensure that you have the following with you:

- The License Entitlement Codes or the license key for the product

- The IP addresses, DNS, NTP, etc. for the customer site (see Appendix A: Installation and Administration Worksheets for more information required at the time of installation)

Follow these steps to configure the Session Manager:

1. Set up the server with the mouse, keyboard, and monitor.

   Note:
   Alternatively, you can connect a laptop to the Eth1 NIC with a standard CAT5 Ethernet cable. Set the laptop IP address as the Avaya standard 192.11.13.5. SSH to craft@192.11.13.6 (Avaya standard).

2. If the server has not been powered on, turn on the power on the server.
3. Log into the Session Manager server with the user name *craft* and password.
4. Run the command **`$ ./SMnetSetup`**

   You will be prompted for a password. Enter the craft password, then press ENTER to continue. This command will run a network configuration script. You will be prompted for the Session Manager management interface IP address, host name, default gateway for this interface, DNS timezone, date and time, NTP, customer SIP domain, and System Manager address. Appendix B: Configuring Individual SIP Entities gives an example of the output of **`SMnetSetup.`**

5. Choose **Configure a device params** and configure eth0 with the IP address, netmask, and default gateway provided for your management network for this Session Manager. When finished, select **OK**, then **Save**.

   Note:
   Change ONLY the IP address, netmask, and default gateway (you must use static addressing) on this form. The IP address assigned to the eth0 network interface on this server is used for management only. You will not be routing an SIP traffic through this interface.

6. Choose **Edit DNS Configuration** and configure the Hostname, Primary DNS, Secondary and Tertiary DNS (if applicable) and the DNS search domains. When finished, select **OK**, then **Save&Quit.**

   Note:
   Enter a system name or Fully Qualified Domain Name (FQDN) for the Hostname. If using an FQDN, make sure the local domain used in DNS matches the domain used in the host name.

7. The Local Timezone is configured next. Select the timezone and choose **OK**.
8. The GUI will now exit and you will be prompted for all remaining required information.
9. Enter the local date and time.
10. If using NTP, enter the Primary NTP server, Secondary and Tertiary (if applicable).
11. Choose to configure a customer login (optional), entering a password for chosen user when prompted. This login may be used to access the Session Manager from the console or SSH over your network.

12. Enter the IP address of the System Manager which will be used to manage this Session Manager. At this point, the configuration will begin and will take approximately 15 minutes.
13. When the configuration is complete, the current settings are displayed. Review the settings and press ENTER if you agree to the settings, or press Ctrl-C to abort.
14. When prompted, enter the trust management password established during the System Manager installation.
15. When prompted, choose to reboot the newly configured Session Manager server. The reboot ensures that all new settings take effect.

Setting product IDs

You need to set the product IDs to complete the configuration. See Obtaining product IDs on page 13 for information on obtaining the product IDs and the command formats.

To set the product IDs:

1. Log in with a login that has root permissions.
2. Enter **`setProductID`** ***`mgdElem productID`***, where ***`mgdElem`*** is the managed element code (or SE code) and ***`productID`*** is the product ID number for one managed element.
3. Enter **`getProductID`** ***`mgdElem`*** to verify that the product ID was entered correctly.
4. Repeat the commands for each managed element.

Final installation steps

Session Manager is now successfully customized with IP addresses and domain names of the organization. However, you must complete the following administration steps before leaving the customer's site.

- Add Session Manager instances and SIP entities. See Adding a SIP entity as a Session Manager instance on page 86 for more information.
- Complete the Network Routing Policy administration tasks in the correct order. See Network Routing Policy initial administration on page 52 for the specific order of the administration tasks.
- Configure the various SIP entities to work with Session Manager. See Appendix B: Configuring Individual SIP Entities on page 103 for the list of some SIP entities and the application note that contains the configuration information.
- Verify security default settings and change as necessary. See Chapter 6: Managing Security on page 37 for more information.

- Set administration users logins and permissions. See Chapter 5: Managing Users on page 33 for more information.
- Test the total installation. See Testing the installation on page 29 for more information.

Testing the installation

Before running these tests, you must verify that the software is installed and configured properly and that the servers and applications are communicating before leaving the customer's site.

1. Log on to the System Manager Common Console (Logging on to the System Manager Common Console)
2. Click **Session Manager > Maintenance Tests** in the left navigation pane.
3. Select the System Manager server in the pull-down list, and click **Execute All Tests.**
4. Verify that all tests show **Success** status.
5. If the data replication test fails, click **Session Manager > Data Replication Status** in the left navigation pane to identify which Session Manager is having replication problems.
6. Click **Session Manager** > **Security Module Status** to display SM100 card status.
7. Verify that **Security Module Deployment** is **Up** for all Session Managers.
8. Click **Session Manager** > **System State Administration** in the left navigation pane.
9. Verify that the installed software versions of all Session Managers are the same version and that all Session Manager servers are in the **Management Enabled** state.
10. Click **Session Manager** > **Maintenance Tests** in the left navigation pane.
11. Select each Session Manager instance, and click **Execute All Tests**.
12. Verify that all tests show **Success** status.

    Note:
    For more information about troubleshooting, refer to *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (03-603325)
13. Change the service state to **Accept New Service** on the **Session Manager** > **System State Administration** screen.

Chapter 4: System Manager Common Console

System Manager is a central management system that delivers a set of shared management services and a common console across multiple products. System Manager includes the following shared management services for Session Manager:

- Asset Management: Manages the resources and licenses.
- User Management: Provides central user administration of all user properties. The centralized administration reduces the need for replicating the user's data across multiple products.
- Monitoring: Provides a central point for receiving alarms from the Secure Access Link (SAL) Agents. Supports alarm monitoring, acknowledgement, configuration, clearing, and retiring. It can also send customer SNMP traps to an external SAL Enterprise or Enterprise Management System (EMS). It also provides a central point for receiving log events formatted in the common log format from the SAL Agents.
- Network Routing Policy: Defines all SIP entities in the network and how calls route to them.
- Applications: Provides an interface to manage the instances of applications running on the different servers.
- Security: The System Manager console provides authentication of administrators and authorization by applying role-based access control. It also provides trust and certificate management where trust management is the definition of trust relationships between hosts and services, and certificate management is the lifecycle management of identity certificates.
- Settings: Provides backup and restore capability including backing up and restoring configuration data, and secure file copy.
- Session Manager: Provides configuration and monitoring of Session Manager instances, setting of tracing properties for security modules, and management of call bandwidth usage.

The System Manager Common Console is the management interface for Session Manager. You must log on to the System Manager Common Console to perform any administration or configuration.

You must have a user account to log on to the System Manager Common Console.

Logging on to the System Manager Common Console

To log on to the System Manager Common Console:

1. Open a Microsoft Internet Explorer or Firefox browser window.
2. Enter the URL for the System Manager Common Console. For example, **https://SystemManagerHostname/IMSM**
3. Enter the user name in the **User Name** field.
4. Enter the password in the **Password** field.
5. Click **Log On**, then click **OK**.

Chapter 5: Managing Users

User management is a shared management service available on the System Manager Common Console navigation pane that provides central user administration of all user properties. The centralized administration reduces the need for replicating the user's data across multiple products. The following is the list of operations that you can perform using the User Management shared service:

- Add a new user profile
- View a user account
- Modify a user account
- Remove a user account

Access to the System Manager Common Console requires a valid user name and password. Avaya recommends that you create a limited number of accounts and ensure that the passwords they use are secure.

Users with administrator privileges can add, modify, and delete accounts on the System Manager Common Console. To obtain a user account and password to the console, contact your system administrator.

Note:
Session Manager 1.1 only supports users with administrator privileges.

Add a new user profile

To create a new user profile:

1. Log in to the System Manager Common Console as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane.
3. Click **New.**
4. On the New User Profile screen, enter the appropriate information and click **Commit.**

Note:
The field names that are marked with * are mandatory fields. You must enter valid information in these fields for the successful creation of the user. See the User Profile field descriptions in the online Help for more information.

Creating a duplicate user

Use this functionality to copy an existing user account to create a new group. When you create a duplicate user account, the system copies all the information from the existing user account to the new user account.

1. Log in to the System Manager Common Console as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane.
3. On the User Management screen, select the user account that you want to duplicate.
4. Click **Duplicate.**
5. On the User Profile Duplicate screen, enter the appropriate information and click **Commit.**

View a user account

To view a user account:

1. Log on to the System Manager Common Console as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane.
3. On the Users screen, select a user. You can view only one user account at one time.
4. Click **View** to view the selected user account.

Modify a user account

To modify a user account:

1. Log on to the System Manager Common Console as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane.
3. On the Users screen, select a user. You can edit only one user account at one time.
4. To edit a user account, perform one of the following steps:
5. Click **Edit.**
6. Click **View** > **Edit.**
7. Modify the information and click **Commit** to save the changes to the database.

Remove a user account

To remove a user account:

1. Log on to the System Manager Common Console as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane.
3. On the User Management screen, click **Delete.**
4. On the User Delete Confirmation screen, click **Delete.**

Note:
This operation marks the deleted users as deleted and stores them in the database in a list of deleted users.

.

Chapter 6: Managing Security

This chapter details the tasks that you need to perform to manage security for Session Manager. Security needs to be managed using:

- trust management and certificates
- network firewall
- SIP Firewall

Trust management

System Manager Trust Management provisions and manages certificates of various applications (servers/devices), enabling them to have secure inter-element communication. It provides Identity (also known as Server) and Trusted (also known as Root, Issuer, or Certificate Authority (CA)) certificates which applications can use to establish mutually authenticated Transport Layer Security (TLS) sessions.

Session Manager ships with a default identity/server certificate issued by a SIP-Certifying Authority (SIP CA), which is a Certificate Authority that is controlled by Avaya and is only used to issue non-unique certificates to enable out-of-box support for TLS sessions. Additionally, Session Manager also bundles a default set of trusted certificates which are used to verify far-end certificates during a TLS session establishment.

During the installation of Session Manager, the installation script prompts you for an Enrollment Password which enables that Session Manager instance to request unique certificates from the System Manager Certificate Authority for services including SIP-TLS and management.

You can perform the following operations related to Trust Management:

- Obtain an Enrollment Password for application install and deployment
- Assign identity certificates to be used by the security module
- Add, view, and remove trusted certificates to the Session Manager security module
- View and obtain the Identity and Server Certificates of the Session Manager security module

The sections that follow describe how you can use System Manager and Session Manager to perform these operations.

Enrollment password

Applications such as Session Manager use the enrollment password during the initial installation and deployment process. This password is also referred to as the certificate enrollment password.

To ensure that a compromised password is not used, there are two constraints that bind the usage of an enrollment password—expiration time and count. You must keep the security implications in mind before selecting the values for these options.

Enrolling a password

To enroll a password:

1. Log on to the System Manager Common Console.
2. Click **Security > Trust Management > Enrollment Password.**

   If a password has already been generated, copy it from the **Existing Password** box if the **Time Remaining** or the **Unused Certificates** fields are not set to zero.
3. If an existing password is not present or the time or count are not set to zero, select the expiration of password in days in the **Password expires in** field.
4. In the **Certificate allowed** field, select the number of certificates.

   Note:
   Select at least ten certificates per Session Manager instance.
5. Click **Generate** if you wish to use a randomly generated string as a password. If you click **Generate**, the password field displays the generated password. If you do not wish to use a randomly generated string, enter a password.
6. Click **Done.**

   Note:
   When you click **Done**, the system updates the number of certificates displayed next to the **Unused Certificate** label with the number of certificates selected in the **Certificate allowed** field. The system also updates the time displayed next to the **Time remaining** label with the value selected in the **Password expires in** field.

   You ***must*** remember this password. You need to provide it as input at the time of installing Session Manager.

Trusted certificate operations

Viewing trusted certificates

To view trusted certificates:

1. Log on to the System Manager Common Console.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management screen, click **More Actions > Configure Trusted Certificates.**
4. On the Trusted Certificates screen, click **View.**

The View Trust Certificate screen displays the details of the selected certificate.

Removing trusted certificates

To remove a trusted certificate:

1. Log on to the System Manager Common Console.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management screen, click **More Actions > Configure Trusted Certificates.**
4. On the Trusted Certificates screen, select the certificates and click **Remove.**

Trust Management removes the certificates from the list of trusted certificates for the application instance.

Identity certificate operations

Assigning an identity certificate

Session Manager provides the capability of switching the active certificate being used by the Security Module to the default certificate or the unique certificate issued for that instance by the System Manager CA.

Note:
This operation has critical security implications. Please refer to the *Avaya Aura Security Guide* to understand when to select one of the two options.

To switch between these certificates, complete these steps:

1. Log on to the System Manager Common Console.
2. Click **Session Manager > Security Module Status**.
3. Under the **Security Module Actions** section on this screen, use the **Security Module Certificate** button to perform a certificate operation on the selected Session Manager Instance. Select one of the following options from the drop-down menu:
   - **Use Default Certificate (Issued By SIP CA)** - use the default identity certificate for the Security Module on that Session Manager instance
   - **Use Certificate from System Manager** - use the unique certificate issued to the Security Module during installation
4. After selecting the option, you should see the status change accordingly in the Statistics section. The Security Module will use the newly assigned identity certificate for future TLS sessions.

Viewing identity certificates

To view identity certificates:

1. Log on to the System Manager Common Console.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management screen, click **More Actions > Configure Identity Certificates.**

The Identity Certificate screen displays the identity certificates.

Replacing an identity certificate

To replace an identity certificate:

1. Log on to the System Manager Common Console.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management screen, click **More Actions > Configure Identity Certificates.**
4. On the Identity Certificate screen, select an Identity Certificate. Click **Replace**.
5. On the Replace Identity Certificate, perform one of the following steps:

- Click **Replace this Certificate with Internal CA Signed Certificate**. Enter Common Name, Org Unit, Organization, and Country in the respective fields. Select Key size/type, subjAltname from the respective fields. Click **Commit** to replace the identity certificate with the internal CA signed certificate.
- Click **Import third party PCKS # 12 file**. Enter the file name in the **Please select a file** field. Enter the password in the **Password** field. Click **Retrieve Certificate**. The Certificate Details section displays the details of the certificate. Click **Commit** to replace the certificate with the imported third party certificate.

Network firewall

Session Manager has the network firewall running on the SM100 and the Session Manager SIP Server.

For both of the network firewall instances, default rules are installed automatically during initial installation:

- All of the ports used by the Session Manager SIP Server and SM100 (defined by port matrix) are opened. All unused TCP/UDP ports are closed.
- SIP Listen ports are opened and closed dynamically in SM100 as per the Network Routing Policy (NRP) SIP Entity configuration.

The network firewall also provides network layer DoS Protection. Following are some examples of the protection provided:

- TCP Syn Flood
- IP Options
- CMP timestamps
- CMP Redirects
- Source Routed Packets
- Reverse Path Forwarding
- Invalid IP Packets
- Bad TCP Packets

Note:
Network Firewall rules are not administrable.

Important:
All of the ports used by Session Manager are documented in *Avaya Aura Session Manager: Port Matrix*. This document is available via SSO and the InSite Knowledge Management Database (must login to see the document) at http://support.avaya.com

SIP Firewall

SIP Firewall is an inline packet-based SIP filtering engine that runs within the Security Module (SM100) of Session Manager. SM100 handles all the SIP connections for Session Manager. All incoming SIP packets are passed through the SIP Firewall before forwarding them to the Session Manager SIP Server. SIP Firewall performs deep packet inspection at the SIP Layer to detect any anomalies and application-layer threats. It also provides protection from SIP Layer Denial of Service (DoS) attacks. You can apply SIP Firewall filtering to SIP TLS connections as well (packets are decrypted before SIP filtering is applied).

Session Manager applies SIP entity trust validations to any new SIP TCP/TLS connection or the SIP UDP packet before the SIP Firewall allows the SIP packets to pass through. For more information regarding SIP entity trust validations, see Authentication of trusted SIP entities on page 69

SIP Firewall configuration is rule-based. These rules are managed using the System Manager Common Console. You can administer three categories of rules: Rules, Blacklist rules, and Whitelist rules.

Rules

Each SIP Firewall rule has the capability to send log or alarm messages to the Secure Access Link (SAL). You can combine logging with other actions. Avaya recommends that you always enable logging in each SIP Firewall rule to have a record of what actions were taken by the SIP Firewall. Logging can be used independently (with the **None** action) and can generate logs and alarms for flood-tracking. Note that SIP Firewall log messages are rate-limited. Each rule can log a maximum of 1 log message per second. This rate-limiting of log messages provides protection from flooding the logging system which may occur because of bad configuration of the SIP Firewall rule.

You can apply SIP filtering and DoS protection to:

- SIP gateway/proxy connections (SIP Multiplexed connection/trunk). For example, a SIP Firewall rule can set rate limit on a number of INVITE messages from a specific user within a SIP connection from a SIP gateway without affecting the traffic from other users in that gateway.
- SIP TLS connection. SM100 decrypts all the incoming SIP TLS packets before any filtering rules are applied by the SIP Firewall.
- Reporting using the Secure Access Link (SAL)

Deep inspection filtering

SIP Firewall rules provide the following filters for deep inspection:

- SIP Layer content
- IP/Transport layer parameters such as IP address, protocol, port, and so on

You can combine both SIP Layer content and IP transport layer parameters in a single firewall rule. For example, a SIP Firewall rule can limit the high rate of INVITE packets from a remote IP address.

Denial of Service protection

SIP Firewall provides protection from the Denial of Service (DoS) attacks as follows:

- Flood Protection from a specified source
- Advanced Flood Protection—A rule may be defined to detect/mitigate flood attacks within the live SIP Stream without knowing the flood source in advance. In other words, the host causing the flood need not be known when the rule is configured. A high performance database tracks all matched messages.
- Rate-Limiting—A “Rate Limit” action may be configured to limit the number of SIP packets that are forwarded within a given period. See Specifying a new SIP Firewall rule on page 46 for details on how to configure Rate Limit rules.
- Rate-Blocking—A “Rate Block” action may be configured to completely block an offending SIP source once the traffic reaches a specified threshold within a given period. Traffic is then blocked until the configured timeout expires. See Specifying a new SIP Firewall rule on page 46 for details on how to configure the Rate Block rules.
- Signature Detection—A rule may be configured to perform signature detection and drop those packets matching signature. Both simple and regular-expression string searching is supported across the entire SIP header region of the message or across the full message (headers and body).

Blacklist

SIP Blacklist enables you to block any known bad SIP elements. The SIP Firewall drops any SIP packet matching a rule in the Blacklist.

Whitelist

SIP Whitelist enables you to allow any known good SIP elements. SIP Firewall allows any SIP packets matching a rule in the Whitelist; no other filtering rule is applied.

Rule precedence and traversal

The precedence order for using the rules is:

- Blacklist
- Whitelist
- Rules

Each list above can contain more than one rule. Session Manager traverses the rules within any of the above lists from top to bottom.

SIP Firewall is a packet-based filtering engine. Any time a packet is matched with a rule, the rule traversal is stopped and the packet is either permitted or dropped as per the rule action. The only exception to this is the rules defined with a **None** Action.

SIP Firewall default rule set

SIP Firewall provides a default rule set. Avaya recommends that default rules be used after the initial installation of Session Manager.

Important:
Mandatory Administration action

Before enabling SIP Firewall, you must add the following IP addresses to the Whitelist. These IP addresses are used by the Session Manager SIP Server. Adding them to the Whitelist ensures that SIP filtering rules are not applied on the outgoing traffic from Session Manager SIP Server and are only applied to the incoming SIP traffic from Network.

- 192.11.13.2 (added as a part of default rules)
- Session Manager Management IP address

Configuring the SIP Firewall

To configure the SIP Firewall:

1. From the System Manager navigation pane, click **Session Manager > SIP Firewall Configuration**.
2. Click the **Session Manager Instances** button to display the list of Session Manager instances. Select a Session Manager instance from the list. Select **More Actions** to retrieve current, default, or backup configuration or to save a configuration as a backup configuration. By default, the system displays the default configuration of the SIP Firewall.

3. To use the default rules, select **Retrieve Default Configuration** under **More Actions** and click **Save** to save the configuration to the selected Session Manager instance(s).
4. Under Rules, you can perform the following operations:
   - **New** —To create a new rule, click **New**. You can define up to 50 rules. For information about creating rules, see Specifying a new SIP Firewall rule on page 46.
   - **Edit** —To modify an existing rule, select the left-most check box and click **Edit**.
   - **Delete** —To delete a rule, select a rule and click **Delete**.
   - **Enabled** —To enable or disable all the rules, select or clear the **Enabled** check box.
   - Select a rule from the list and click **Up** or **Down** to move the rule and change the order in which it gets executed.
5. Under Blacklist, specify the following:
   - **Enabled**—Select **Enabled** to drop messages from untrusted hosts.
   - ***Key***—Select a key for filtering messages for blacklisting from Remote IP address, CONTACT, and FROM.
   - **Value**—Value of the Key. Specify the following values.

     Remote IP address—IP address of the host from where the messages are sent.

     CONTACT—String to look for in the “Contact” SIP Header in the SIP message. This string need not be an exact match with the “Contact” SIP header content and can be a subset of the string present in the “Contact” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.

     FROM—String to look for in the “From” SIP Header in the SIP message. This string need not be an exact match with the “From” SIP header content and can be a subset of the string present in the “From” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
   - **Mask**—Specify the Subnet mask only when you have used the Remote IP address in the Key. This can be used to Blacklist an entire IP subnet.
   - **New**—Create a new rule to drop messages from untrusted hosts. You can create up to 200 Blacklist rules.
   - **Delete**—Delete a selected blacklist rule.
6. Under Whitelist, specify the following:
   - **Enabled**—Select **Enabled** to allow messages from trusted hosts to bypass the SIP Firewall.
   - **Key**—Select a key for filtering messages for whitelisting from Remote IP address, CONTACT, and FROM.

- **Value**—Value of the Key. Specify the following values.

  Remote IP address—IP address of the host from where the messages are sent.

  CONTACT—String to look for in the “Contact” SIP Header in the SIP message. This string need not be an exact match with the “Contact” SIP header content and can be a subset of the string present in the “Contact” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.

  FROM—String to look for in the “From” SIP Header in the SIP message. This string need not be an exact match with the “From” SIP header content and can be a subset of the string present in the “From” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.

- **Mask**—Specify the Subnet mask only when you have used the Remote IP address in the Key. This can be used to Whitelist an entire IP subnet.
- **New**—Create a new rule to allow messages from trusted hosts.
- **Delete**—Delete a selected whitelist rule.

7. Before enabling SIP Firewall, you must add the following IP addresses to the Whitelist. These IP addresses are used by the Session Manager SIP Server. Adding them to the Whitelist ensures that SIP filtering rules are not applied on the outgoing traffic from Session Manager SIP Server and are only applied to the incoming SIP traffic from Network.
   - 19.2.11.13.2 (added as a part of default rules)
   - Session Manager Management IP address
8. Click **Save** to save the SIP Firewall configuration. After saving, you can review the results of the configuration changes to the SIP Firewall using **Monitoring** > **Logging** from the System Manager navigation pane. (See *Maintaining and Troubleshooting Avaya Aura Session Manager* for specific details of the log messages.)

Specifying a new SIP Firewall rule

To specify a new SIP Firewall rule:

1. From the navigation pane, click **Session Manager** > **SIP Firewall Configuration**.
2. On the Firewall Configuration screen, under Rules, click **New**.
3. Under General, specify the following options:
   - **Enabled**—Select or clear the check box to enable or disable this rule for the selected Session Manager.
   - **Name**—Name of the rule. The name can have a maximum of 80 characters.

- **Action Type**—Specify the action to be taken if rule conditions are met. The valid action types are:

  None—No specific action required. This action can be used when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the **None** action.

  Permit—If the rule conditions are fulfilled, allow the SIP message to pass through the SIP Firewall.

  Drop—If the rule conditions are fulfilled, drop the SIP message.

  Rate Block—If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout (as defined by the Threshold parameters).

  Rate Limit—If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of remaining period (as defined by the Threshold parameters).

- **Log Type**—Specify if a log is to be generated or not, and if an alarm should be sent. You must specify **Log Type** when the **Action Type** is None.
- **Log Message**—Specify the log message that should be stored.

4. Under IP Layer Match Options, specify the following:
   - **Protocol**—Select a protocol if you want the rule to be used for a specific protocol.
   - **Remote IP Address**—For any incoming SIP message, select **Any** to use the rule for all IP addresses, or select **Specify** to use the rule for a specific IP address.
   - **IP Address**—Type the IP address if you selected **Specify** for **Remote IP Address**.
   - **Mask**—Network mask for the specific IP address.
   - **Remote Port**—For any incoming SIP message, select **Any** to use the rule for all ports, select **Specify** to use a single port, or select **Specify Range** for a range of ports.
   - **Start**—For the **Specify** option, select a port number. For the **Specify Range** option, specify the port number to start the range.
   - **End**—For the **Specify Range** option, specify the port number to end the range. The range includes both the Start and End port numbers specified.
   - **Local Port**—For any incoming SIP message, select **Any** to use the rule for all ports, select **Specify** to use a single port, or select **Specify Range** for a range of ports.
   - **Start**—For the **Specify** option, select a port number. For the **Specify Range** option, specify the port number to start the range.
   - **End**—For the **Specify Range** option, specify the port number to end the range. The range includes both the Start and End port numbers specified.
5. Under SIP Layer Match Options, specify the following:

- **Key Type**—Select the key type that the rule should match from the list. You can add up to five key type match options. If more than one match options are defined, then logically, AND of the options is used to create a search pattern.

  All SIP Headers—This option searches for the Value within all the SIP headers for the SIP packet

  All SIP Headers/Body—This option searches for the Value in the SIP headers & body portions for the SIP packet

  REQUEST-METHOD, RESPONSE-CODE—All the remaining entries in the **Key Type** list are SIP headers and look for the value within the specified SIP header only.

- **Value Type**—Specify whether the key type is a string or a regular expression. You can create regular expressions using the PERL version 5.8 syntax.
- **Value**—Value of the selected key type. This string need not be an exact match and can be a subset of the string present in the SIP header being used for search.

6. Under IP/SIP Layer Track, select an option for tracking SIP messages only if you have selected either **Rate Block** or **Rate Limit** in the **Action Type** field or with **None** in the **Action Type** with **Log Type** enabled. You cannot use IP/SIP Layer Track with Permit/Drop Actions. This option provides advanced flood tracking in the SIP Firewall. Refer to the SIP Firewall Configuration Section in the *Avaya Aura Security Guide* for details and examples on using IP/SIP Layer Track
   - **None**—No tracking used.
   - **Remote IP address**—Track messages for a specific IP address of the remote host.
   - **Local Port**—Track messages for a specific local port.
   - **From**—Track messages for a specific sender.
   - **To**—Track messages sent to a particular receiver.
   - **Contact**—Track messages for a specific contact.
   - **Request URI**—Track messages for a specific request-URI.
7. Under Threshold, specify the following options only if you have selected either **Rate Block** or **Rate Limit** in the **Action Type** field or with **None** in the **Action Type** with **Log Type** enabled. You cannot use Threshold with Permit/Drop Actions.
   - **Count (packets)**—Threshold for the number of matching packets. The value can range from 10 to 100000. The default value is 20.
   - **Period (secs)**—Threshold for the period for matching packets. The value can range from 1 to 60. The default value is 20.
   - **Timeout (secs)**—Action timeout in seconds. Specify Timeout only if you have selected the **Rate Block** action. The value can range from 30 to 36000. The default value is 900.

8. Click **Commit** to save the rule or **Cancel** to cancel the changes.

   This does not save the SIP Firewall configuration to the Session Manager. To save the configuration to the Session Manager after creating or editing the configuration, return to the SIP Firewall Configuration screen and click **Save**.

Chapter 7: Administering Session Manager routing

This chapter details the procedures that are required to set up Session Manager enterprise routing. To complete the administrative procedures, you must use the Network Routing Policy (NRP) selection from the System Manager Common Console navigation pane.

Once the initial setup is completed, administrators can use the same screens and procedures for administering and modifying the various NRP entities as well as Session Manager instances.

The primary task of Session Manager is to route session creation requests from one server to another based on the address specified in the session creation request.

The addresses which are specified to identify the ultimate destination of a session creation request are in the form of a SIP Uniform Resource Identifier (URI). It consists mainly of a user part and a domain part. Session Manager uses both parts in its routing decisions in the following manner:

- The domain part is normally a DNS domain.
- The user part is an alphanumeric string (or handle). Session Manager has special rules for efficiently routing and manipulating handles which consist entirely of digits (for example, telephone numbers).

The servers which send their session creation requests to the Session Manager are called SIP Entities. Session Manager routes these requests to other SIP Entities based on the routing rules you have administered.

Session Manager associates SIP Entities with specific locations and can make different routing decisions based upon the location from which a session creation request arrives.

Prerequisites

This chapter assumes that the following requirements are met:

- The System Manager server is installed. See System Manager Installation on page 18.
- All Session Manager instances are installed. See Session Manager installation on page 22.

Network Routing Policy

A Network Routing Policy (NRP) tells the system which SIP entity should receive a call that matches the configured dial pattern or regular expression. Administrators can use NRP to administer Session Manager instances and related routing policies. The configuration data is distributed from the NRP database to each remote Session Manager instance. For an example of how to set up network routing policy, see Appendix D: A Network Case Study on page 113.

All calls originate from a SIP entity. Routing policies describe how a call is routed when it comes from a particular location associated with the SIP entity and a distinct pattern is dialed (or a regular expression is given) during a particular time range with a distinct ranking/cost for the route to another SIP entity.

Locations are used for origination-based routing and specifying bandwidth for call admission control.

NRP and Session Manager allow administrators to define routing:

- by combining several locations
- by combining several dial patterns and SIP domains
- for several ToD and rankings
- for a single routing destination

Typically, Session Manager uses the NRP data to route a call in the following manner:

1. It tries to match the domain to one of the authoritative domains.
2. If Session Manager is authoritative for the domain, then it tries to match the digit pattern.
3. If Session Manager is not authoritative for the domain or if a digit pattern match is not found, it tries to use the regular expression table.
4. If no regular expression match is found, it sends the request to a Session Manager-provisioned outbound proxy.
5. If no outbound proxy has been administered for the Session Manager and it is not authoritative for the domain, then it uses DNS to determine where to route the request.
6. If the DNS lookup is not successful, the call fails.

Network Routing Policy initial administration

Once you have completed the initial setup as a part of ongoing administration, you can modify the created entities or delete them as required.

The recommended order for the initial set up of the Session Manager using the System Manager Network Routing Policy screens is as follows:

1. Accept or change default personal settings

2. Create SIP domains
3. Create locations
4. Create adaptations
5. Create SIP entities, some of which are routing destinations
   - create other SIP entities
   - assign locations and adaptations to the SIP entities
6. Create entity links
   - between Session Managers
   - between Session Managers and other SIP entities
7. Create time ranges
8. Create routing policies
9. Create dial patterns and assign them to routing policies and locations
10. Create regular expressions and assign them to routing policies
11. Create Session Manager instances using the **Session Manager** menus on the System Manager navigation pane.

Synchronizing configuration changes

Session Manager allows you to save the domain data to System Manager and distribute the changes to all the Session Manager instances.

To save the data to System Manager and distribute it to the Session Managers, click **Commit**.

When you click **Commit**, System Manager saves the data to the System Manager database. System Manager synchronizes and distributes the data to all the Session Manager instances. For example, renaming an adaptation also changes that data on the SIP Entity Details screen, or changing dial pattern data also changes that data in the routing policy where that dial pattern is used.

Duplicating NRP elements

You can use the **Duplicate** button on the relevant Session Manager NRP screens to duplicate NRP elements. Select the check box for the relevant element and click **Duplicate**. Duplication of data is useful if you want to create elements that are similar and want to rename them or copy an entity and make minimal changes to the entity attributes.

For example, to use a routing policy and to add a dial pattern to the copied routing policy, you can duplicate the routing policy and then add the required dial pattern to it.

Exporting NRP element data

You can export data for NRP entities to a file. After you have created or modified NRP entities, you can export the NRP element data to an XML file. You can browse to a required location to save this exported file in the XML format. You can also manually create the NRP data file or modify an existing file in the XML format.

You can export data for all NRP entities. You can save the zipped file containing all the XML files to a specified location using the **Export All Data** option.

You can export data for the following NRP entities:

- Adaptations
- Dial patterns
- Entity links
- Locations
- Regular expressions
- Routing policies
- SIP domains
- SIP entities
- Time Ranges

To export NRP element data:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > *<Any NRP element>.***
2. From the NRP Entity screen, click **More Actions > Export *<NRP Element>***

   For example, to export adaptations, from the navigation pane, you can click **Network Routing Policy > Adaptations**. From the Adaptations screen, select **More Actions > Export Adaptations**.

   To export regular expressions, from the navigation pane, you can click **Network Routing Policy** > **Regular Expressions**. From the Regular Expressions screen, click **More Actions** > **Export Regular Expressions**.
3. Select a check box for the entity to be exported from the list of entities on the screen.
4. Click **Browse** to export files to a required location and click **Export**.

   You must export a file in the XML format. This file can be manually modified.

Importing NRP element data

You can import data for NRP entities from a file. To be able to import data, after you have created or modified NRP entities, you can export the NRP element data to an XML file. You can browse to a required location to save this exported file. You can also manually create the NRP data file or modify an existing file in the XML format and then import it.

You can import data for all NRP entities using the **Import All Data** option and then selecting files from which to import data.

You can import data for the following NRP entities:

- Adaptations
- Dial patterns
- Entity links
- Locations
- Regular expressions
- Routing policies
- SIP domains
- SIP entities
- Time Ranges

To import element data:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > *<Any NRP element>.***
2. From the NRP Element screen, click **More Actions >** Import ***<NRP Element>.***

   For example, to import dial patterns, from the navigation pane, click **Network Routing Policy > Dial Patterns**. From the Dial Patterns screen, click **More Actions > Import Dial Patterns**.
3. Click **Browse** to import files from the required location and click **Import**.

   You must import a file in the XML format. This file can be an exported file, or a manually created or modified file.

Modifying the default personal settings

You can use the Personal Settings screen to change the default values or ranges for parameters that are used by the other NRP menu options

These values are used as defaults when creating new NRP elements. Modifying these values does not change the values of already created entities.

To modify the personal settings:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Personal Settings**.
2. Under **Adaptations**, specify the minimum and maximum number of characters for pattern-matching. These values are used by the NRP Adaptations option. The default minimum and maximum values are 1 and 36 respectively.
3. Under **Dial Patterns**, specify the minimum and maximum length for dial pattern. These values are used by the NRP Dial Patterns option. The default minimum and maximum values are 1 and 36 respectively.
4. Under **Entity links**, specify the port number to be used as a listen port. The default port is 5060. This port is used by the NRP Entity Links option.
5. Under **SIP Domains**, specify a domain suffix. The default suffix is avaya.com.
6. Under **SIP entities**, specify the following:
   - Select the default SIP entity type from the **Type** pull-down menu. The default type is Session Manager. You can optionally select SBC, CM, Voice Portal, Gateway, SIP Trunk, and Other.
   - Select the default time zone from the **Time Zone** pull-down menu. The default time zone is America/Denver.
   - Select the default transport protocol for ports. The default protocol is TLS. Optionally, you can select TCP or UDP.
   - With entity links from both the Session Manager instances, checking the **Override Port & Transport with DNS SRV** check box on the SIP entity form indicates that both the Port and Protocol (Transport) on the SIP entity form are ignored.
     - If you select the check box, the port and transport administered in the local host name resolution table is used, which could override the entity link.
     - If the FQDN is not in the local table and DNS is consulted, if you have not selected the check box, only an A-Record lookup is done in DNS to resolve the host name to an IP address. Transport and port specified in the entity link are used. If you selected the check box, a full DNS lookup (as described in RFC 3263) is done, and the transport and port specified in the entity link could be overridden.
7. Under **Time Ranges**, specify the default start time and end time that should be used by the NRP Time Ranges option. The default is to use a 24-hour time range, that is, the start time is 00:00 hours and the end time is 23:59 hours.
8. Under **Application Settings**, select the Show warning message check box to get a warning message if you try to navigate to another screen when a screen has unsaved data or when data import is in progress.
9. Click **Apply** to save the changes, or click **Revert** to revert to the settings before the last applied values. To revert to the original default settings, click **Restore Defaults**.

SIP domains

You can use the SIP Domains screen to create a set of SIP domains and sub-domains to enable the Session Manager to use domain-based routing. This information is used to determine if a SIP user is part of the SIP network. Domains determine if the Session Manager's dial plan can be used to route a particular call. Subdomains are automatically checked if not provisioned. For example, Session Manager needs to check dial patterns for avaya.com if a request to 123@myserver.avaya.com comes in and myserver.avaya.com is not administered as a domain.

The administrator can create a SIP domain and subdomains based on the corporate requirement.

The Domain name can be ***<domain-or-company-name>***.xyz, for example, avaya.com

The sub-domain can be named based on the geographical location or any other corporate requirements such as office location, for example, us.avaya.com and fr.avaya.com can be sub-domains for Avaya offices in the US and in France, or dr.avaya.com and br.avaya.com can be sub-domains for Avaya offices in Denver and in Basking Ridge.

Creating SIP domains

Create a SIP domain or a set of SIP domains if you plan to use domain-based routing.

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **SIP Domains**.
2. Click **New**.
3. Enter the domain name and notes for the new SIP domain or sub-domain.
4. Click **Commit**.

Modifying SIP domains

To modify a SIP domain:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > SIP Domains**
2. Select the check boxes for the domains that you want to change and click **Edit**.
3. Make changes to the domain data as required.
4. To copy existing domain data to a new domain, select the domain and click **Duplicate**. You can edit the duplicate domain name as required.
5. Click **Commit**.

Deleting SIP domains

To delete a SIP domain:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > SIP Domains**.
2. Select the check boxes for the domains that you want to delete and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

NRP Locations

You can use the NRP Locations screen to set up and configure gateway and user locations. Call processing uses locations to determine the location of the calling and the called gateways or users. The IP address of the device determines the current physical location of the caller or the called user. Session Manager matches the IP address against the patterns defined on location screens. If there is no match in the IP address patterns, Session Manager uses the SIP entity's location as the location.

Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are dial patterns administered for specific locations.

Locations are also used to limit the number of calls coming out of or going to a physical location. This is useful for those locations where the network bandwidth is limited. This is also known as Call Admission Control (CAC). You can enable CAC in Session Manager by specifying **Average bandwidth per call** and **Managed Bandwidth** on the Locations screen. If the **Managed Bandwidth** field has a non-blank value, Session Manager keeps track of the bandwidth in use based on the calls coming out of and going to that specific location and denies new calls when the bandwidth in use reaches the limit.

If the Managed Bandwidth field is blank for a location, no CAC is done for that location.

Session Manager allows you to use the following wildcard characters to specify a location:

- * (star) is used to specify any number of allowed characters at the end of the string.
- X is used to specify a digit.

The Locations screen can contain one or several IP addresses. Each SIP entity has a particular IP address. Depending on the physical and geographic location of each SIP entity, some of the SIP Entities can be grouped into a single location. For example, if there are two Communication Managers located at Denver, they can form one location named *Denver*.

Creating locations

To create locations:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Locations**
2. Click **New**.
3. Enter the location name in the **Name** field.
4. Enter notes about the location, if required.
5. Specify the managed bandwidth for the location in the **Managed Bandwidth** field.
6. Specify the average bandwidth per call for the location in the **Average Bandwidth per Call** field.
7. Specify the time to live in the **Time to Live (secs)** field.
8. To add a location pattern, click **Add** under **Location Pattern**.
9. Enter an IP address pattern to match.
10. Enter notes about the location pattern, if required.
11. Continue clicking the Location Pattern **Add** button until all the required matching location patterns have been configured.
12. Click **Commit**.

Modifying locations

To modify locations:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Locations**
2. If required, modify the managed bandwidth for the location in the **Managed Bandwidth** field.
3. If required, modify the average bandwidth per call for the location in the **Average Bandwidth per Call** field.
4. If required, modify the time to live in the **Time to Live (secs)** field.
5. To edit a location name or location matching pattern, select a check box for the required location and click **Edit** and make the required changes to the location or location pattern for that location.
6. To add or remove a location pattern, click **Add** or **Remove** under **Location Pattern**.
7. Click **Commit**.

Deleting locations

To delete locations:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Locations**
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

NRP adaptations

You can optionally use adaptations to modify SIP messages which are leaving a Session Manager instance (egress adaptation) and which are entering a Session Manager instance (ingress adaptation). This adaptation function is needed to convert strings containing calling and called party numbers from the local dial plan of a SIP entity to the dialplan administered on the Session Manager, and vice-versa. Adaptation is also used when other SIP Entities require special SIP protocol conventions. Each administered SIP entity may have its own unique adaptation, or one adaptation can be shared among multiple entities.

Adaptations are implemented as software modules that can be created and are used to fit the needs of the system.

Session Manager is installed with a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as host names in the Request-URI and other headers. It also contains adaptation modules which perform protocol conversions on systems such as for AT&T, Verizon, Cisco, and Nortel, as well as the digit conversion. All of these adapters allow for modification of URIs specified using unique name-value pairs for egress adaptation. For example, these adapters can replace the hostname in the Request-URI with an administered hostname during egress adaptation. For details, see Creating NRP adaptations on page 62.

In an adaptation administered using NRP, you can specify the module to use as well as the digit conversion which is to be performed on headers in the SIP messages. You can specify different digit conversions for ingress and egress adaptation.

Additionally, digit conversion can be specified to modify only “origination” type headers, only “destination” type headers, or both.

The origination/source type URIs are:

- P-Asserted-Identity
- History-Info (calling portion)
- Contact (in 3xx response)

The destination type URIs are:

- Request-URI
- Message Account (in NOTIFY/message-summary body)
- Refer-To (in REFER message)

Adaptation example

In the following example, an adaptation for AT&T service provider is needed at least for international calls.

For incoming calls, AT&T sends the 10 digit local number. To convert this into E.164, Session Manager must add a plus sign. Specify the following values:

- Matching pattern: 1
- Min: 10
- Max: 10
- Delete Digits: 0
- Insert Digits: +
- Address to modify: both

For outgoing calls to AT&T, Session Manager must convert the E.164 form to a format that AT&T supports, either 1+10 digits for North America calls, or 011+country code + number for international calls. For example, for calls to North America, specify the following values:

- Matching Pattern: +1
- Min: 12
- Max: 12
- Delete Digits: 1
- Insert Digits: <None>
- Notes: Calls to North America

For calls to Germany, specify the following values:

- Matching Pattern: +49
- Min: 13
- Max: 13
- Delete Digits: 1
- Insert Digits: 011
- Address to modify: destination
- Notes: Calls to Germany

Adaptation Module administration

The following is information regarding the **Adaptation Module** field on the Adaptation Details screen. The format of the **Adaptation Module** field is:

<Name of adaptation module> <name1=value1> <name2=value2>,...

There are currently 4 names defined which can be administered using either the full name or shortcut name:

EGRESS Domain Modification Parameters

- `overrideDestinationDomain (`or abbreviated name `odstd)`: {parameter #1 if not named}, replaces the domain in Request-URI and Notify/message-summary body with the given value for **egress** only.
- `overrideSourceDomain (`or abbreviated name `osrcd)`: replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for **egress** only.

INGRESS Domain Modification Parameters:

- `ingressOverrideDestinationDomain (`or abbreviated name i`odstd)`: replaces the domain in Request-URI and Notify/message-summary body with the given value for **ingress** only.
- `ingressOverrideSourceDomain (`or abbreviated name i`osrcd)`: replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for **ingress** only.

Example:

```
CiscoAdapter osrcd=dr.avaya.com odstd=ny.avaya.com
```

The same value in verbose form:

```
CiscoAdapter overrideSourceDomain=dr.avaya.com
overridenDestinationDomain=ny.avaya.com
```

Creating NRP adaptations

To create NRP adaptations:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Adaptations**
2. Click **New**. The system displays the Adaptation Details screen.

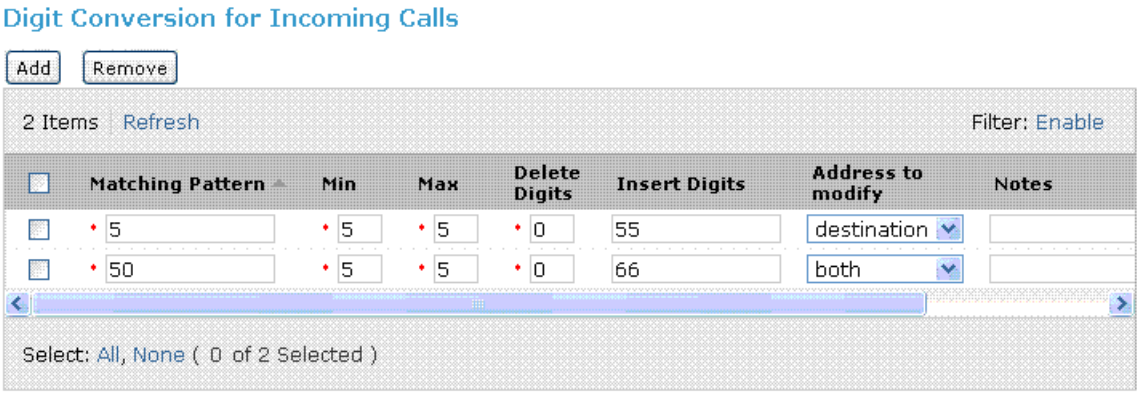
   All adaptation modules have the ability to replace the domain (also known as hostname) portion of the URI with a specified value for source and destination type URIs on outgoing calls (egress) and to append parameters to the Request URI for outgoing calls (egress).

This adaptation functionality is expandable to adapt additional deployments needing further flexibility.

3. Enter the **Name**, **Adaptation Module** and any other required fields in the first section.
   - Enter a descriptive name for the adaptation.
   - Specify an adaptation module. This module is the adaptation module to use and host name adaptations to perform. See Adaptation Module administration.
   - Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.

     URI parameters can be added to the Request-URI. For example, the parameter “user=phone” can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the **Egress URI Parameters** field.

     The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A leading ';' is optional. Entry “;user=phone;custApp=1” is equivalent to “user=phone;custApp=1”.
   - Enter description about the adaptation module in the **Notes** field.
4. Click **Add** under **Digit Conversion for Incoming Calls** if you need to configure ingress digit conversion. Ingress adaptation administers digit manipulation for calls coming into the Session Manager instance.



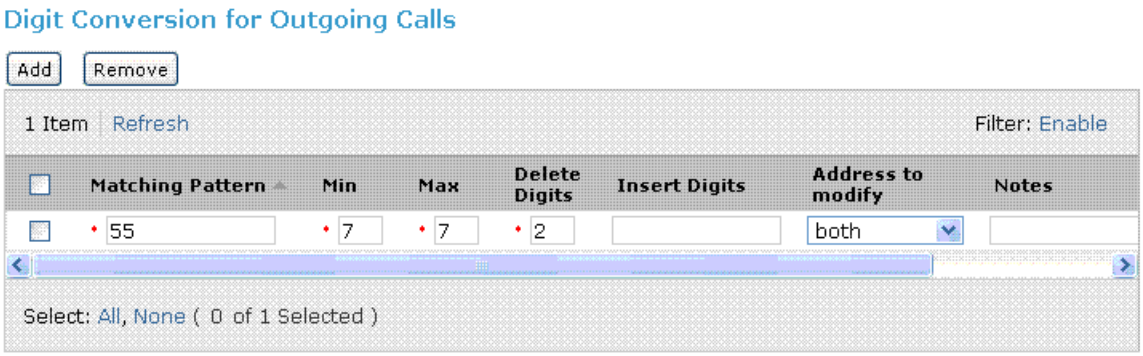
5. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters.

   Mouse over the input field to view a tool tip describing valid input.

6. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

   The minimum value can be 1 or more. The maximum value can be 36.

7. Enter the number of digits that you want deleted of the dialed number in the **Delete Digits** field.
8. Enter the digits that you want inserted before the number in the **Insert Digits** field.
9. From the drop-down list, select the value for **Address to modify**. A setting of **both** looks for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination always take priority over entries that match a pattern of both.
10. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
11. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
12. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.



13. Enter the matching pattern and other required fields. The Matching Pattern field can have 1 to 36 characters.

    Mouse over the input field to view a tool tip describing valid input.

14. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

    The minimum value can be 1 or more. The maximum value can be 36.

15. Enter the number of digits that you want deleted from the left of the dialed number in the **Delete Digits** field.
16. Enter the digits that you want inserted before the number in the **Insert Digits** field.
17. From the drop-down list, select the value for **Address to modify**. A setting of **both** looks for adaptations on both origination and destination type headers. Entries that match a pattern

of type origination or destination always take priority over entries that match a pattern of both.

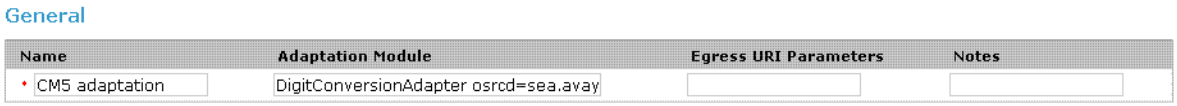
18. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
19. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
20. Click **Cancel** or **Commit**.

Modifying NRP adaptations

To modify NRP adaptations:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Adaptations**
2. Select the adaptation for modification and click **Edit**.

   All adaptation modules have the ability to replace domain (also known as host name) portion of the URI with a specified value for source and destination type URIs on outgoing calls (egress) and to append parameters to the Request URI on for outgoing calls (egress). This adaptation functionality is expandable to adapt additional deployments needing further flexibility.



3. Enter the **Name**, **Adaptation Module** and any other required fields in the first section.
   a. Enter a descriptive name for the adaptation.
   b. Specify an adaptation module. This module is the adaptation module to use and host name adaptations to perform.
   c. Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.
4. Click **Add** under **Digit Conversion for Incoming Calls** if you need to configure ingress digit conversion. Ingress adaptation administers digit manipulation for calls coming into the Session Manager instance.
5. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters.

   Mouse over the input field to view a tool tip describing valid input.

6. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

   The minimum value can be 1 or more. The maximum value can be 36.

7. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
8. Enter the digits that you want inserted before the number in the **Insert Digits** field.
9. From the drop-down list, select the value for **Address to modify**. A setting of **both** looks for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination always take priority over entries that match a pattern of both.
10. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
11. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
12. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
13. Enter the matching pattern and other required fields. The Matching Pattern field can have 1 to 36 characters.

    Mouse over the input field to view a tool tip describing valid input.

14. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

    The minimum value can be 1 or more. The maximum value can be 36.

15. Enter the number of digits that you want deleted from the left of the dialed number in the **Delete Digits** field.
16. Enter the digits that you want inserted before the number in the **Insert Digits** field.
17. From the drop-down list, select the value for **Address to modify**. A setting of **both** looks for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination always take priority over entries that match a pattern of both.
18. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
19. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
20. Click **Cancel** or **Commit**.

Deleting NRP adaptations

To delete NRP adaptations:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Adaptations**.
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

Installed vendor adapters

The following sections describe how the various vendor adapters work with Session Manager.

Cisco Adapter (CiscoAdapter)

The Cisco Adapter provides two basic header manipulations: converting between Diversion and History-Info headers and converting between P-Asserted-Id and Remote-Party-Id headers. The Diversion and Remote-Party-Id headers have not been accepted by the IETF. They are replaced by History-Info and P-Asserted-Identity respectively, but are still used in the Cisco products. The Cisco Adapter also performs all the conversions available by the Digit Conversion Adapter.

Case 1: Cisco requires the use of the Diversion header, rather than the History-Info header to provide information related to how and why the call arrives to a specific application or user. The following examples illustrate the adaptations:

Example 1:

Communication Manager user 66600001 forwards to Cisco user 60025.

Communication Manager's outgoing INVITE has this history-info:

```
History-Info: "<sip:66600001@ny.avaya.com>;index=1
History-Info: "stn 66600001"
<sip:66600001@ny.avaya.com?Reason=SIP%3Bcause%3D302%3Btext%3D%22Moved%
20Temporarily%22&Reason=Redirection%3Bcause%3DCFI>;index=1.1
History-Info: <sip:600025@ny.avaya.com>;index=1.2
```

In the message sent to Cisco this is converted to:

```
Diversion: "stn 66600001" <sip:66600001@ny.avaya.com>;reason=no-
answer;privacy=off;screen=no
```

Example 2:

Communication Manager user calls Cisco user 60025. The call is routed to Message Manager at extension 688810.

The INVITE message from the Cisco server contains the Diversion Header:

```
Diversion: "Ken's Desk" <sip:600025@ny.avaya.com>;reason=user-
     busy;privacy=off;screen=no
```

The message is adapted and the outgoing INVITE to MM replaces the Diversion header with the following:

```
History-Info: <sip:600025@ny.avaya.com>;index=1
History-Info: "Ken's Desk"
<sip:600025@ny.avaya.com?Reason=SIP%3Bcause%3D486%3Btext%3D%22Bus
y%20Here%22&Reason=Redirection%3Bcause%3DNORMAL%3Bavaya-cm-reason%3D%2
2cover-busy%22%3Bavaya-cm-vm-address-digits%3D81080000%3Bavaya-cm-vm-a
ddress-handle%3Dsip:80000%40avaya.com>;index=1.1
History-Info: "MM" <sip:688810@ny.avaya.com>;index=1.2
```

Case 2: Cisco requires information in the P-Asserted-Identity (PAI) header to be received in the Remote-Party-Id (RPI) header. Any incoming message containing a P-Asserted-Identity header being routed to Cisco will replace that header with the Remote-Party-Id header. Similarly, calls from Cisco containing the Remote-Party-Id header will be converted to a P-Asserted-Identity header when routed to non-Cisco entities.

Example 3:

A call is placed from 12345 at Communication Manager and routed to the Cisco PBX.

The INVITE from Communication Manager contains:

```
P-Asserted-Identity: "Ryan" <sip:12345@avaya.com>
```

This header is converted to RPI when the request is sent to the Cisco PBX:

```
Remote-Party-Id: "Ryan"
<sip:12345@avaya.com>;party=called;screen=no;privacy=off
```

Example 4:

A call is placed from 23456 at Cisco PBX and routed to Communication Manager.

The INVITE from Cisco PBX contains:

```
Remote-Party-Id: "Ryan"
<sip:23456@avaya.com>;party=called;screen=no;privacy=off
```

This header is converted to PAI when the request is sent to CM:

```
P-Asserted-Identity: "Ryan" <sip:23456@avaya.com>
```

Verizon Adapter (VerizonAdapter)

The Verizon adapter requires the same History-Info to Diversion adaptations that the Cisco Adapter uses. The Verizon Adapter also performs all the conversions available by the Digit Conversion Adapter.

AT&T Adapter (AttAdapter)

AT&T does not handle the History-Info header. The adaptation module removes, on egress to AT&T, any History-Info headers in a request or response. Messages from AT&T do not change. The AT&T Adapter also performs all the conversions available by the Digit Conversion Adapter.

SIP entities

SIP Entities are all the network elements that are a part of the SIP System. SIP Entities include Session Manager instances, Communication Managers, Session Border Controllers (SBCs), SIP trunks, and so on.

Authentication of trusted SIP entities

Network Routing Policy (NRP) uses the following information for the authentication of SIP entities by performing validation on IP/Transport Layer and TLS Layer:

- FQDN or IP Address of the SIP entity
- Credential name of the SIP entity
- Protocol of the Entity Links. This is a SIP connection transport type (TCP/TLS/UDP)
- Trust State of the Entity Link (This defines whether the entity link is Trusted or not)

For information about administering these fields, see Creating NRP SIP entities on page 71.

IP and transport layer validation

When a SIP entity connects to Session Manager over a TCP or TLS port, Session Manager validates that:

- The IP address matches one of the SIP Entities configured in NRP that have trusted entity links with the Session Manager. If the SIP entities are configured as FQDN, Session Manager performs a DNS resolution before doing the verification.
- Transport for the incoming SIP connection matches with one of the entity links associated with this SIP entity and the Session Manager. Also, the **Trust State** of the entity link must

be configured as trusted. Session Manager does not accept connections matching untrusted entity links.

For SIP packets over UDP, above validation is performed for each packet. For SIP TLS connections, further validation is performed as described in the next section.

TLS layer validation

Session Manager applies the following additional validations for SIP TLS connections:

1. During a TLS handshake, mutual TLS authentication is performed, that is, Identity certificate of the SIP entity is validated against the trusted CA certificate repository in the Session Manager for SIP TLS. If this verification fails, Session Manager does not accept the connection.
2. If the mutual TLS authentication is successful, further validation is performed on the SIP entity Identity Certificate as per the Credential Name or the far-end IP address.
   - If the Credential Name string is empty, the connection is accepted.
   - If the Credential Name string is not empty, the Credential Name and the IP address of the far-end is searched for in the following fields in the identity certificate provided by the SIP entity:
     - CN value from the subject
     - subjectAltName.dNSName
     - subjectAltName.uniformResourceIdentifier (For IP address comparison, IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. Also, case insensitive search is performed in this case)

With entity links from both Session Manager instances, checking the **Override Port & Transport with DNS SRV** check box on the SIP entity form indicates that both the Port and Protocol (Transport) on the SIP entity form are ignored.

- If you select the check box, the port and transport administered in the local host name resolution table is used, which could override the entity link.
- If the FQDN is not in the local table and DNS is consulted, if you have not selected the check box, only an A-Record lookup is done in DNS to resolve the host name to an IP address. Transport and port specified in the entity link are used. If you selected the check box, a full DNS lookup (as described in RFC 3263) is done, and the transport and port specified in the entity link could be overridden.

Creating NRP SIP entities

Use the NRP SIP Entities screen to create SIP entities. To administer minimal routing via Session Manager, you need to configure a SIP entity of type CM and a second SIP entity of type Session Manager.

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **SIP Entities**
2. Click **New**.
3. Enter the Name, FQDN (fully Qualified Domain Name) or IP address of the SIP entity, Type (Session Manager, CM, and so on) and any other required fields in the first section.
4. To specify an **Adaptation Module** for the SIP entity, click the drop-down selector for the **Adaptation** field.
5. If you need to specify the location for the SIP entity, click the drop-down selector for the **Location** field.
6. If the SIP entity **Type** is “Session Manager” and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** field.
7. Select the correct time zone from the Time Zone drop-down list.
8. Enter a value in seconds in the **SIP Timer B/F (secs)** field. This value must be between 1 and 32 seconds. The default is 4. This is the time Session Manager should await a response from a SIP entity before trying an alternate route.
9. Enter a regular expression string in the Credential name. The Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate. For more information, see Viewing trusted certificates on page 39.
   - If you do not want to perform the additional validation on the SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
   - If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
   - If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax. Please note that IP Address is searched by default when any string is configured in the Credential Name.

Note:

The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some examples:

For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”.

For “192.14.11.22”, use string “192\.14\.11\.22”.

You can look for a subset of the string or can create a wild card search. For example, to look for “domain.com” as a substring, use the string “domain\.com”

10. Under SIP Link Monitoring, the following options are available from the drop-down menu:
    - **Use Session Manager Configuration** – Use the settings under **Session Manager > Session Manager Administration**
    - **Link Monitoring Enabled** – Enables link monitoring on this SIP entity.
    - **Link Monitoring Disabled** – Link monitoring will be turn off for this SIP entity.
11. If you need to specify the Port parameters, click **Add** under Port. This information is used when Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager. It associates one of the administered domains with the port on which the request was received.
12. Enter the necessary Port and transport Protocol parameters.
13. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
14. Click **Cancel** or **Commit**.

Modifying SIP entities

To modify SIP entities:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > SIP Entities**
2. Select the SIP entity for modification and click **Edit**.
3. Modify the **Name**, **FQDN** (fully Qualified Domain Name) or IP address of the SIP entity, Type (Session Manager, CM, and so on) and any other required fields in the first section.
4. To specify or modify an **Adaptation Module** for the SIP entity, click the drop-down selector for the **Adaptation** field.
5. If you need to specify or modify the location for the SIP entity, click the drop-down selector for the **Location** field.
6. If the SIP entity Type is “Session Manager” and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** field.
7. Select the correct time zone from the **Time Zone** drop-down list.

8. Enter or modify a value in seconds in the **SIP Timer B/F (secs)** field. This value must be between 1 and 32 seconds. The default is 4. This is the time Session Manager should await a response from a SIP entity before trying an alternate route.
9. Enter or modify a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate. For more information, see Viewing identity certificates on page 40.
   - If you do not want to perform the additional validation on SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
   - If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
   - If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax. Please note that the system looks for the IP Address by default when any string is configured in the Credential Name.

   Note:
   The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some of the examples:

   - For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”.
   - For “192.14.11.22”, use string “192\.14\.11\.22”.
   - You can search a subset of the string or can create a wild card search. For example, for searching for “domain.com” as a substring, use the string “*domain\.com*”
10. Under SIP Link Monitoring, the following options are available from the drop-down menu:
    - **Use Session Manager Configuration**
    - **Link Monitoring Enabled** – Enables link monitoring on this SIP entity.
    - **Link Monitoring Disabled** – Link monitoring will be turn off for this SIP entity.
11. If you need to specify the Port parameters, click **Add** under Port. This information is used when Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager. It associates one of the administered domains with the port on which the request was received.
12. Enter the necessary Port and transport Protocol parameters.
13. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
14. Click **Cancel** or **Commit**.

SIP entity references

Session Manager enables you to see all references to a SIP entity such as its location, the routing policy that is created for the SIP entity, and adaptations, if any. If a single SIP entity has more than one combination of these references, Session Manager displays each of the combinations on a separate row.

Displaying SIP entity references

To display SIP entity references:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > SIP Entities**.
2. Select the check box for a SIP entity whose references you want to see.
3. From the **More Actions** drop-down list, select **Display SIP Entity References**.

   Session Manager displays the overview of SIP entity references such as the entity location, name of the routing policy attached to the entity, and adaptations, if any.
4. Click **Back** to navigate to the SIP entities.

Deleting SIP entities

To delete a SIP entity:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > SIP Entities**
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

NRP entity links

Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity. You must configure an entity link between a Session Manager and any entity that you have administered if you want Session Manager to be able to send or receive messages from that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network. Session Manager does not need to know the port and

transport protocol if the **Override Port & Transport** box is checked on the SIP entity. Port and transport must be administered ***even if*** the **Override Port & Transport** box is checked on the SIP entity, although their values will not be used.

NRP entity links connect two SIP entities through the Session Manager. They enable you to define the network topology for SIP routing.

- Entity Links are configured to connect two SIP Entities.
- Trusted Hosts are indicated by assigning the **Trust State** to the link that connects the entities.

Creating NRP entity links

Use the Entity Links screen for this task. The general configuration of connections between SIP entities enables NRP and Session Manager to identify specific connection configurations (for example, Trusted Hosts, outbound proxy, and so on) between SIP Entities.

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Entity Links**
2. Click **New**.
3. Enter 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 port is the port on the Session Manager to which the remote entity needs to send requests to. Default ports in SIP are 5060 for TCP and UDP and 5061 for TLS. You can specify a port other than these default ports.
5. Enter the SIP entity 2 by selecting the required 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. If the SIP entity is trusted, select the **Trusted** check box. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
7. Select the transport protocol you require for the link using the **Protocol** drop-down list.
8. Click **Cancel** or **Commit**.

Modifying NRP entity links

To modify NRP entity links:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Entity Links**
2. Select an entity link for modification and click **Edit**.
3. Modify the name in the **Name** field if required.
4. If required, modify 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.
5. If required, modify the SIP entity 2 by selecting the required SIP entity from the drop-down list and provide the required port.
6. If you want to indicate that the link is a trusted link, select the **Trusted** check box.
7. Select the transport protocol you require for the link using the **Protocol** drop-down list.
8. Click **Cancel** or **Commit**.

Deleting NRP entity links

To delete an NRP entity link:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Entity Links**
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

NRP time ranges

Time ranges indicate when a particular rank or cost of a routing policy is to be used when determining the least-cost route. They do not indicate when routing policies are available to be considered for routing.

You must specify as many time ranges as necessary to cover all hours and days in a week for each administered routing policy.

For example, routing policy A can be in effect on all weekdays from 9:00 a.m. to 5:59 p.m., routing policy B can be in effect on all weekdays from 6:00 pm. to 9 a.m., and routing policy C

can be in effect on weekends. These three time ranges together cover how calls should be routed throughout the week.

Creating NRP time ranges

The NRP Time Ranges screen is used to administer time ranges with start and end times.

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Time Ranges**.
2. Click **New**.
3. Enter the name, then select the required days by entering the start and end times and notes for the new time range. Start times begin with the first second of the hour:minute. End Times go through the last second of the end hour:minute.
4. Click **Cancel** or **Commit**.

Modifying NRP time ranges

To modify NRP time ranges:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Time Ranges**
2. Select a time range for modification and click **Edit**.
3. If required, modify the name.
4. If required, modify the days by modifying the start and end times and notes. Start times begin with the first second of the hour:minute. End Times go through the last second of the end hour:minute.
5. Click **Cancel** or **Commit**.

Deleting NRP time ranges

To delete NRP time ranges:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Time Ranges**
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

NRP routing policies

Use the Routing Policies screen to create and modify routing policies.

- All routing policies together form the “enterprise-wide dial plan”.
- Routing policies can include the “Origination of the caller”, the “dialed digits” of the called party, the “SIP domain” of the called party and the actual time the call occurs.
- Optionally, instead of “dialed digits” of the called party and the “SIP domain” of the called party, a “regular expression” can be defined.
- Depending on one or multiple of the inputs mentioned above, a destination where the call should be routed is determined.
- Optionally, the destination can be qualified by “deny” which means that the call will not be routed.
- Session Manager uses the data configured in the routing policy to find the best match against the number (or address) of the called party.

Creating NRP routing policies

To create an NRP routing policy:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Routing Policies**
2. Click **New**.
3. Enter a policy name and notes in the relevant fields in the General section.
4. To disable the routing policy, select the **Disabled** check box.
5. Click **Select** under the SIP Entity as Destination section. This is where you can select the destination SIP entity for this routing policy.
6. Select the required destination and click **Select**.
7. If you need to associate the Time of Day routing parameters with this routing policy, click **Add** from the Time of Day section.
8. Select the Time of Day patterns that you want to associate with this routing pattern and press **Select**.

   If there are gaps in the Time of Day coverage that you select, Session Manager displays a warning message. If such gaps exist in the Time of Day coverage, randomness in routing selections may be observed.
9. Enter the relative rankings that you would like associated with each Time Range. Lower ranking values indicate higher priority.

10. Under **Dial Patterns** or **Regular Expressions**, click **Add** to associate existing dial patterns and regular expressions with the routing policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**. This field can be left blank; the routing policy can be added to the dial pattern or regular expression when you add it.
11. Under **Dial Patterns** or **Regular Expressions**, click **Remove** to dissociate existing dial patterns and regular expressions with the routing policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**. This field can be left blank.
12. Click **Commit** or **Cancel**.

Modifying NRP routing policies

To modify an NRP routing policy:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Routing Policies**
2. Select a routing policy for modification and click **Edit**.
3. If required, modify the policy name and notes in the relevant fields in the General section. Note that the routing policy can be disabled by selecting the **Disabled** check box.
4. Click **Select** under the SIP Entity as Destination section. This is where you can select the destination SIP entity for this routing policy.
5. If required, select or modify the required destination and click **Select**.
6. If you need to associate the Time of Day routing parameters with this routing policy, click **Add** from the Time of Day section.
7. Select the Time of Day patterns that you want to associate with this routing pattern and press **Select**.
8. Enter the relative rankings that you would like associated with each Time Range. Lower ranking values indicate higher priority.
9. If you need to dissociate the Time of Day routing parameters from this routing policy, click **Remove** from the Time of Day section.
10. Under **Dial Patterns** or **Regular Expressions**, click **Add** to associate existing dial patterns and regular expressions with the routing policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.
11. Under **Dial Patterns** or **Regular Expressions**, click **Remove** to dissociate existing dial patterns and regular expressions with the routing policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.
12. Click **Commit** or **Cancel**.

Deleting NRP routing policies

To delete an NRP routing policy:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Routing Policies**
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

Note:
If you delete a routing policy, all dial patterns and regular expressions that are linked *only* to this routing policy are also deleted.

Dial patterns

A dial pattern specifies which routing policy or 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 you apply any administered ingress adaptation.

The originating location of the call and the domain in the request-URI also decide how the call gets routed.

Session Manager tries to match the request-URI of a request to a row in the dial pattern table. The rows considered for the match are all rows where:

- The domain in the dial pattern table matches the domain in the request-URI, and,
- The originating location in the dial pattern table row matches the originating location of the request, or, if there are no rows matching the originating location, the originating location in the table is set to -ALL-, or, if there was no originating location, the originating location in the table is -ALL-, and
- The digit pattern in the row matches the user-part of the request-URI, ignoring any parameters that are in the user part of the request-URI

If no rows match using the above criteria, Session Manager modifies the domain in the request URI to remove one level of subdomain. For example, if *us.yourcompany.com* was tried, then Session Manager tries *yourcompany.com*.

As another example, you have two Communication Manager instances. Each Communication Manager has a call number range including all direct inward dialing (DID) numbers. Any user on CM-1 has a dial pattern +1301501xxxx. Similarly, any user on CM-2 has a dial pattern +1301601xxxx. You would enter the 2 dial patterns as:

- CM-1: +1301501
- CM-2: +1301601

A call to +13015016789 would match the dial pattern for CM-1.

A call to +13016011234 would match the dial pattern for CM-2.

The pattern matching algorithm works as follows:

- Valid digits are 0-9
- Valid characters for the leading position are,+, *, and #. Any other characters are not matched.
- x (lowercase only) is a wildcard character that matches a character from the allowed characters above. White spaces are not allowed.
- Longer matches get a higher priority over shorter matches. For example, +1601555 has a higher priority as compared to +1601.
- For matches of equal length, exact matches have a higher priority over wildcard matches. For example, +1601555 has a higher priority as compared to +1xxx555.
- For both routing policies and adaptations, the pattern matching works in the same manner.

Creating dial patterns

The NRP Dial Patterns screen creates dial patterns and associates the dial patterns to a routing policy and locations.

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Dial Patterns**
2. Click **New**.
3. Enter the general dial pattern information in the **General** section. Note that you can provide a SIP domain so as to restrict the dial Pattern to the specified SIP domain.
4. Click **Add** under the **Originating Locations and Routing Policies** section.
5. Select all the required locations and routing policies that you want associated with the dial pattern by selecting the check box in front of each item.
6. Click **Select** to indicate that you have completed your selections.
7. If you need to specify that calls from the specified locations will be denied, click **Add** under the **Denied Locations** section.
8. Select all the locations that are to be denied and click **Select** to indicate that you have completed your selections.
9. Click **Commit** or **Cancel.**

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

Modifying dial patterns

To modify a dial pattern:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Dial Patterns**
2. Select a dial pattern for modification and click **Edit**.
3. Enter the general dial pattern information in the **General** section. Note that you can provide a SIP domain to restrict the dial pattern to the specified SIP domain.
4. Click **Add** under the **Originating Locations and Routing Policies** section.
5. Select all the required locations and routing policies that you want associated with the dial pattern by selecting the check box in front of each item.
6. Click **Select** to indicate that you have completed your selections.
7. Similarly, to remove locations, click **Remove**, select the locations to remove, and click **Select**.
8. If you need to specify that calls from the specified locations will be denied, click **Add** under the **Denied Locations** section.
9. Select all the locations that are to be denied and click **Select** to indicate that you have completed your selections.
10. Similarly, to remove locations from the denied list, click **Remove**, select the locations to remove, and click **Select**.
11. Click **Commit** or **Cancel**.

Note:
You cannot save a dial pattern unless it has at least one routing policy or a denied location associated to it.

Deleting dial patterns

Deleting a dial pattern removes it from all of the routing policies that the dial pattern is associated with.

To delete a dial pattern:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Dial Pattern**s
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

Regular expressions

You can configure routing in Session Manager by creating regular expressions and associating them with a routing policy.

Regular expression syntax is based on Perl version 5.8.

The asterisk character "*" matches any character string.

The dot character "." matches one character.

The backslash character "\ " makes a character lose its special meaning, if any

Some examples are:

- For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”
- For “192.14.11.22”, use string “192\.14\.11\.22”.
- The routing policy with a regular expression **.*@.*\.de** routes all calls requesting a SIP domain in Germany (for example, name@company.de) to a Frankfurt Gateway.

Creating regular expressions

The NRP Regular Expressions screen is used to create regular expressions and associate them with the routing policies. You cannot save a regular expression unless it has a routing policy associated to it.

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Regular Expressions**
2. Click **New**.
3. Enter the regular expression pattern in the **Pattern** field.
4. Specify a rank order for the regular expression. A lower rank order indicates a higher priority.
5. To deny routing for a matched regular expression pattern, select the **Deny** check box.
6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
7. Select the required routing policies that you want associated with the regular expression by selecting the respective check boxes.
8. Click **Select** to indicate that you have completed your selections.
9. To remove an associated routing policy, select the policy and click **Remove**.
10. Click **Commit** or **Cancel**.

Modifying regular expressions

To modify a regular expression:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Regular Expressions**
2. Select the regular expression for modification and click **Edit**.
3. Modify the regular expression pattern as required in the **Pattern** field.
4. If required, modify the rank order for the regular expression. A lower rank order indicates a higher priority.
5. To allow or deny routing for a matched regular expression pattern, clear or select the **Deny** check box.
6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
7. Select the required routing policies that you want associated with the regular expression by selecting the respective check boxes.
8. Click **Select** to indicate that you have completed your selections.
9. To remove an associated routing policy, select the policy and click **Remove**.
10. Click **Commit** or **Cancel**.

Note:
You cannot save a regular expression unless it has at least one routing policy associated with it.

Deleting regular expressions

Deleting a regular expression deletes it from all of the routing policies that it is associated with.

To delete a regular expression:

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy > Regular Expressions**
2. Select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation screen.

Chapter 8: Configuring and Monitoring Session Manager Instances

This chapter describes the procedures to:

- configure and monitor Session Manager instances
- add, edit, or remove local host name entries (overriding DNS information)
- configure the trace properties for one or more security modules
- manage call bandwidth usage

Prerequisites

Before you start configuring the Session Manager instances, ensure that the following requirements are met:

- All Session Manager instances are installed on servers that are connected to the same LAN to which the System Manager server is linked.
- All Session Manager instances are configured as SIP entities using the Session Manager Network Routing Policy (NRP) screen. You can add only the SIP entities that you have administered as Session Manager instances.

Accessing Session Manager

From the System Manager Common Console navigation pane, click **Session Manager**. The navigation pane expands to display the following screen options.

- Session Manager Administration
- System State Administration
- Security Module Status
- Data Replication Status
- Local Host Name Resolution
- Maintenance Tests
- SIP Firewall Configuration

- SIP Monitoring
- Tracer Configuration
- Trace Viewer
- Call Routing Test
- Managed Bandwidth Usage

The system displays the Session Manager Administration screen as the default on the content pane. For the menu descriptions not included in this guide, refer to *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (03-603325).

Session Manager administration

Select the Session Manager Administration menu option to add a SIP entity as a Session Manager instance. Once added, these Session Manager instances form a link with the Session Manager Element Manager and can be used for obtaining and monitoring the status of that Session Manager instance.

Data replication and monitoring operations are possible only after these Session Manager instances are added and configured.

In addition to creating new Session Manager instances, the Session Manager Administration screen also allows you to view, edit, or delete the Session Manager instances that you have created.

Adding a SIP entity as a Session Manager instance

Before starting this procedure, make sure that the SIP entity that you want to add was created and is in a synchronized state. See Creating NRP SIP entities on page 71 to create the SIP entity.

1. From the navigation pane on the System Manager Common Console, click **Session Manager > Session Manager Administration**
2. Click **New** on the Session Manager Administration screen. The system displays the **Add Session Manager** screen.
3. Under the **General** section, enter the following information:
   - Select the **SIP Entity Name** from the drop-down list.
   - In the **Description** field for this entity, add a comment if required.

- In the **Management Access Point Host Name/IP** field, add the IP address of the host on which the management agent is running; that is, the host on which the Session Manager is installed.

Note:

To be a part of the Session Manager instances network of an enterprise, a Session Manager instance must first be administered as a management access point. This is the network mask of the domain name of the server that hosts the Session Manager application. The address is passed to the SM100 agent to allow the agent to query the server for the required information.

4. Under the **Security Module** section, enter the following information to configure the security module:
   - In the **Network Mask** field, enter the value for the network mask. The network mask is passed to the SM100 agent. The agent configures the network mask to define the subnet that the SM100 card is to be associated with.
   - In the **Default Gateway** field, add the correct IP address.
   - In the **Call Control PHB** field, enter a value.

     The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 that you may expect as it travels through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence—they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.
   - The **Speed & Duplex** field allows the configuring of the security module interface speed and duplex values. The drop-down menu contains a list of the valid values.
   - In the **QOS Priority** field, enter a 802.1q priority value.

     This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.
   - In the **VLAN ID** field, enter an integer value. This is the VLAN that the Session Manager is to be associated with. Call traffic segregation could be based on the VLAN associated with the Session Manager.
5. Under the **Monitoring** section, enter the following information to configure how this Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Session Manage instance, select or clear the **Enable Monitoring** check box.

- Type a required value in seconds for **Proactive cycle time (secs)**. The default is 900 seconds. Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
- Type a required value in seconds for **Reactive cycle time (secs)**. The default is 120 seconds.

  This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds.

  Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities screen for a specific entity.
- Type an integer value in **Number of Retries**. The default is 1. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default is 1.

6. Under the **CDR** section, enter the following information:
   - Select the **Enable CDR** check box to enable Call Detail Recording. This controls whether CDR is enabled at the system level for that Session Manager instance. If CDR is enabled, you can individually control call detail recording for specific SIP entities using the Call Detail Recording drop-down menu.
   - Type a password that must be used to access the CDR record and retype to confirm the password. This password is used by an external CDR processing adjunct for connecting to Session Manager and to transfer the generated CDR files. Normally the adjunct logs in as "CDR_User" user ID, with a default password. The password that you specify here becomes the default password. Once the CDR adjunct logs in using "sftp", it is automatically placed in the Session Manager CDR home directory of the CDR_User, which is **/var/home/ftp/CDR**.
7. Click **Return** to return to the previous screen.

Viewing the Session Manager administration settings

To view Session Manager administration settings:

1. From the navigation pane on the System Manager Common Console, click **Session Manager > Session Manager Administration**
2. Select a Session Manager from the Session Manager Instances list and click **View**. The system displays the **View Session Manager** screen. This screen displays information about:
   - SIP entity name (Session Manager instance)
   - Description

- Name of the MAP host where the Session Manager instance is installed
- The network mask; default gateway; and call control PHB, QOS priority, and VLAN ID values for the Security module
- Whether monitoring is enabled or not, and, if so, the proactive and reactive cycle times (in seconds), and the number of retries.
- Whether CDR is enabled or not.

3. After you have viewed the information, click **Return**.

Modifying the Session Manager administration settings

This option allows you to modify the configuration settings for an already configured Session Manager.

1. From the navigation pane on the System Manager Common Console, click **Session Manager > Session Manager Administration**
2. Click **Edit** on the Session Manager Administration screen.
3. Under the **General** section, change the following information, if required:
   - Add a comment in the **Description** field for the Session Manager SIP entity.
   - Change the IP address of the host on which the Session Manager is installed in the **Management Access Point Host Name/IP** field. This is the IP address of the domain name of the server that hosts the Session Manager application. Session Manager passes the address to the SM100 agent to allow the agent to query the server for the required information. To be a part of the Session Manager instances network of an enterprise, a Session Manager instance must first be administered as a management access point.
4. Under the **Security Module** section, change the following information, if required
   - Modify the network mask in the **Network Mask** field. Session Manager passes this network mask to the SM100 agent. The agent configures the network mask to define the subnet that the SM100 card is to be associated with.
   - Modify the IP address in the **Default Gateway** field.
   - Modify the value for **Call Control PHB**. The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 that you may expect as it travels through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a

different level of precedence--they must either support this by default or be specially configured to do so.

Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.

- Modify the **QOS Priority** value. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.
- Modify the value for **VLAN ID**. This is the VLAN that the Session Manager is to be associated with. Call traffic segregation could be based on the VLAN that the Session Manager is associated with.

5. Under the **Monitoring** section, modify the following information as required to configure how this Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default is 900 seconds.
   - Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default is 120 seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds.

     Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities screen for a specific entity.
   - Type an integer value in **Number of Retries**. The default is 1.This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable.
6. Under the **CDR** section, change the following information, if required
   - Select the **Enable CDR** check box to enable Call Detail Recording. This enables CDR at the system level for that Session Manager instance. If CDR is enabled, you can individually control call detail recording for specific SIP entities using the Call Detail Recording drop-down menu.
   - Type a password that must be used to access the CDR record and retype to confirm the password. This password is used by an external CDR processing adjunct for connecting to Session Manager and to transfer the generated CDR files. Normally the adjunct logs in with the "CDR_User" user ID with a default password. The password that you specify here becomes the default password. Once the CDR adjunct logs in using "sftp", it is

automatically placed in the Session Manager CDR home directory of the CDR_User, which is **/var/home/ftp/CDR**.

7. Click **Return** to return to the previous screen.

Deleting a SIP entity as a Session Manager instance

To delete a SIP entity as a Session Manager instance:

1. From the navigation pane on the System Manager Common Console, click **Session Manager > Session Manager Administration**
2. Select a Session Manager instance from the list and click **Delete**.
3. On the Delete Confirmation screen, click **Delete** to delete the Session Manager instance.

Local host name resolution

To route a SIP INVITE, Session Manager needs the IP addresses corresponding to the Fully Qualified Domain Name (FQDN) in the INVITE. To resolve a host name by replacing it with its IP address, Session Manager checks for the host name on the local network. When the host name cannot be resolved through broadcasting on the local network, Session Manager searches for it in the host names file or by querying the DNS server that maintains the host name to IP address mapping.

Resolving local host name

The Local Host Name Resolution screen allows you to create, edit, and delete local host name entries. Host name entries on this screen override the information provided by DNS.

To resolve a local host name:

1. From the navigation pane on the System Manager Common Console, click **Session Manager > Local Host Name Resolution**
2. To add a host name entry, click **New**. The system displays the New Local Host Name Entries screen.
3. Enter host name information as follows. You can enter a maximum of ten host names.
   - **Host name**—Name of the host that is to be modified in the local host name table. The host name entries override the information provided by DNS.
   - **IP Address**—IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.

- **Port**—Port number that the host should use for routing using the particular IP address.
- **Priority**—If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
- **Weight**—If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
- **Transport**—The transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default is TLS.

4. Click **Save** to save the host name entry to the host name table.

SIP tracing

The SIP tracer allows tracing of SIP messages exchanged between the Session Manager server and remote SIP entities. SIP messages which are dropped by any of the SM100 components such as SIP Firewall are also logged by the SIP tracer. You can trace all the messages belonging to a user, for a call, or for a selected Session Manager instance. The SIP tracer provides statistics of SIP messages within the SM100 framework. SIP tracer is located under Session Manager on the System Manager Common Console navigation pane. SIP tracer user interface has the following components:

- Tracer Configuration defines the characteristics of messages to be traced for the capturing engine in the security module.
- Trace Viewer displays the captured SIP messages.

Configuring the SIP tracer

The Trace Configuration screen has the following options enabled by default:

- **Enabled**–SIP message tracing is enabled.
- **Dropped**–SIP message tracing is enabled for calls dropped by the security module.
- **From Network to Security Module**–SIP message tracing is enabled for ingress calls sent to the Session Manager instance from the network.
- **From Security Module to Network**–SIP message tracing is enabled for egress calls originating from the Session Manager instance and sent to the network.

The Trace Configuration screen has the following options disabled by default:

- **From Server to Security Module**–SIP message tracing is disabled for internal SIP messages from the Session Manager SIP Server to the security module.

- **From Security Module to Server**–SIP message tracing is disabled for internal SIP messages from the security module to the Session Manager SIP Server

To configure SIP message tracing for each administered Session Manager:

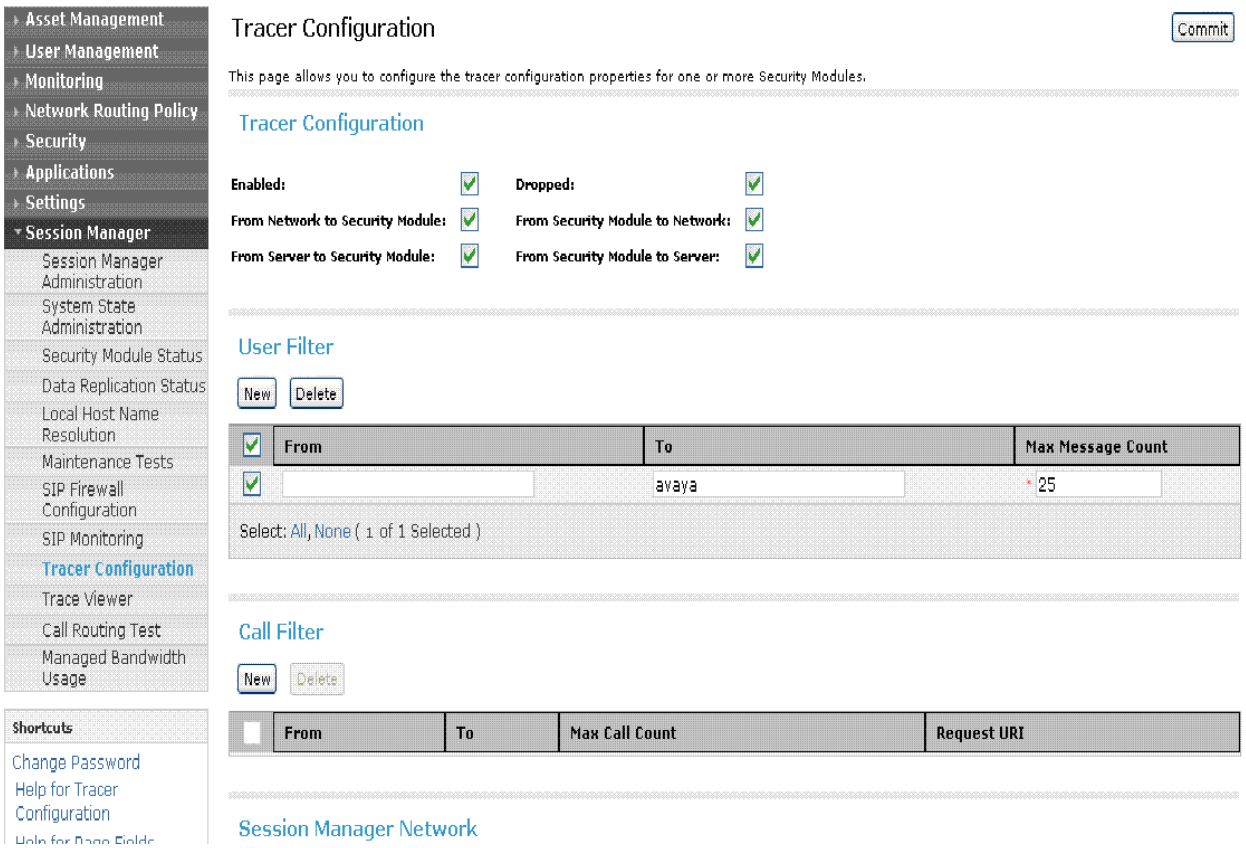
1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Tracer Configuration**
2. To filter SIP messages based on the users, click **New** under **User Filter**. You can define a maximum of three separate user filters:
   - **From**—Traces SIP messages that match the sender from the SIP header. For example, a rule to trace all messages from user “pqr”: to=”” from=”pqr” stop-count=50
   - **To**—Traces SIP messages that match the receiver from the SIP header. For example, a rule to trace all messages to user “xyz”: to=”xyz” from=”” stop-count=50
   - **Max Message Count**—Defines the maximum number of SIP messages to be traced that match the above **To** and **From** definition.

   Note:
   If you do not specify the **From** and **To** filters, Session Manager traces all SIP messages.
3. To delete an existing user filter, select the filter and click **Delete**.
4. Call tracing identifies a “call” by capturing the unique call ID from the first message which matches the filter, and then tracing all of the messages which have a matching call ID. You can define up to three possible filters containing the sender, the receiver, and the request URI characterization. To filter all SIP messages that start a new call (such as INVITE or REGISTER) click **New** under Call Filter.
   - **From**—Traces SIP messages that match the sender from the SIP header. For example, a rule to trace all messages from user “per”: to=”” from=”pqr” stop-count=50
   - **To**—Traces SIP messages that match the receiver from the SIP header. For example, a rule to trace all messages to user “xyz”: to=”xyz” from=”” stop-count=50
   - **Max Message Count**—Defines the maximum number of SIP messages to be traced that match the above **To** and **From** definition.
   - Type the URI address in the **Request URI** field. A valid Request URI format, for example, is .@192.111.11.111.

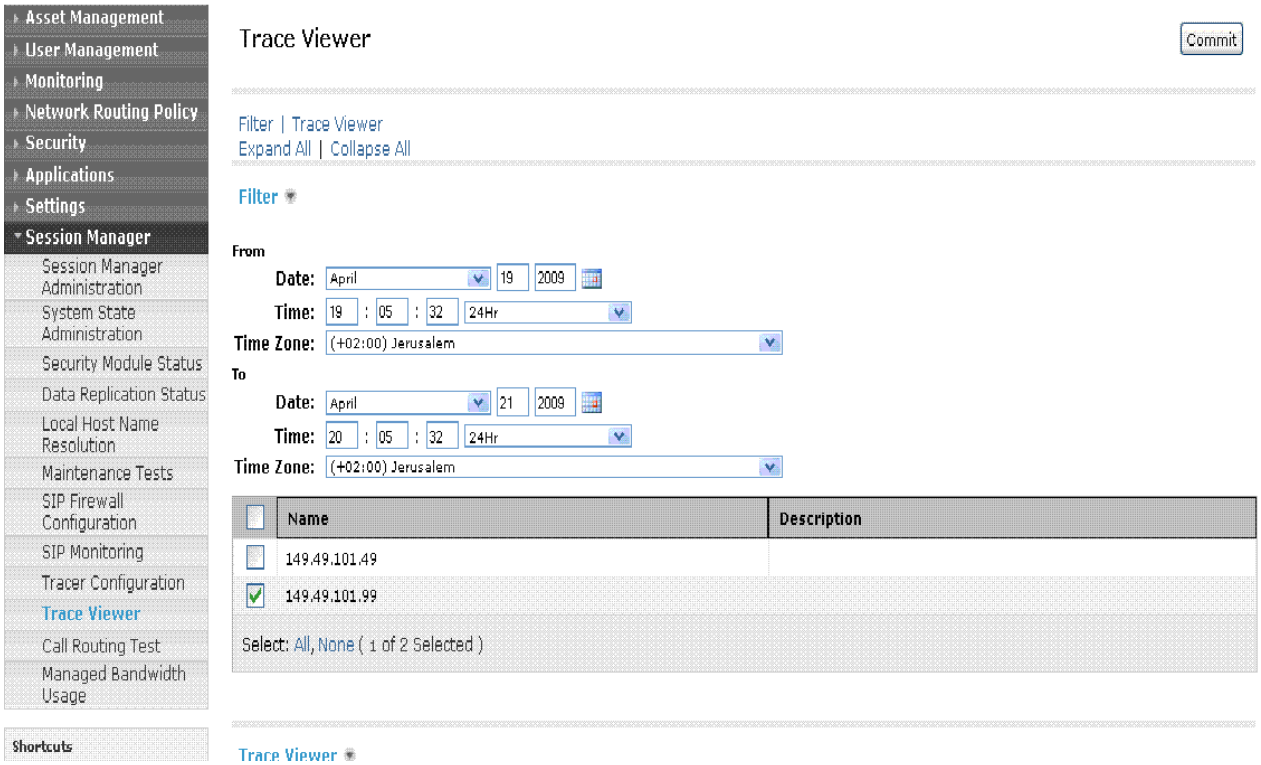
   Note:
   If you do not specify the **From**, **To,** and **Request URI** filters, Session Manager traces all SIP messages.
5. To delete an existing call filter, select the filter and click **Delete**.
6. To use these configured filters for specific Session Manage instances, select one or more configured Session Manager instances from the list under Session Manager Network.
7. To save the configuration changes to the SIPMsgTracer.conf file, click **Commit**. The system overwrites the earlier configurations.

Example: SIP trace

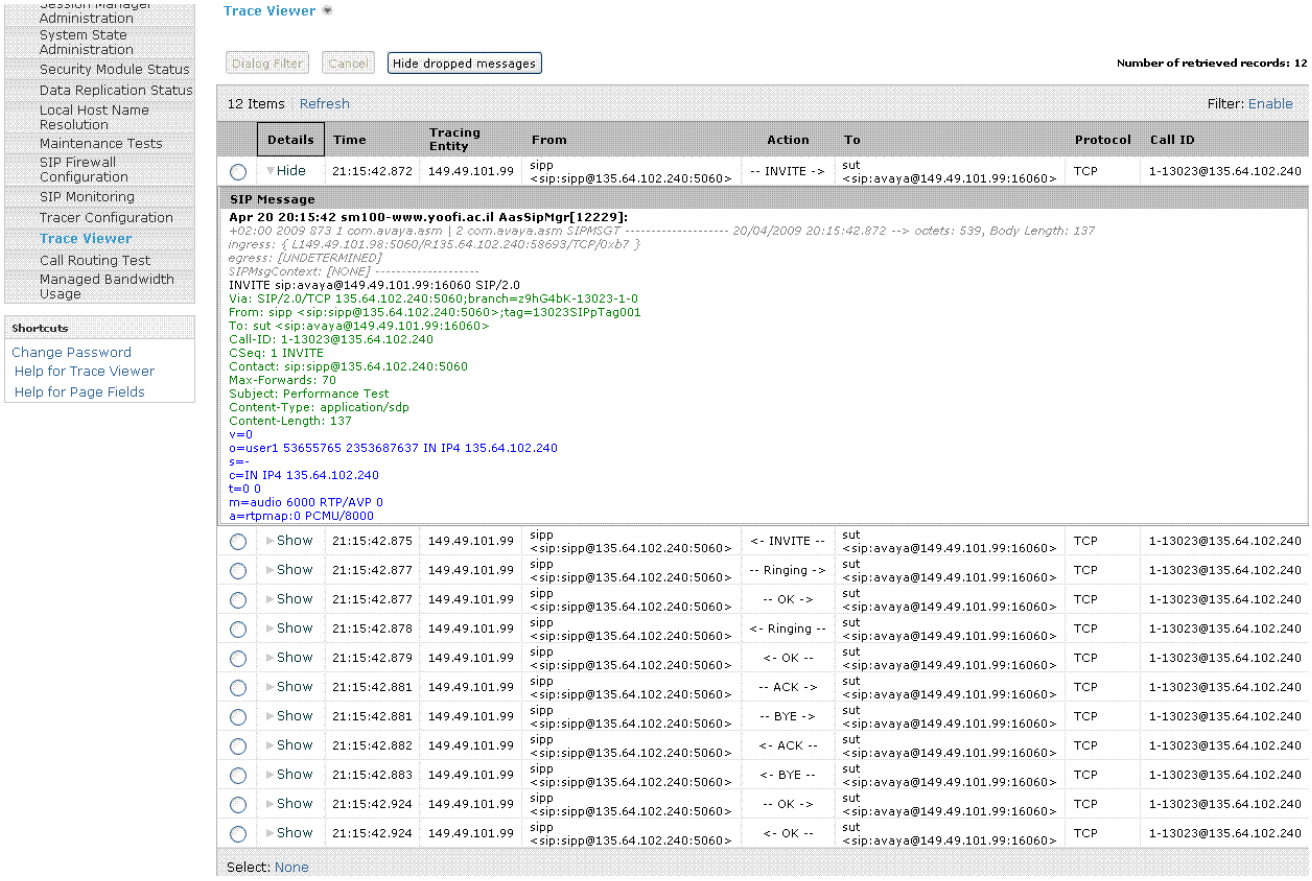
In the following example, the filter is configured to capture a maximum of 25 SIP messages addressed to “avaya” going through the administered Session Manager 149.49.101.99.



The Session Manager and the time frame selected for viewing the SIP trace are as shown below:



The following figure displays the resulting messages addressed to “avaya”:



The **Dialog Filter** button allows you to filter trace log entries. Select a trace log and click **Dialog Filter**. You can also click **Filter Enable** to filter log entries based on a value or to sort them based on selected columns.

Cancel cancels the filtering of the trace log entry.

Clicking on the **Hide dropped messages** button causes dropped messages to not be displayed in the trace log entries and changes the button to **Show dropped messages**. Clicking on the **Show dropped messages** button will displayed dropped messages in the trace log entries and change the button to **Hide dropped messages**.

Managed bandwidth

The Managed Bandwidth Usage screen displays Managed Bandwidth (Call Admission Control) real-time data. It displays a read-only table containing one row for each administered location where usage is managed. The row contains current bandwidth usage and the maximum values

and provides an estimated usage percentage and number of calls that can be made before the limits are reached.

You can also expand each row to display a breakdown of usage and capacity by Session Manager, which can be helpful in debugging network utilization or the distribution algorithm. If no bandwidth management is administered, this table contains no data.

Viewing managed bandwidth usage

To view managed bandwidth usage:

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Managed Bandwidth Usage**

   The Managed Bandwidth Usage screen displays system-wide bandwidth usage information for locations where usage is managed. If the Managed Bandwidth field on the location form is blank, this table has no information for that location.

2. On the Managed Bandwidth Usage screen, click **Refresh** to refresh the following data:
   - **Details**—Shows the breakdown of usage among the administered Session Managers in the enterprise.
   - **Location**—Locations that you have administered in NRP
   - **Bandwidth per Call (kbit/sec)**—This is the value that you enter in the NRP Location Details screen
   - **Bandwidth in Use (kbit/sec)**—Current bandwidth used
   - **Total Bandwidth Available**
   - **Percent Used**—Percent of the total bandwidth used
   - **New Call Capacity**—Number of calls that can be made before the maximum bandwidth capacity is reached

Appendix A: Installation and Administration Worksheets

This appendix contains the worksheets for configuring and administering Session Manager on a server. Use the worksheets to capture the information you will need to enter on the various configuration and administration screens.

Installation information

Make a copy of this worksheet for each Session Manager instance in your System Manager network.

Field	Information to enter
IP address for Eth0 (management interface for Session Manager on the customer network)	
Netmask IP address for Eth0	
Default Gateway for Eth0	
System Manager server hostname	
Session Manager IP address	
Primary DNS	
Secondary DNS (if applicable)	
Tertiary DNS (if applicable)	
DNS Search Domains (space separated for multi-entry)	
Local time zone	
NTP server	
Secondary NTP server (if applicable)	
Tertiary NTP server (if applicable)	

Field	Information to enter
10-digit Session Manager Alarming Product Identifier	
IP address of the System Manager server	
SIP domains (enter only the IP address of ETH0 here)	

You can use the following three tables to collect some of the key information ahead of time that you need to administer Session Manager-related entities using the System Manager. Note that this does not represent all of the information needed, but it does represent the information that may take some lead time to collect. Collecting this information prior to performing System Manager Administration can expedite the Session Manager administration process.

SIP entity information

You need the following information for each Session Manager or Communication Manager SIP entity administered using System Manager. This information is used to administer NRP SIP Entities, NRP Entity Links, and for Session Manager administration.

Field	Information to enter
Entity Name	
Entity Type (Session Manager, Communication Manager, and so on)	
Location Name	
IP Address	
FQDN	
Port (5061)	
Transport (TCP or TLS)	
SM100 IP Address (Session Manager only)	
SM100 Network Mask (Session Manager only)	
SM100 Default Gateway (Session Manager only)	

Field	Information to enter
CLAN/PROCR (Communication Manager only)	
Signaling Group (Communication Manager only)	
Trunk Group (Communication Manager only)	

SIP domain and location information

You need this information for each location. This information is used to administer NRP SIP domains and NRP locations.

Field	Information to enter
SIP Domain (for example, avaya.com)	
Location Name	
Location IP Address Patterns (for example, 135.9.*.*) You can have more than one IP address patterns	

Dial plan information

You need this information for each dial pattern. This information is used to administer NRP dial patterns and NRP routing policies.

Field	Information to enter
Dial Pattern (for example, 303538)	
Min number of digits	
Max number of digits	
Destination(s)	

Appendix B: Configuring Individual SIP Entities

For SIP entities to work with Session Manager, they must be configured. SIP entities which work with Session Manager provides a list of several SIP entities with reference to application notes that provide configuration procedures. These application notes are available within the Avaya Resource Library.

Table 2: SIP entities which work with Session Manager

SIP Entity	Release	Application Note
PBXs		
Communication Manager	5.1,5.2	Configuring Avaya Aura™ Communication Manager To Work with Avaya Aura™ Session Manager
Cisco CallManager	7.x	Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Cisco Unified Communications Manager
Nortel CS1000	4.5	
PSTN service providers		
AT&T (IP FlexReach)	NA	SIP Trunking to AT&T with Session Manager 1.1 through Acme Packet Session Director
Verizon	NA	
SIP gateways		
Avaya G860 Trunk Gateway	2.0	Voice Portal First Solution: Configuring Avaya Aura™ Session Manager with Avaya G860 High Density Trunk Gateway, Avaya Aura™ Communication Manager, and Avaya Voice Portal
Adjuncts		
Modular Messaging	5.1	
Voice Portal	4.1,5.0	Voice Portal First Solution: Configuring Avaya Aura™ Session Manager with Avaya G860 High Density Trunk Gateway, Avaya Aura™ Communication Manager, and Avaya Voice Portal

Table 2: SIP entities which work with Session Manager

SIP Entity	Release	Application Note
Meeting Exchange	5.1	
Extended Meet-Me Conference	1.0.7	Avaya Aura™ Session Manager and Expanded Meet Me Conference (EMMC)

Appendix C: Default Certificates used for SIP-TLS

The Trusted/CA certificate of the issuer that follows is used to generate the default Identity certificate for SIP-TLS:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Avaya Inc., OU=SIP Product Certificate Authority,
CN=SIP Product Certificate Authority
        Validity
            Not Before: Jul 25 00:33:17 2003 GMT
            Not After : Aug 17 05:19:39 2027 GMT
        Subject: C=US, O=Avaya Inc., OU=SIP Product Certificate Authority,
CN=SIP Product Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:dc:3b:2b:72:c7:b6:11:cd:3e:d5:60:9a:2f:f0:
                    51:9e:ea:0d:46:27:48:7e:e1:8e:d8:67:3c:e6:80:
                    73:ea:a6:09:fe:da:39:6e:42:2d:4d:34:79:62:30:
                    b6:d8:2e:7a:ef:7f:ab:37:f9:7f:f3:87:b6:4d:0f:
                    6b:72:ac:a6:4c:09:86:88:f0:55:fa:5f:7b:58:4c:
                    e3:59:f4:4a:d3:62:78:12:24:2a:4b:78:2b:a3:73:
                    ea:a0:b7:54:a6:46:cc:9a:d7:ed:45:f6:2e:63:be:
                    b1:71:a0:eb:91:6f:93:74:e5:8b:f7:70:8f:39:48:
                    52:f0:ee:41:2b:e3:57:10:0e:fb:21:44:15:99:7e:
                    8e:ab:7f:76:c1:26:39:6a:45:31:dc:e7:21:9b:5d:
                    77:84:b3:e2:6b:b4:8b:de:10:21:41:d9:0f:f0:dc:
                    48:3f:19:b7:16:1a:13:f5:ba:a1:ea:38:f1:fb:e9:
                    a3:4c:63:24:0f:18:cc:c3:06:da:42:7c:68:7b:1e:
```

```
                    40:fb:8e:44:f6:12:5f:80:88:12:89:cb:47:0e:72:
                    3d:b6:f8:02:9b:2e:f8:79:6d:f7:c9:31:37:02:3d:
                    7d:81:6b:1d:82:0f:62:35:ba:c4:3e:a2:c4:c6:f8:
                    57:6f:ba:14:41:c7:e5:8f:a8:13:96:b1:0d:30:44:
                    a1:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114187.7.2.1.1
                  CPS: mailto:sipca@avaya.com;

            X509v3 Subject Key Identifier:
                A0:82:07:29:5C:3A:A0:C4:29:B8:3D:C3:1D:B9:06:55:13:BE:56:2A
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:

keyid:A0:82:07:29:5C:3A:A0:C4:29:B8:3D:C3:1D:B9:06:55:13:BE:56:2A
                DirName:/C=US/O=Avaya Inc./OU=SIP Product Certificate
Authority/CN=SIP Product Certificate Authority
                serial:00

    Signature Algorithm: sha1WithRSAEncryption
        60:3e:b6:92:b6:8f:be:f8:a0:05:32:d5:12:19:59:b8:8e:c6:
        e4:9d:6c:1a:cd:1e:72:17:19:6d:5a:b8:28:a2:c3:0d:fb:5b:
        77:e7:50:04:25:e7:75:0c:2b:d4:5a:26:db:7d:2c:a5:87:5d:
        cf:37:36:0b:85:22:25:98:a3:d1:f7:c2:d5:43:83:f9:97:6e:
        82:da:cb:89:3d:ac:9e:11:45:fc:ef:00:c2:1d:ef:1e:34:d1:
        bd:de:f9:79:e1:4e:1a:40:3b:a6:f7:c1:52:4d:19:58:8d:d4:
        a2:2f:d4:77:b6:b2:8b:3a:28:98:94:b0:44:d6:82:47:04:63:
        e2:17:34:57:81:cd:17:54:65:97:31:f0:2a:b8:d4:34:d6:9c:
        ca:aa:ee:c4:4f:4f:40:5a:c6:1b:51:2e:1c:f8:9e:6d:75:89:
        3d:9d:89:37:e5:8d:56:b4:ac:0e:cf:c3:12:83:09:01:da:77:
        32:d6:b2:3a:22:e5:af:2c:05:1d:77:d0:4a:70:16:06:2d:23:
        15:ba:55:46:8e:5d:ce:8b:45:77:e7:1c:4d:a3:22:0a:43:df:
```

```
        11:3c:86:fd:45:c3:04:ce:18:88:92:15:0e:92:d9:9e:60:77:
        bd:05:89:fc:12:7e:fa:ab:9a:0e:5c:7d:02:68:84:0e:95:df:
        55:a2:87:7f
-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFByb2R1Y3QgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkwHhcNMDMwNzI1MDAzMzE3WhcNMjcwODE3MDUxOTM5WjB6MQsw
CQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFBy
b2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDcOytyx7YRzT7VYJov8FGe6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQi1N
NHliMLbYLnrvf6s3+X/zh7ZND2tyrKZMCYaI8FX6X3tYTONZ9ErTYngSJCpLeCuj
c+qgt1SmRsya1+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r
f3bBJjlqRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGhP1uqHqOPH76aNMYyQP
GMzDBtpCfGh7HkD7jkT2El+AiBKJy0cOcj22+AKbLvh5bffJMTcCPX2Bax2CD2I1
usQ+osTG+FdvuhRBx+WPqBOWsQ0wRKGNAgMBAAGjggEsMIIBKDA/BgNVHSAEODA2
MDQGC2CGSAGG/AsHAgEBMCUwIwYIKwYBBQUHAgEWF21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggcpXDqgxCm4PcMduQZVE75WKjASBgNVHRMBAf8E
CDAGAQH/AgEBMAsGA1UdDwQEAwIBBjCBpAYDVR0jBIGcMIGZgBSgggcpXDqgxCm4
PcMduQZVE75WKqF+pHwwejELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIVNJUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
MCgGA1UEAxMhU0lQIFByb2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBgPraSto+++KAFMtUSGVm4jsbknWwazR5yFxltWrgo
osMN+1t351AEJed1DCvUWibbfSylh13PNzYLhSIlmKPR98LVQ4P5l26C2suJPaye
EUX87wDCHe8eNNG93vl54U4aQDum98FSTRlYjdSiL9R3trKLOiiYlLBE1oJHBGPi
FzRXgc0XVGWXMfAquNQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS
gwkB2ncy1rI6IuWvLAUdd9BKcBYGLSMVulVGjl3Oi0V35xxNoyIKQ98RPIb9RcME
zhiIkhUOktmeYHe9BYn8En76q5oOXH0CaIQOld9Vood/
-----END CERTIFICATE-----
```

Following set of default certificates (in PEM format) are trusted by the Session Manager Security module for SIP-TLS. Append any additional certificates to this list before using the update_ca_cert.sh script:

```
-----BEGIN CERTIFICATE-----
MIICaDCCAdECBEgQqykwDQYJKoZIhvcNAQEEBQAwezELMAkGA1UEBhMCVUsxEDAO
BgNVBAgTB1MgV2FsZXMxEDAOBgNVBAcTB0NhcmRpZmYxDjAMBgNVBAoTBWF2YXlh
MRcwFQYDVQQLEw5VSyBFbmdpbmVlcmluZzEfMB0GA1UEAxMWYXZheWEgZGV2ZWxv
cG1lbnQgdGVhbTAeFw0wODA0MjQxNTQ1NDVaFw0xODAzMDMxNTQ1NDVaMHsxCzAJ
BgNVBAYTAlVLMRAwDgYDVQQIEwdTIFdhbGVzMRAwDgYDVQQHEwdDYXJkaWZmMQ4w
DAYDVQQKEwVhdmF5YTEXMBUGA1UECxMOVUsgRW5naW5lZXJpbmcxHzAdBgNVBAMT
FmF2YXlhIGRldmVsb3BtZW50IHRlYW0wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALpOPDPCHq8jpMs+Guaam66iBPOeFBB0SNrLu5Ua1K7fkqEmjG6O+xvnb0Dm
2keo87gZkgSnktazUHfqSQmK9UC12GpomBuJPTZPlSrhcovtadTvjBpnYylp7tVZ
cvsuQxVlaICqr067w6uq0woP4cGSG9kyuhzqvtLCmIiZOFKHAgMBAAEwDQYJKoZI
hvcNAQEEBQADgYEAnLwTrvc4WZsDWw3cuCZlTLYEEIoY9oebhx4EEgOKBz/HXjr5
yA0JiSd+KWdWdfGryhc7YYSbTruO6Hclmq7uJeaFqexdfEYtWQ0ZE1UFAZwLcz5c
Vast/vxri4NVsM+HZ4caayKPAio8csWhiQkfFDp783ho8dBW9uKQkImd8KU=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIE3zCCA8egAwIBAgIBWzANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kx
HjAcBgNVBAMTFUF2YXlhIFByb2R1Y3QgUm9vdCBDQTAeFw0wNzEyMjExMTU0NDBa
Fw0yNzEyMDIxMTU0NDBaMGsxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLExFBdmF5YSBQcm9kdWN0IFBLSTErMCkGA1UEAxMiQXZheWEg
TWFudWZhY3R1cmluZyBTdWJvcmRpbmF0ZSBDQTCCASAwDQYJKoZIhvcNAQEBBQAD
ggENADCCAQgCggEBAMNFdBihMGWSsTAx24rWE5sbjMVkHe0ybSAoZZliLrow9Jau
UfasJ7dm49GQAbeVWqYZ15kFjR9vxUj4ExGt/TcEbBcTau4wkG1tGrf9IsFLzJ9J
dWuC3EWuXcUr4N3UTuSuARh+Q/J31AsXOkSY+N0Tt2QhNedSeqCAXhUKhDp9FySS
ICcobqJgS70W34wXvbgXTrWvlWRanphiADN7lUoUtFpqS+qIfnpTABDG0TUGu9pk
ej3/ftzmfsACdPw5CzLUklglW5c8l6iJYH1stwkTPrrJkLPaCV1NOLZnpiSgQ9ru
3IbVXAn8MUPkiVU91bitZoB1bCS1WgkF+Q4tiM0CAQOjggGbMIIBlzAdBgNVHQ4E
FgQUbuW8D4RGjxrxDTFJElm8Mf7Bz+wwgYYGA1UdIwR/MH2AFMKatvFzIYImbROw
/v5R9l6b3DV7oWKkYDBeMQswCQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5j
LjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kxHjAcBgNVBAMTFUF2YXlhIFBy
```

```
b2R1Y3QgUm9vdCBDQYIBADAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjCB0QYD
VR0gBIHJMIHGMIHDBgtghkgBhvwLBwEBATCBszAqBggrBgEFBQcCARYeaHR0cHM6
Ly93d3cuYXZheWEuY29tL3BraS9DUFM7MIGEBggrBgEFBQcCAjB4MBcWEEF2YXlh
IFByb2R1Y3QgQ0EwAwIBARpdQXZheWEgSW5jLiBMaW1pdGVkIExpYWJpbGl0eSBQ
S0kgQ0EuICBQbGVhc2UgdmlzaXQgaHR0cDovL3d3dy5hdmF5YS5jb20vcGtpL0NQ
UyBmb3IgZGV0YWlscy47MA0GCSqGSIb3DQEBBQUAA4IBAQBv40OigRG3iXiqmVwX
WUdK1DaNQ7wDYCVPteNa9smLrdswAohdqMpyBS0Fut+QfqWQkn2p4eL90ZICeqlr
hPYWUFKSmlpKhf93WH+0jsfvuzWefFg4JtlNsWgbVdi1wPdG9wddkgs4Bt6GzwOL
r0iUuZwnHyUahR8KEvFnab0+KA5gTIOqNnF0dGzaePzPzIJ2Tp8ybpSYQTjBVZmP
/YwkociqOMjUwbuUqDKlsARbeZMAUxmLx6V8fv96G+OPf3MUuvclTTVCP7+6i35y
dV5DG/qP4OpAZcFO/HNdtzreIYjDnlbplw2Fy9LClBZmUwHTmSzp1nJjk6Wg3OAD
DVSH
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIE1DCCA7ygAwIBAgIBADANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kx
HjAcBgNVBAMTFUF2YXlhIFByb2R1Y3QgUm9vdCBDQTAeFw0wMzA4MjIxMTI1MzZa
Fw0zMzA4MTQxMTI1MzZaMF4xCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLExFBdmF5YSBQcm9kdWN0IFBLSTEeMBwGA1UEAxMVQXZheWEg
UHJvZHVjdCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+EpellesygWvwACRNRh/6FbkPYDGrf5jpqIzgd3KG1w7gvvQ/ID953REm2DS7DEI
4y7l+zY0MLtNv+I3rASpdxufsFwkHa5zR1FjpkiaP7XhMKXNpSY7No78rko9uiGt
xCx9VdW20kcP4IiEN23jQWfKjGFzkZItCl/aOf2+peh8bSS2MIprGx4rnCMZN1dU
Nnw8nJFGu7IxRlGDA2XqJ7BWBn/pvPMLdaVU60oI1/4IT9lHPUCaRVAC56jJdtxq
F9sNW0ZsBy05/vtopUiStfq8aMtMWCqGkSwjWB2VDWhWj6HTuGk27YsTsFIREJuT
i7rXYBQqRJN0o15aERM6BwIDAQABo4IBmzCCAZcwHQYDVR0OBBYEFMKatvFzIYIm
bROw/v5R9l6b3DV7MIGGBgNVHSMEfzB9gBTCmrbxcyGCJm0TsP7+UfZem9w1e6Fi
pGAwXjELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIEluYy4xGjAYBgNVBAsT
EUF2YXlhIFByb2R1Y3QgUEtJMR4wHAYDVQQDExVBdmF5YSBQcm9kdWN0IFJvb3Qg
Q0GCAQAwDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYwgdEGA1UdIASByTCBxjCB
wwYLYIZIAYb8CwcBAQEwgbMwKgYIKwYBBQUHAgEWHmh0dHBzOi8vd3d3LmF2YXlh
LmNvbS9wa2kvQ1BTOzCBhAYIKwYBBQUHAgIweDAXFhBBdmF5YSBQcm9kdWN0IENB
MAMCAQEaXUF2YXlhIEluYy4gTGltaXRlZCBMaWFiaWxpdHkgUEtJIENBLiAgUGxl
YXNlIHZpc2l0IGh0dHA6Ly93d3cuYXZheWEuY29tL3BraS9DUFMgZm9yIGRldGFp
bHMuOzANBgkqhkiG9w0BAQUFAAOCAQEAQYNqOpJSkAn6tZOAbp7IW2RMFQO2rwNe
```

UFdyWywqWKdoCNv/+9dAkHXp8wSEwRGPuXRJLuSZloRlK7OnT4GBH+YaFMarHpUr
rChkrmcR9smgN1WvSjvTk1HiFXEyurvpRarLRem3spDdN6Cyu/fhroJJEHc0j97O
U2HTNgz0papOAFxYN497y3teENVmRBGNKoUo6NxayOCjv55JBxegvd6bOtabRv1L
OCNK8yeomL5ri9jiTLUgEEZIn3aFXetuKxTjhQqbxcpy16t70SQctIzLXqdp9ZZu
xz27CykJXlmexi5qREs+MLV0jrduRE50nTHMhkHKZBX7yKIgEb9GwQ==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDvDCCAqSgAwIBAgIBADANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCVVMx
FzAVBgNVBAoTDk1vdG9yb2xhLCBJbmMuMTkwNwYDVQQLEzBTZWFtbGVzcyBDb252
ZXJnZWQgQ29tbXVuaWNhdGlvbiBBY3Jvc3MgTmV0d29ya3MxHTAbBgNVBAMTFFND
Q0FOIFNlcnZlciBSb290IENBMB4XDTAzMTIwNTIxMjg0M1oXDTMzMTIwNDIxMjg0
M1owgYAxCzAJBgNVBAYTAlVTMRcwFQYDVQQKEw5Nb3Rvcm9sYSwgSW5jLjE5MDcG
A1UECxMwU2VhbWxlc3MgQ29udmVyZ2VkIENvbW11bmljYXRpb24gQWNyb3NzIE5l
dHdvcmtzMR0wGwYDVQQDExRTQ0NBTiBTZXJ2ZXIgUm9vdCBDQTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANHrAz5BUuNXL3cH9eAodevZY+5C1IaBtmxe
K7+TweCWSljAeX/e2EKMQatNIOFHO3cXqV7ERBUp0ymmrnnmLeqVfbS9anWOzoGr
MCZ3grohkFWh41uBzxlgYhDoGhGc1H8RZJBEE3Rmo5djZrTzAutSuOi7iAO7S9IC
a9RBZF/db3Z8jkc0ucSi3pDTolIJvjVx5ccztRd133uUyvHSAoXAwyFVx/9trZHp
rQr76xUC/8nOAhXlUlt8Vnp5C30X5WywCOXWelIUaLldH55fxDVcGL5h7Yu8SLb9
iynrlJ6XeDKp+fDtWCVySIZBCLx0Ho29f8hOmLpg5/vb691Q6mUCAwEAAaM/MD0w
DwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUc50Q0MwSbfz43CTFP6gsFsrWv+Uw
CwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBBQUAA4IBAQA956Nf5ldsVXTLbRMRBMuS
y1mdFnbtFN3hd8j8PcqDH9du+411JR1DL7cOJEJWDJwO1qlG44A6Mj/JnvwIA0M4
s3AAKV+EBj1du+TBLhZluuEcvgpX1xiQehIFqTS6fp+CBLL2NYEeze0x1d/IHNNA
eBhYfGBNnhbU0YGOlNERYyT+nTgPgVVwuNaagJPyxHkZKWE2BmMT3OBt3vsdJS7S
c+8Xiivl/KSfF3003/hQrzFH6mDtqSwLgFzKadZ2QE3HVdcajt/fW9sGyaq5PfWO
mwyOTwtrcuo2/EQqX03XHeTEohEoqMTTiNXxTLOwaPgAf/dkwmqPDjuZohtAUphg
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIC0DCCAjmgAwIBAgIBADANBgkqhkiG9w0BAQQFADBVMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEVMBMGA1UECxMMTWVkaWEgU2VydmVyMRowGAYD
VQQDExFBdmF5YSBDYWxsIFNlcnZlcjAeFw0wMjAxMTAwMzQwNDdaFw0zMjAxMDMw
MzQwNDdaMFUxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJbmMuMRUwEwYD
VQQLEwxNZWRpYSBTZXJ2ZXIxGjAYBgNVBAMTEUF2YXlhIENhbGwgU2VydmVyMIGf

```
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDABs8TR5L3cDQNZTsA+t1HJZDOM/Sr
Ngq6TRWf3r8KdzUpYZVAxecODQ2gu9ccfLraxhi8Vn1X6DD/uBT90WdqkhpZs0+f
o6WE7fZZqGFJyVHhtqrN58IOOdQTfjKywhi0w+GTKfEvS/IHXLNM7Rr55KN4Jqa7
3GzklP0d//it4QIDAQABo4GvMIGsMB0GA1UdDgQWBBQ7f+X4y7uDnQ2lkDsVYuFr
ESzohDB9BgNVHSMEdjB0gBQ7f+X4y7uDnQ2lkDsVYuFrESzohKFZpFcwVTELMAkG
A1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIEluYy4xFTATBgNVBAsTDE1lZGlhIFNl
cnZlcjEaMBgGA1UEAxMRQXZheWEgQ2FsbCBTZXJ2ZXKCAQAwDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQQFAAOBgQAa1P7y67oAqwsnM268fXWKTjhqixG2N2+BVkkk
2CEgKzFIjUuwV0kllR+RkyijKXsEnFBvXDdDDbuK+K9O2KO//i3I1eRIsMeVJ4Jj
wE9iYt8+Fniir4moMidQW9KT7SK0Db4ARY4GWezJQPFVoPng7Ny6rDooUIcNmZc4
YK9Wbw==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFByb2R1Y3QgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkwHhcNMDMwNzI1MDAzMzE3WhcNMjcwODE3MDUxOTM5WjB6MQsw
CQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFBy
b2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDcOytyx7YRzT7VYJov8FGe6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQi1N
NHliMLbYLnrvf6s3+X/zh7ZND2tyrKZMCYaI8FX6X3tYTONZ9ErTYngSJCpLeCuj
c+qgt1SmRsya1+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r
f3bBJjlqRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGhP1uqHqOPH76aNMYyQP
GMzDBtpCfGh7HkD7jkT2El+AiBKJy0cOcj22+AKbLvh5bffJMTcCPX2Bax2CD2I1
usQ+osTG+FdvuhRBx+WPqBOWsQ0wRKGNAgMBAAGjggEsMIIBKDA/BgNVHSAEODA2
MDQGC2CGSAGG/AsHAgEBMCUwIwYIKwYBBQUHAgEWF21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggcpXDqgxCm4PcMduQZVE75WKjASBgNVHRMBAf8E
CDAGAQH/AgEBMAsGA1UdDwQEAwIBBjCBpAYDVR0jBIGcMIGZgBSgggcpXDqgxCm4
PcMduQZVE75WKqF+pHwwejELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIVNJUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
MCgGA1UEAxMhU0lQIFByb2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBgPraSto+++KAFMtUSGVm4jsbknWwazR5yFxltWrgo
osMN+1t351AEJed1DCvUWibbfSylh13PNzYLhSIlmKPR98LVQ4P5l26C2suJPaye
EUX87wDCHe8eNNG93vl54U4aQDum98FSTRlYjdSiL9R3trKLOiiYlLBE1oJHBGPi
```

```
FzRXgc0XVGWXMfAquNQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS
gwkB2ncy1rI6IuWvLAUdd9BKcBYGLSMVulVGjl3Oi0V35xxNoyIKQ98RPIb9RcME
zhiIkhUOktmeYHe9BYn8En76q5oOXH0CaIQOld9Vood/
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIBADANBgkqhkiG9w0BAQQFADBvMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUExEDAOBgNVBAcTB0FuZG92ZXIxDjAMBgNVBAoTBUFWQVlBMQ0w
CwYDVQQLEwRFTU1DMSIwIAYJKoZIhvcNAQkBFhNpZ29uemFsZXNAYXZheWEuY29t
MB4XDTA0MTAxMzE1Mzc1N1oXDTMyMDIyOTE1Mzc1N1owbzELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk1BMRAwDgYDVQQHEwdBbmRvdmVyMQ4wDAYDVQQKEwVBVkFZQTEN
MAsGA1UECxMERU1NQzEiMCAGCSqGSIb3DQEJARYTaWdvbnphbGVzQGF2YXlhLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA3+P7zLbpBTyyvhYUsrAuh3x6
emQRxA6QtJlNOMWZKLtLSWuap+KFYOLtNd36MZl/KavEn6wCChR5IM1GAPwCIvZV
pG907FRxPoxdZOAZZRqgWzG7L9mC30NxBiBwA3DO9GbFqOdeW8zupf5SBZqpQ7k/
DZO7oAuYZE8GFhNkUVECAwEAAaOBzDCByTAdBgNVHQ4EFgQUixd7HNzpgfqPlLcc
uhqhDYZUX6QwgZkGA1UdIwSBkTCBjoAUixd7HNzpgfqPlLccuhqhDYZUX6Shc6Rx
MG8xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTEQMA4GA1UEBxMHQW5kb3ZlcjEO
MAwGA1UEChMFQVZBWUExDTALBgNVBAsTBEVNTUMxIjAgBgkqhkiG9w0BCQEWE2ln
b256YWxlc0BhdmF5YS5jb22CAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQF
AAOBgQCLiZfxwyTbfC5C5KRnz9tbDLLEzCHoHqZASlUtIK/cY6fzmEtkNb/k6pdM
0CwYeY5u7rBMhj9UmnhvgGSqQKAMZHsFDIYZU6H3HmV6P+l7kKiWYvSag+adwYH4
T0m2+rzTOu/lYioczR5MIrxT3Txrovs8cEYgJNzewPm2/jQeXw==
-----END CERTIFICATE-----
```

Appendix D: A Network Case Study

The following case study describes a network which uses Session Manager to provide the following solutions:

- Harmonizing disparate PBXs, both extension lengths and brands
- VoIP connections to SIP service providers (access to the public switched telephone network [PSTN] via SIP signaling)
- Tail-end hop-off - maintaining calls on the internal core network as long as possible, hopping off to the PSTN at a point where calls are local and/or where they possibly cost less.
- Access to SIP foundation servers including Avaya Aura Modular Messaging.

These solutions make use of the following Session Manager features:

- Geographically redundant network session control structure
- Least cost routing
- Alternate routing around network faults based on active SIP monitoring
- Network bandwidth use limitation based on session admission control
- Load balancing
- Session (or call) detail recording.

The network

This Case Study network consists of:

- Two Session Managers in the core network for redundancy
- Avaya Communication Managers in Westminster, Highlands Ranch, New Jersey HQ, and Avaya Labs New Jersey with differing length (3, 4, and 5-digit) dial plans
- Cisco CallManager in San Jose with a 5-digit dial plan
- A separate SIP trunk to the AT&T SIP service provider
- A session border controller through which trunks to Verizon and hypothetical SIP service providers can be accessed
- Modular Messaging system that serves all users in the enterprise
- A Voice Portal Service for 1-866-GO-Avaya provided in separate locations in the network.

Before beginning to administer Session Manager, we must decide:

- Domains that are used for routing. We make Session Manager authoritative for both avaya.com and avayalabs.com. The avayalabs.com domain is used for calls originated from the Avaya Labs NJ Communication Manager.
- The enterprise-wide dial plan and any domain-specific dial plans. Each user on one of the PBXs can dial another user, local or remote, through a unique 7-digit enterprise-canonical number.
- The locations that are defined for call admission control and any location-specific dial plans.

We adopt a basic philosophy to guide us in administering adaptation and the dial plan:

- The Session Manager dial plan routes internal enterprise-wide numbers and E.164 numbers (including E.164 representations of internal numbers).
- Calling party numbers are sent from the local PBXs in their local dial plan format. These numbers are all converted to enterprise-canonical on ingress to the Session Manager.
- Called party numbers are sent from the local PBXs in their local dial plan format. These numbers are all converted to either enterprise-canonical numbers or E.164 on ingress to the Session Manager.
- Calling party numbers that are in enterprise-canonical format are converted to whatever the service provider requires when a request is forwarded by the Session Manager.

After some initial, core provisioning, for each solution, we follow the administration of this configuration in the order recommended in Network Routing Policy (NRP). This suggests defining in order, domains, locations, adaptations, SIP entities, SIP entity links, time ranges, routing policies, and dialing patterns.

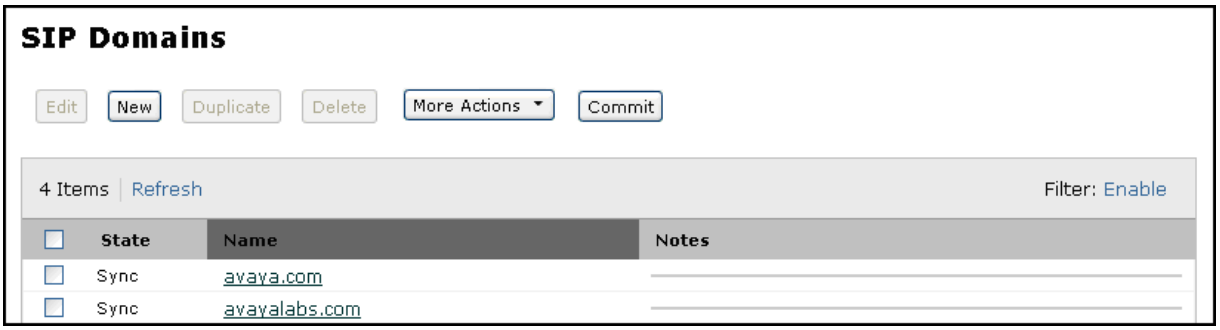
Core provisioning

Core provisioning includes:

- The SIP domains for which Session Manager is authoritative. However, these can be added as more are created.
- The SIP entities for the Session Manager servers. You can add these as more entities are created, linking other SIP entities as appropriate.
- Locations used to group entities for differing dial plans and/or bandwidth management. Again, you can add these as necessary.

SIP domains

First, we add the two domains that appear in the request-URI of INVITE messages sent by the Communication Managers:



The Cisco PBX and the service providers send the IP address of the Session Manager in the request-URI. Later, we administer the Session Manager to convert this IP address into the avaya.com domain so that calls from these entities can be routed.

SIP entities for Session Managers

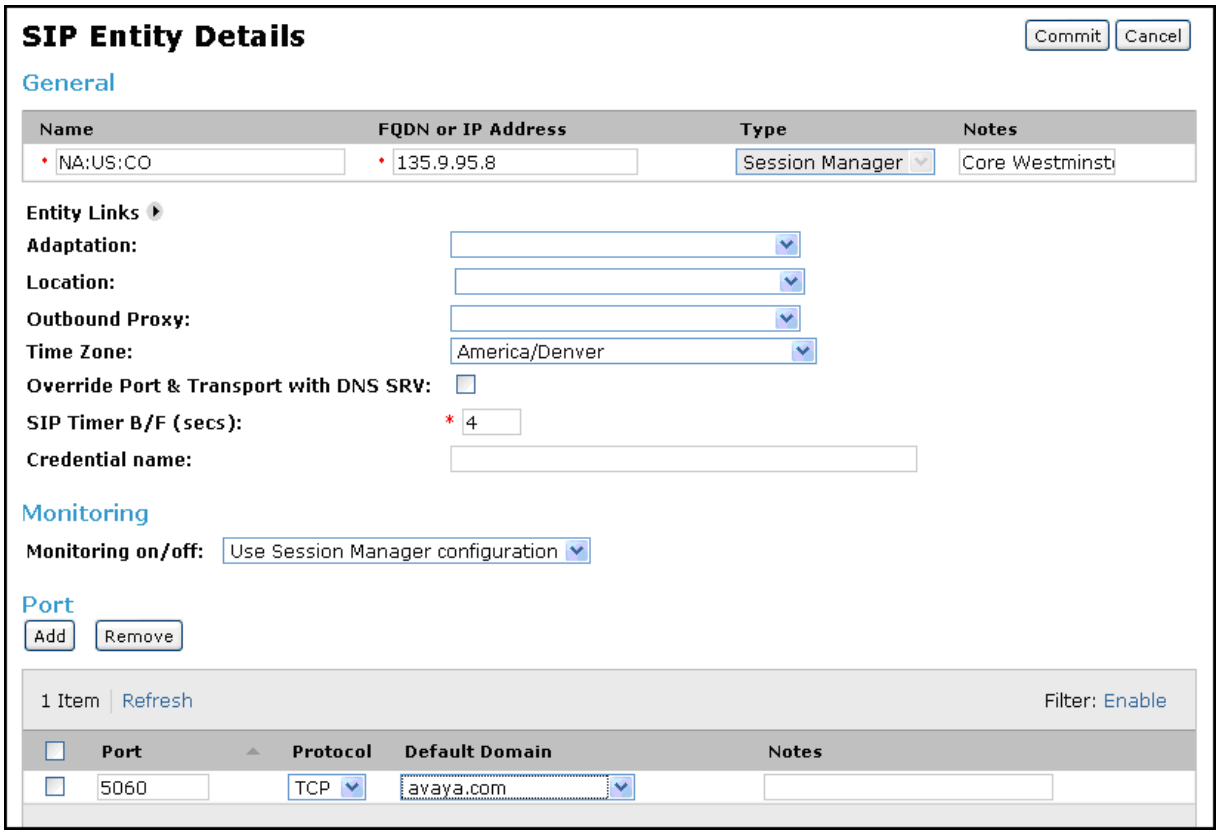
Though NRP suggests finishing the locations and adaptations before beginning SIP entities, Session Manager typed SIP entities are special in that they are not associated with a location nor an adaptation. The other SIP entities normally have both associations. Another, possibly more natural, course is to provision the location, adaptation and SIP entity detail for each SIP entity in turn rather than doing all locations and adaptations before proceeding to the SIP entities.

SIP entity for Westminster Session Manager

Adaptation and location are not necessary for Session Manager instances which essentially define the core network. These are necessary only for other SIP entities.

Generally, Session Manager listens for connections on ports specified in the entity link table, which is detailed later in this case study. If a port is specified in the Session Manager's sip entity port table (as shown below), SIP messages which contain this Session Manager's IP address in their Request-URI have it replaced by the domain specified in the port table. The Cisco PBX and some service providers can send a request with the Session Manager's IP address in the

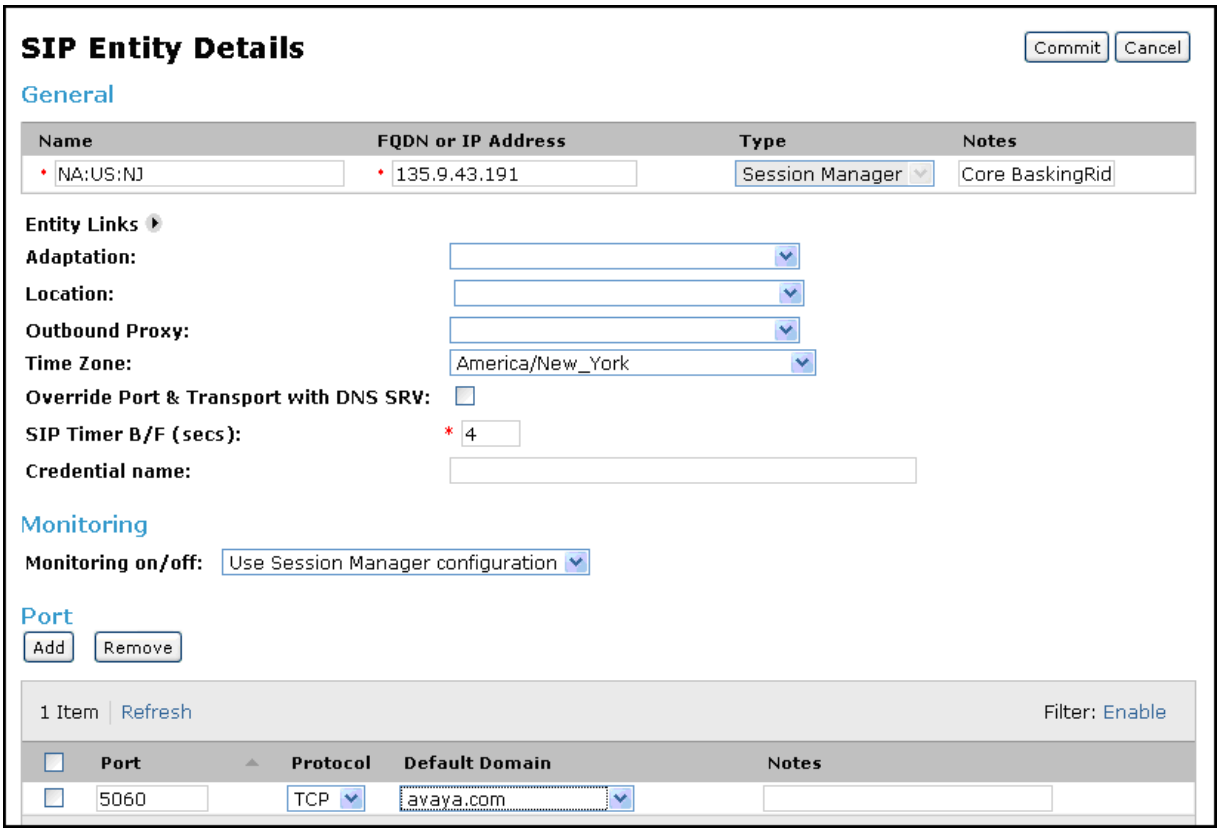
Request-URI. This port table entry is also currently necessary if SIP monitoring is to be used to monitor connectivity between Session Manager instances within the core network.



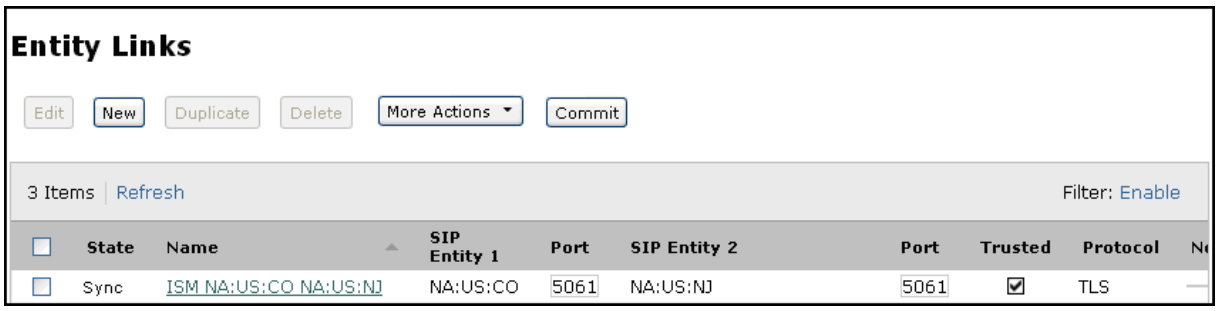
SIP entity for NJ Session Manager

This differs only in minor ways from the Westminster Core Session Manager. A network with two Session Manager instances would normally have each SIP entity connecting to both

instances so that one instance can act as backup for the other in case of network or Session Manager failure.



So that sessions can be alternately routed through another Session Manager in the case of network failure of connectivity between a non-Session Manager SIP entity and a particular Session Manager, the Session Manager instances need to be connected. This connection, like all inter-SIP entity connections, is specified with an entity link entry.



Currently, all entity links should be marked as **Trusted** or else they will not function. Unless there are restrictions against its use, the inter Session Manager entity link should use the **Protocol** TLS. If TLS is used by other SIP entities then it must be used, the reason being that

SIP security standards do not allow passing secure information (like media encryption keys) over a connection where one of the inter-proxy connections is not TLS. Using TLS works, however, even if a SIP entity does not support TLS on its connection to Session Manager.

If there were three Session Manager instances in this case study, there would need to be an entity link between each pair, for a total of three.

Locations

Putting SIP entities into different locations currently serves two purposes:

- Provides a way to use different dialing plans. Calls originating from SIP entities in different locations can match different dialing pattern entries and route differently even though the dialed address are precisely the same.
- Can be used to limit the bandwidth used between the core network and that location.

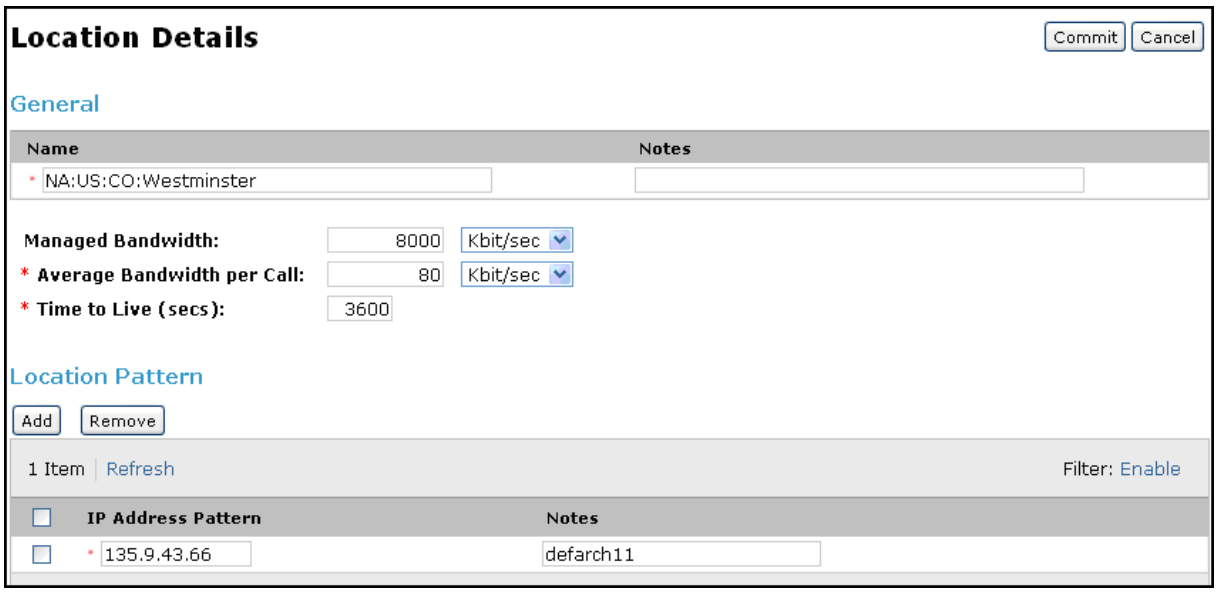
In this case study each edge SIP entity is given its own location. Locations can be created and the location with which a given SIP entity is associated can be changed at any time.

Locations with managed bandwidth

In this case study the Westminster location exemplifies one where bandwidth is managed by setting the **Managed Bandwidth:** value to only allow 100 simultaneous calls in or out of Westminster. The current release of Session Manager assumes that each call to and from the location use the **Average Bandwidth per Call** amount of network bandwidth. Note that the calls that stay within the location, even if they route through Session Manager, are not counted. Thus, the number of simultaneous calls allowed to and from that location are calculated by dividing the **Managed Bandwidth** value by the **Average Bandwidth per Call** value. The two values may be scaled differently, so this might not be a simple division. In the example below, the **Managed Bandwidth** is 8000 Kbits/s and the **Average Bandwidth per Call** is 80 Kbits/s, so the calculation is simple (8000/80 => 100). But if the **Managed Bandwidth** was instead 8 Mbits/s, then the 8 would need to be scaled to 8000 Kbits/s before the calculation is performed.

Incoming calls are associated with SIP entities in varying ways. If the call is associated with a particular SIP entity, it is deemed to have come from the location associated with that SIP entity. If a location contains location pattern IP address patterns, it can override the location

association with the SIP entity. If a SIP entity's IP address is listed explicitly in the IP address patterns, as in this example, then there is no doubt about with which location it is associated.

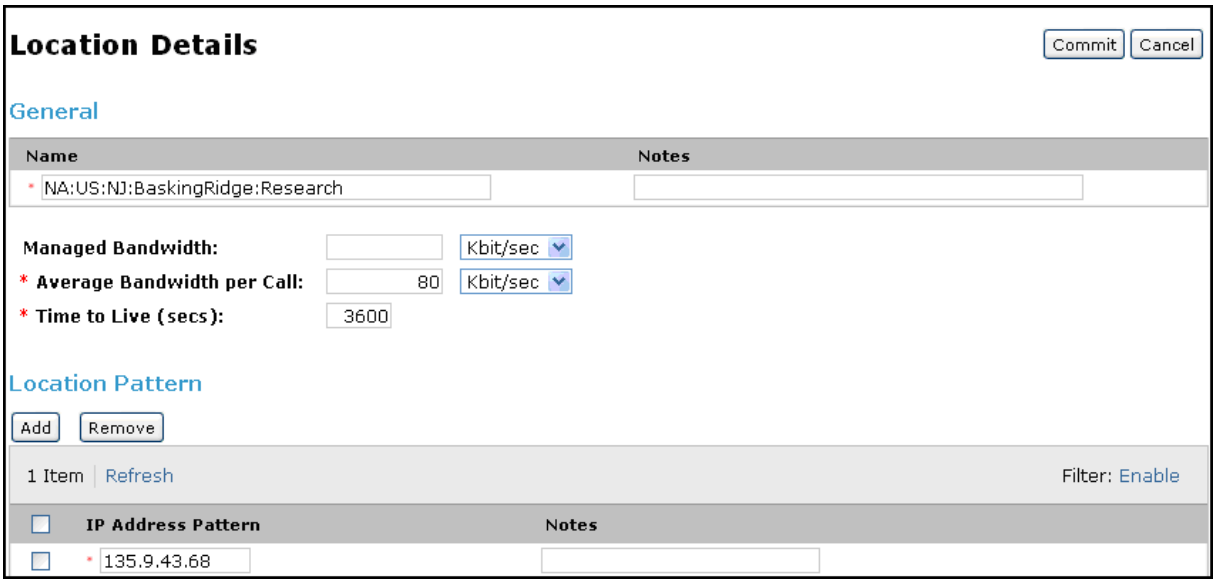


Locations without managed bandwidth

The Research location exemplifies one without managed bandwidth. This does not mean there is unlimited bandwidth between this location and the core, just that Session Manager does not manage the bandwidth and does not limit the number of calls it sends to this location. There may be other limiting factors (like the number of calls the SIP entity will accept) to which Session Manager reacts. Simply leaving the **Managed Bandwidth:** field blank keeps Session Manager from managing the bandwidth.

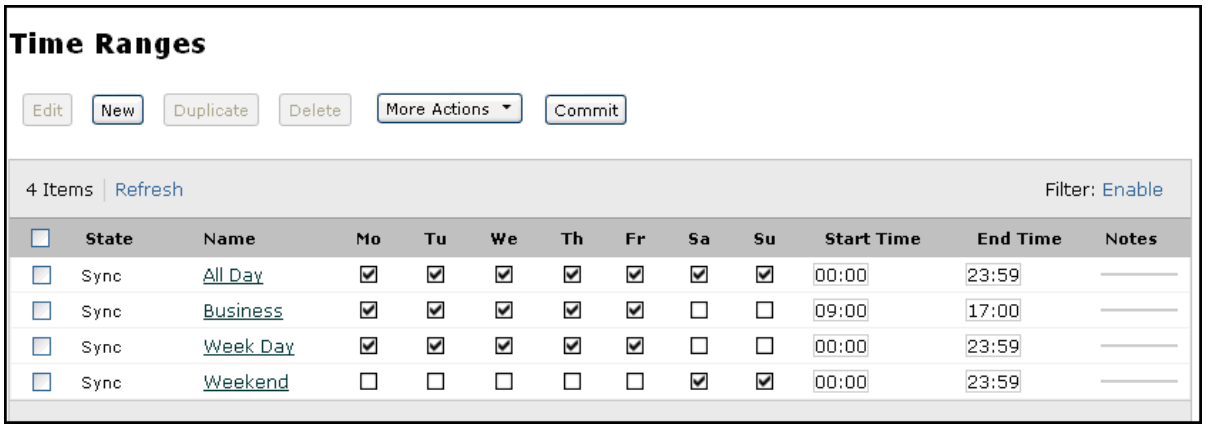
The advantage to having Session Manager manage bandwidth is that it recognizes bandwidth exhaustion to a particular location before attempting to route a call there and it can then perform alternate routing earlier than if it had to wait for the SIP entity at that end to tell it that bandwidth was not available. Additionally Session Manager can associate multiple SIP entities with a given

location and manage the bandwidth to the entire location where each SIP entity would not know the full bandwidth status of the location.



Time ranges

These are used for alternate routing. They are not associated with any particular SIP entity, but are needed for the specification of the ranking of routing preferences (even if routing does not depend upon the time of day). It is useful to have defined at least the All Day time range.

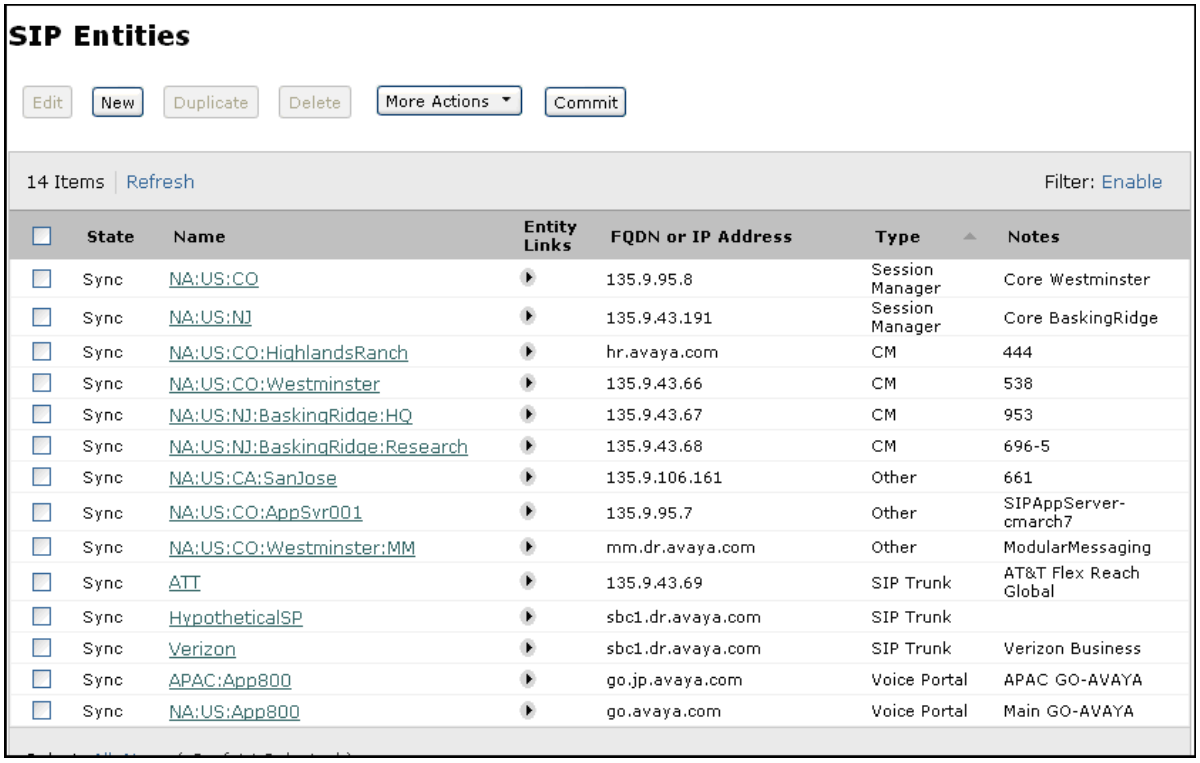


Non-Session Manager SIP entities

The provisioning details of the non-Session Manager SIP entities is outlined as the solutions with which they are associated are explained below. The resulting SIP entities in this case study are listed here in the SIP Entities table. Note that currently the **Type** of the entity matters only if it is Session Manager. All other types are effectively the same, though this could change in future releases, so it is best to choose an appropriate type.

In this case study non-Session Manager SIP entities fall into one of three categories:

- PBXs that front telephones and PSTN trunks
- SIP service providers that essentially 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.
- SIP foundation servers such as Avaya Modular Messaging or Voice Portal or any other server that creates communication sessions with SIP.



SIP Entities

Edit | New | Duplicate | Delete | More Actions | Commit

14 Items | Refresh | Filter: Enable

	State	Name	Entity Links	FQDN or IP Address	Type	Notes
	Sync	NA:US:CO		135.9.95.8	Session Manager	Core Westminster
	Sync	NA:US:NJ		135.9.43.191	Session Manager	Core BaskingRidge
	Sync	NA:US:CO:HighlandsRanch		hr.avaya.com	CM	444
	Sync	NA:US:CO:Westminster		135.9.43.66	CM	538
	Sync	NA:US:NJ:BaskingRidge:HQ		135.9.43.67	CM	953
	Sync	NA:US:NJ:BaskingRidge:Research		135.9.43.68	CM	696-5
	Sync	NA:US:CA:SanJose		135.9.106.161	Other	661
	Sync	NA:US:CO:AppSvr001		135.9.95.7	Other	SIPAppServer-cmarch7
	Sync	NA:US:CO:Westminster:MM		mm.dr.avaya.com	Other	ModularMessaging
	Sync	ATT		135.9.43.69	SIP Trunk	AT&T Flex Reach Global
	Sync	HypotheticalSP		sbc1.dr.avaya.com	SIP Trunk	
	Sync	Verizon		sbc1.dr.avaya.com	SIP Trunk	Verizon Business
	Sync	APAC:App800		go.jp.avaya.com	Voice Portal	APAC GO-AVAYA
	Sync	NA:US:App800		go.avaya.com	Voice Portal	Main GO-AVAYA

Harmonizing disparate PBXs

This case study has two brands of PBXs: Avaya Communication Manager and Cisco Call Manager. Additionally the PBXs have different length extensions (or dial plans). These two aspects require the Session Manager to adapt (that is, alter) SIP messages to the standard SIP messaging performed by Session Manager as well as the E.164 and Enterprise Canonical (that is, common) dial plan used in this example.

Adaptations for PBXs

Adaptation is normally needed for all of the PBX devices that connect to the Session Manager. They, like locations, can be created before a given PBXs SIP entity. This is particularly useful if two PBXs might use the same adaptation. Alternatively, one can create SIP entities with blank adaptations first and then modify the SIP entity to use a particular adaptation created later.

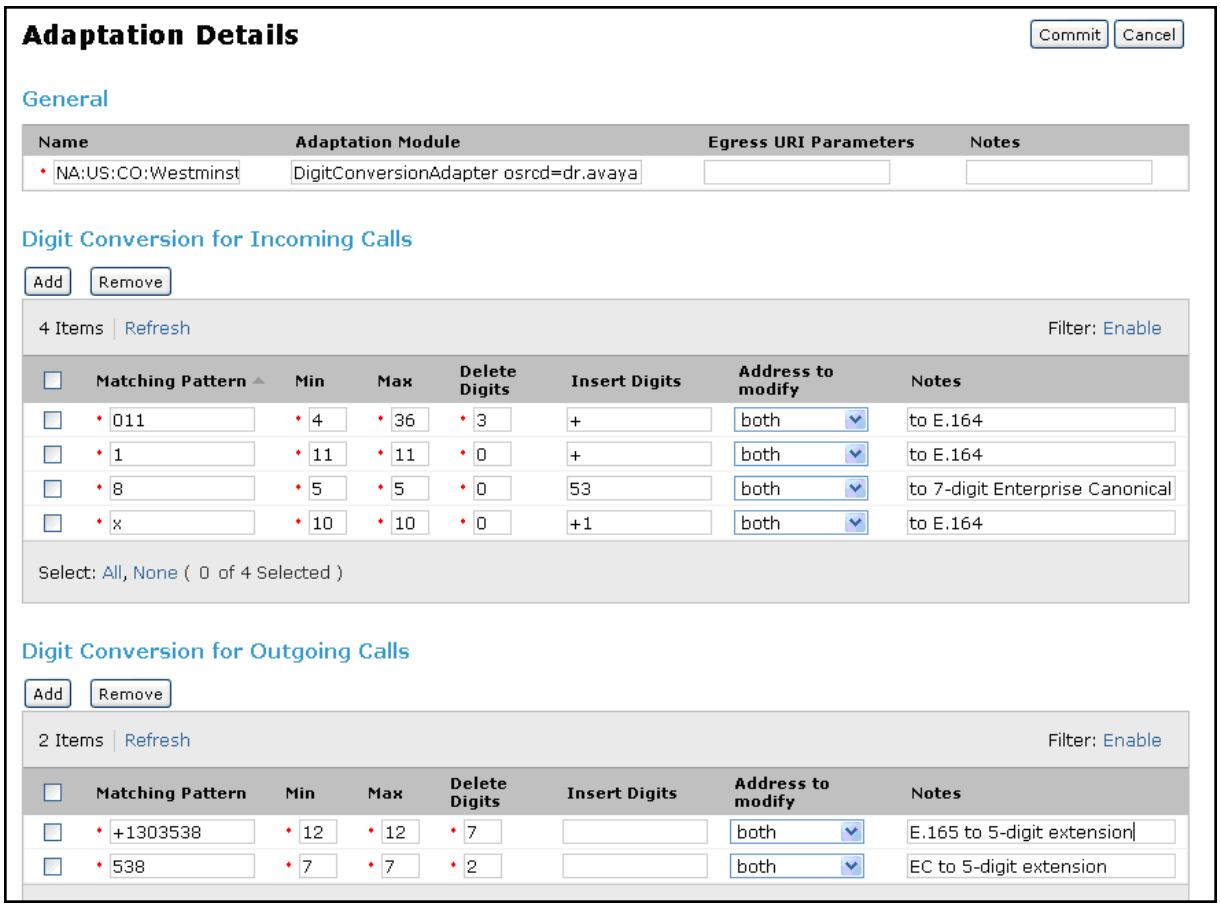
Adaptation digit conversion is likely the most complex aspect of and requires the most planning for the deployment of this example.

Westminster PBX adaptation

The Westminster Communication Manager has a local 5-digit dial plan (8xxxx). Each extension can also be dialed from other systems using the 7-digit enterprise canonical number 538-xxxx. The PBX also has DID numbers assigned; a PSTN caller can dial +1303538xxxx to reach an extension.

This adaptation uses the DigitConversionAdapter. The Westminster PBX is set up to be authoritative for dr.avaya.com on its network region form. This means that INVITEs sent from Session Manager to the PBX must have dr.avaya.com in the host part of the request-URI. The **odstd** parameter to the adaptation module specifies this. The PBX also uses dr.avaya.com as the far-end domain on the signaling group to the Session Manager, which means that the P-Asserted-Identity header of incoming INVITEs must be changed to dr.avaya.com. We use the **osrcd** parameter to the adaptation module to accomplish this.

The digit conversion tables are set up accordingly. The text that is placed in the Adaptation Module box is DigitConversionAdapter odstd=dr.avaya.com osrcd=dr.avaya.com (the parameter **osrcd** means override source domain).

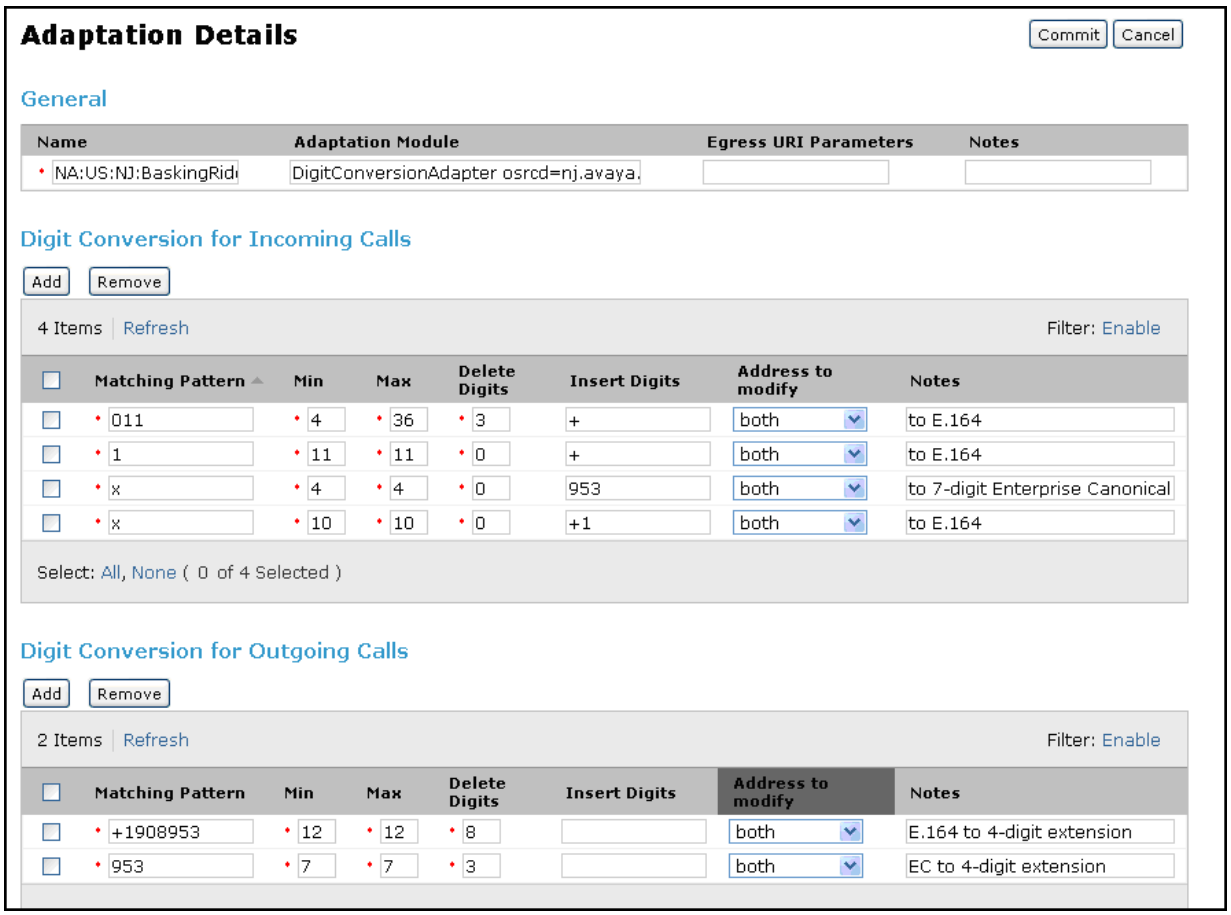


NJ HQ Communication Manager adaptation

The NJ HQ Communication Manager has a local 4-digit dial plan (xxxx). Each extension can also be dialed from other systems using the 7 digit enterprise canonical number 953-xxxx. The PBX also has DID numbers assigned; a PSTN caller can dial +1908953xxxx to reach an extension.

This adaptation uses the DigitConversionAdapter. The NJ HQ PBX is set up to be authoritative for nj.avaya.com on its network region form. It also uses nj.avaya.com as the far-end domain on the signaling group to the Session Manager. These domain conversions are specified as

parameters to the adaptation module. The text that is placed in the Adaptation Module box is DigitConversionAdapter odstd=dr.avaya.com osrcd=dr.avaya.com

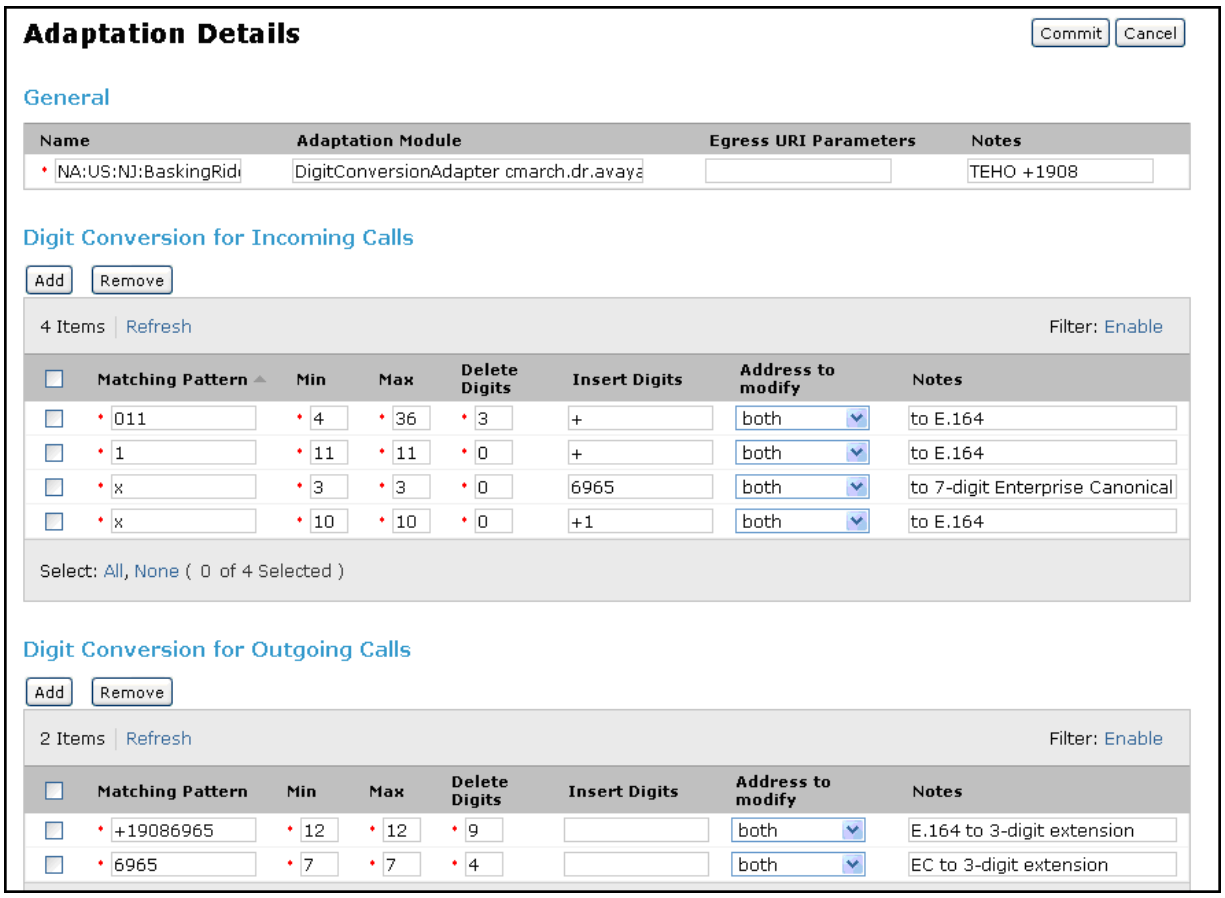


Avaya Labs research PBX adaptation

The Avaya Labs Communication Manager has a local 3-digit dial plan (xxx). Each extension can also be dialed from other systems using the 7-digit enterprise canonical number 696-5xxx. The PBX also has DID numbers assigned; a PSTN caller can dial +19086965xxx to reach an extension.

This adaptation uses the DigitConversionAdapter. The Communication Manager is set up to be authoritative for avayalabs.com on its network region form. It also uses avayalabs.com as the far-end domain on the signaling group to the Session Manager, which means that the P-Asserted-Identity header of incoming INVITEs must be changed to avayalabs.com.

The text that is placed in the Adaptation Module box is DigitConversionAdapter odstd=avayalabs.com osrcd=avayalabs.com



San Jose PBX adaptation

The San Jose PBX has a local 5-digit dial plan (1xxxx). This means that extensions connected to this PBX normally dial each other by entering only five digits. Each extension can also be dialed from other systems using the 7-digit enterprise-canonical number 661-xxxx. The PBX also has DID (direct inward dialing) numbers assigned; a PSTN caller can dial +1408661xxxx to reach an extension. For calls made by local users, adaptation converts

- Numbers dialed by local users into enterprise canonical numbers (for example, a San Jose user calls another San Jose user via the Session Manager)
- Local Calling party numbers into enterprise-canonical numbers (for example, San Jose user calls a Westminster user. The calling party number displayed in Westminster is the enterprise-canonical number)
- Calls to international numbers to E.164 format (for example, someone dials 011+digits)

- Calls to North American numbers to E.164 format

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

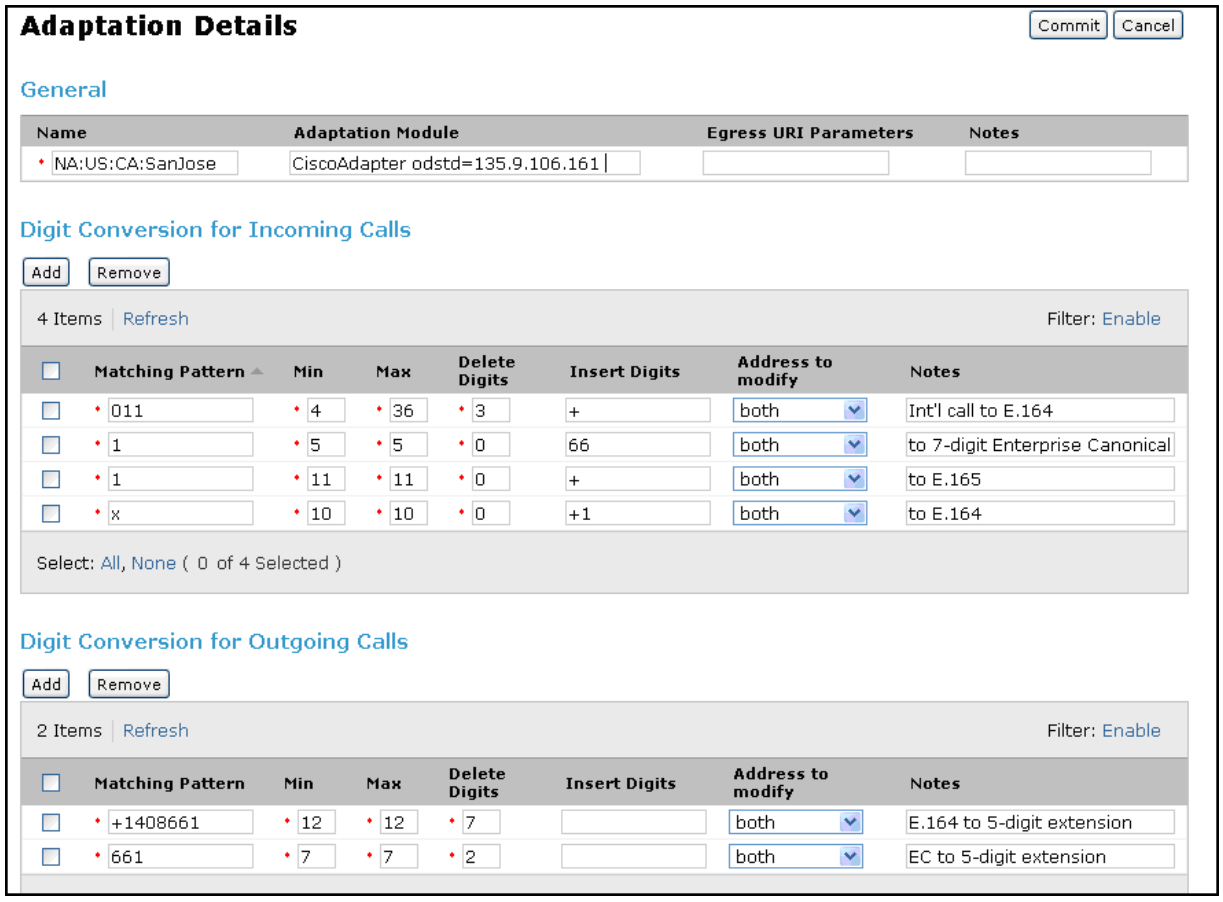
- The called party enterprise-canonical number into a local extension number (for example, a 661-xxxx number into a 1xxxx number)
- The E.164 number into a local extension number, for calls coming from a service provider (for example, +1408661xxxx into 1xxxx)

This adaptation uses the CiscoAdapter to convert between the proprietary headers Cisco uses to convey display and diversion information with the standard headers used by Avaya products. CiscoAdapter, like all currently available adapters, can also perform digit conversion. The Cisco PBX also needs its IP address (135.9.106.161) as the host part of the request-URI, so this conversion is specified as a parameter (odstd, which means override destination domain).

The digit conversion tables convert between the local 1xxxx dial plan and the enterprise canonical 661-xxxx dial plan. On ingress to the Session Manager, digit strings in the local 1xxxx dial plan need to be converted into the enterprise canonical form. On egress from the Session Manager, the 661-xxxx enterprise canonical numbers need to be converted into the local extensions.

The digit conversion tables also convert dialed numbers for international calls (011+digits) or calls within North America (10 digit, 1+10 digit) to E.164 form when requests enter the Session

Manager. Similarly, E.164 and enterprise canonical calls to local users must be converted into local form on egress from the Session Manager.



Adaptation Details Commit Cancel

General

Name	Adaptation Module	Egress URI Parameters	Notes
* NA:US:CA:SanJose	CiscoAdapter odstd=135.9.106.161		

Digit Conversion for Incoming Calls

Add Remove

4 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
	* 011	* 4	* 36	* 3	+	both	Int'l call to E.164
	* 1	* 5	* 5	* 0	66	both	to 7-digit Enterprise Canonical
	* 1	* 11	* 11	* 0	+	both	to E.165
	* x	* 10	* 10	* 0	+1	both	to E.164

Select: All, None (0 of 4 Selected)

Digit Conversion for Outgoing Calls

Add Remove

2 Items | Refresh Filter: Enable

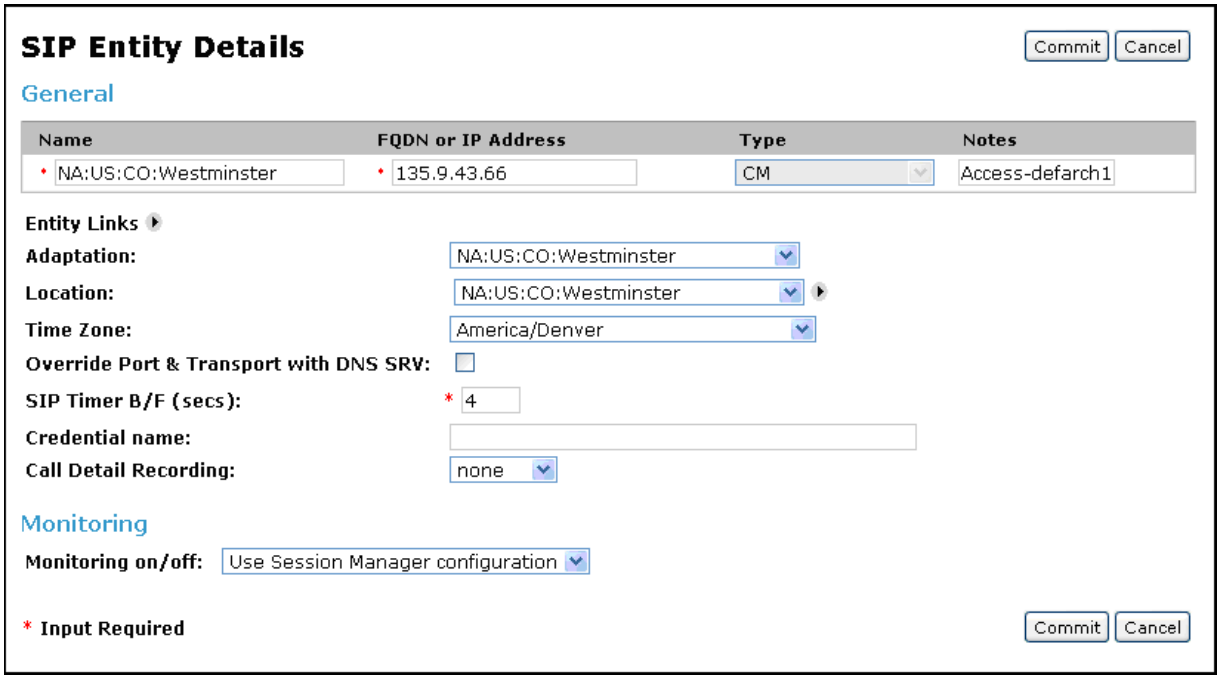
	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
	* +1408661	* 12	* 12	* 7		both	E.164 to 5-digit extension
	* 661	* 7	* 7	* 2		both	EC to 5-digit extension

SIP entities for PBXs

The PBXs in this case study are shown in the SIP entity table above as type Communication Manager or Other (though not all Other-typed SIP entities are edge PBXs). They are each administered similarly. The FQDN/IP Address is the primary distinguishing attribute. It is used to identify sessions as originating from that SIP entity and to where it should send messages to establish sessions to the entity. The location associated with the SIP entity (unless overridden) factors into the routing and the adaptation affects how the messages may be modified.

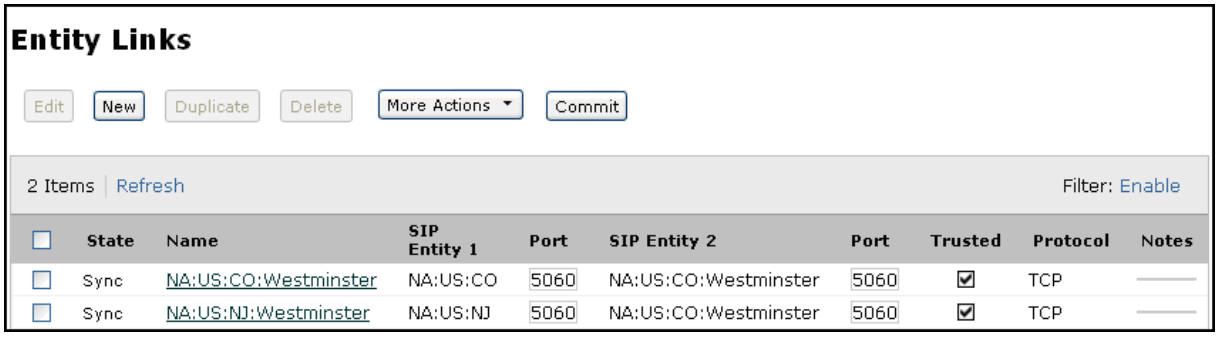
Single interface

The Westminster Communication Manager exemplifies one with a single interface, where its IP address is specified. The other PBXs: Basking Ridge HQ, Basking Ridge Research, and San Jose (even being a Cisco Call Manager) are all similar.



Generally, PBXs do not need call detail records created for each call, so the **Call Detail Recording:** field is set to none. SIP monitoring should be used for all SIP entities that support it (and most all PBXs do), and so the value of **Monitoring on/off:** should be left as Use Session Manager configuration, which allows specification of global (to this Session Manager instance) SIP monitoring parameters.

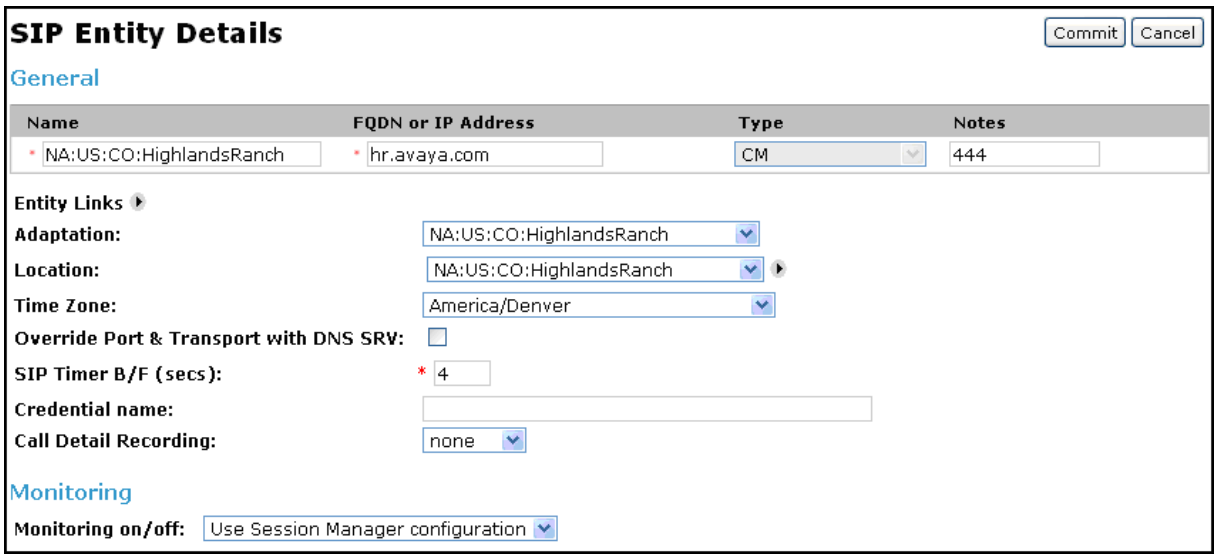
To define the ports and transport types supported by this SIP entity, **Entity Links** entries are made. The entity link table for this SIP entity shows that this SIP entity connects to both Session Manager instances in the network.



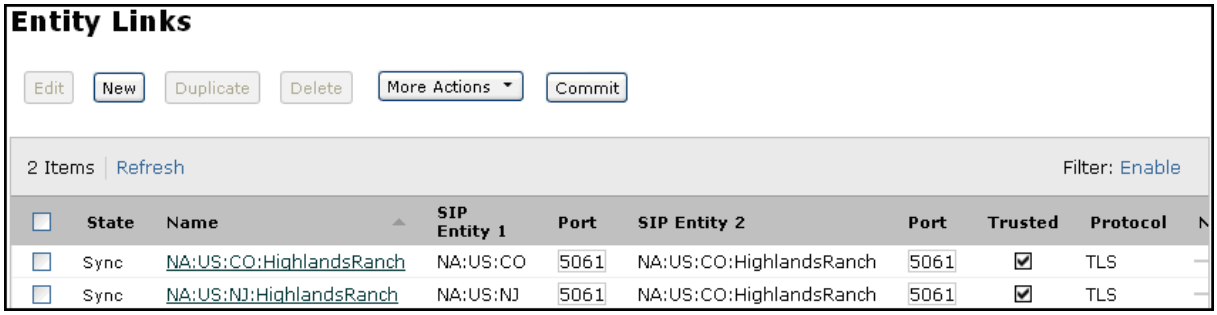
In both cases TCP port 5060 is used, not only for connections out to the SIP entity, but connections in from it. **SIP Entity 1** is always a Session Manager SIP entity. Conventionally, the **Name**, which must be unique for all links in the system, contains some representation of the name of the Session Manager SIP entity and that of the non-Session Manager SIP entity, though this is not necessary. Currently, the entity link must always be marked as **Trusted** or else it fails to function.

Multiple interfaces

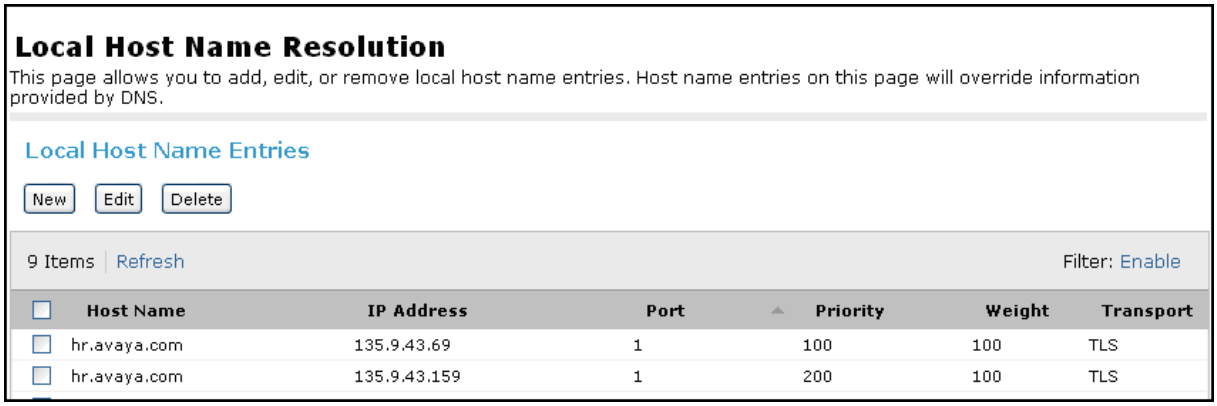
The Highlands Ranch Communication Manager shows a SIP entity with multiple interfaces. This might be typical of a large Communication Manager with more than one C-LAN. It allows for redundant routing and a higher level of fault tolerance. Routing to it is handled by specifying an FQDN for it, which resolves to multiple IP addresses.



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



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



This table is used both for simple FQDN to IP address mapping (like this example) plus full port and transport specification (shown later). For the simple case, the **Port** and **Transport** values are ignored because they are specified in the entity link table (5061 and TLS). The convention of giving the **Port** a value of 1 is used to indicate this. The **Priority** is used, and given that the first line has a higher priority (lower numbered value), it is always used first. The only time the second entry is used is if a failure is encountered while using the first IP address.

To realize this connectivity, the HighlandsRanch Communication Manager requires four signaling and trunk groups: one from each C-LAN to each of the Session Managers. The first signaling group:

```
display signaling-group 1
                                SIGNALING GROUP

 Group Number: 1                Group Type: sip
                          Transport Method: tls
  IMS Enabled? n




   Near-end Node Name: cmc-clan              Far-end Node Name: NA:US:CO
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1
Far-end Domain: avaya.com

                                              Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                  Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 4

Command:
```

The transport method and port match those specified in the entity link from each Session Manager to the Communication Manager. The IMS Enabled field should not be set for standard SIP scenarios. Level 3 tests enabled has the Communication Manager perform OPTIONS monitoring of the Session Manager instances. The Bypass request should probably not be enabled. Communication Manager tests if the network characteristics between its media

processors and the Session Manager are suitable for media and Communication Manager should not be sending media to the Session Manager. 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
```

Assuming all the SIP trunk groups associated with the signaling groups used the same group number, an outgoing routing pattern would look like:

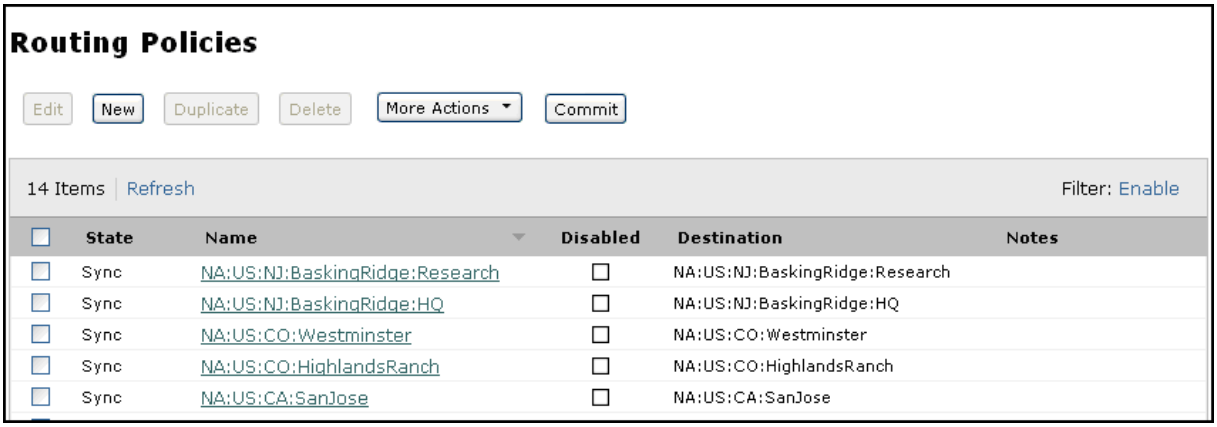
```
change route-pattern 2                                          Page   1 of   3
                     Pattern Number: 2   Pattern Name: External
                                   SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/  IXC
    No          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 would try each of its connections to its local Session Manager (PBX and Session Manager NA:US:CO are both in CO) before trying the remote Session

Manager (NA:US:NJ in NJ). The LAR (look-ahead routing) field must be next on every preference that needs to skip to the next route on an error.

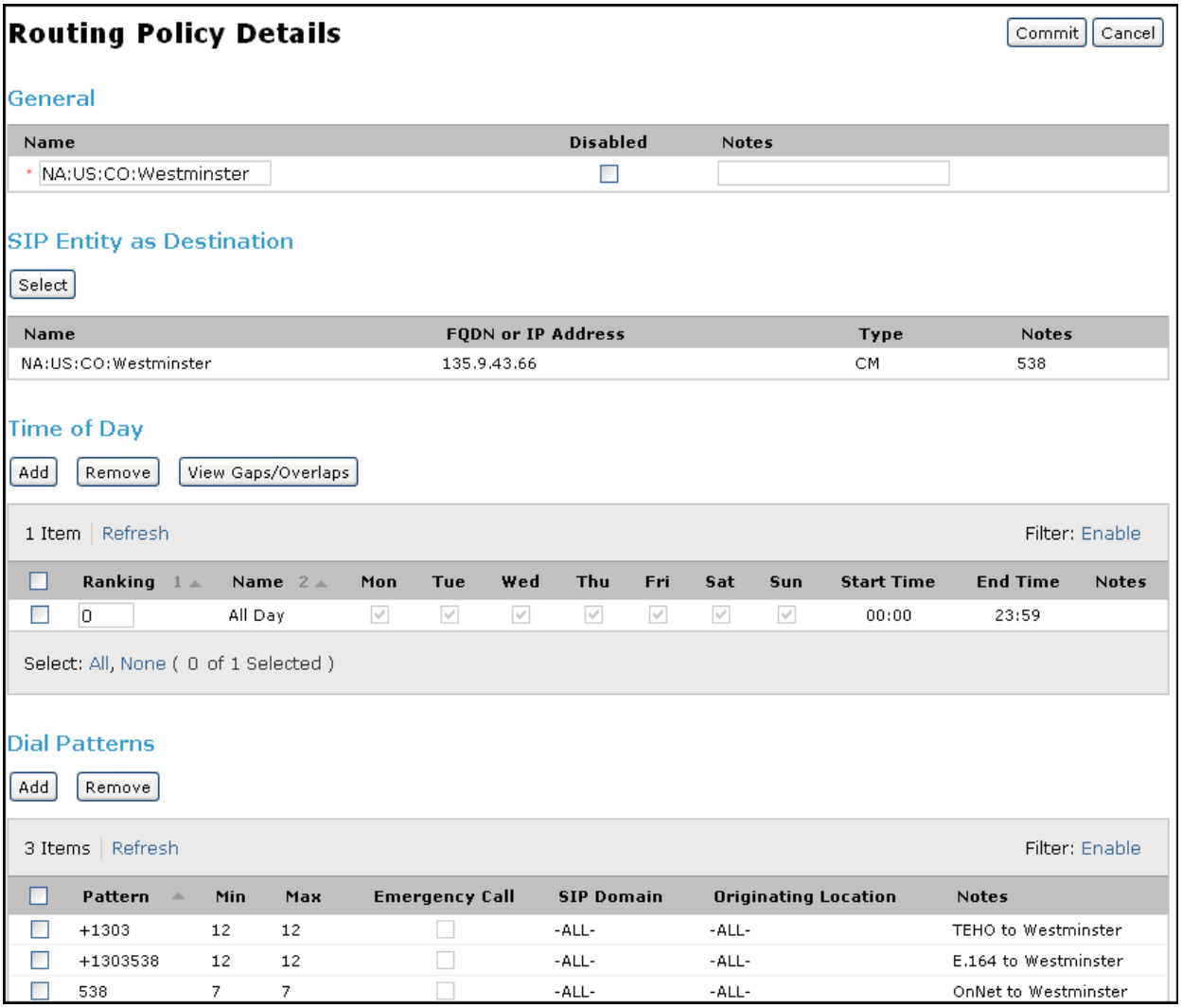
Routing policies for PBXs

Routing policies indicate the rank order of a particular SIP entity. Multiple routing policies can be associated with a dial pattern (as shown later) to specify alternate routing. Additionally, the rank of a routing policy can be changed by the time of day. For simple PBX routing (like in this example) specific dial patterns are associated with only one PBX and these do not vary by the time of day. For these types of routing policies the convention is to use the SIP entity's name as the routing policy name too.



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 not to be part of an alternate route so Ranking of 0 is used. The dial patterns are shown here, but they are defined on another form.



Routing Policy Details

Commit Cancel

General

Name	Disabled	Notes
* NA:US:CO:Westminster	☐	

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
NA:US:CO:Westminster	135.9.43.66	CM	538

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	All Day	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

Select: All, None (0 of 1 Selected)

Dial Patterns

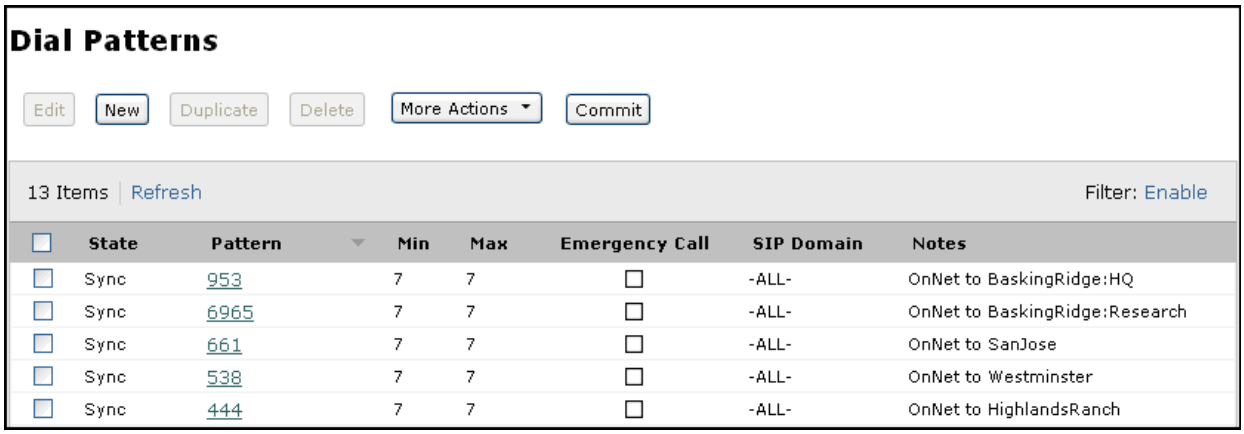
Add Remove

3 Items | Refresh Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	+1303	12	12	☐	-ALL-	-ALL-	TEHO to Westminster
☐	+1303538	12	12	☐	-ALL-	-ALL-	E.164 to Westminster
☐	538	7	7	☐	-ALL-	-ALL-	OnNet to Westminster

Dial patterns for PBXs enterprise canonical numbering

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



Dial Patterns

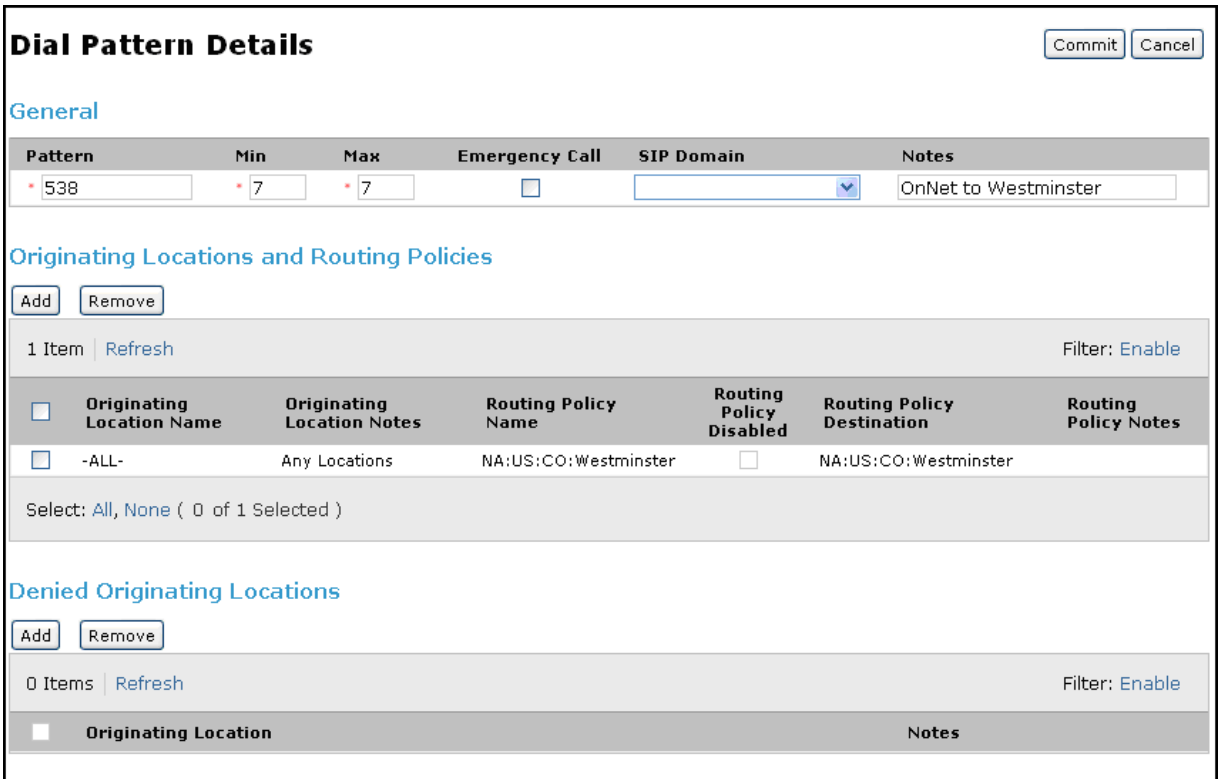
Edit | New | Duplicate | Delete | More Actions | Commit

13 Items | Refresh | Filter: Enable

State	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
Sync	953	7	7	☐	-ALL-	OnNet to BaskingRidge:HQ
Sync	6965	7	7	☐	-ALL-	OnNet to BaskingRidge:Research
Sync	661	7	7	☐	-ALL-	OnNet to SanJose
Sync	538	7	7	☐	-ALL-	OnNet to Westminster
Sync	444	7	7	☐	-ALL-	OnNet to HighlandsRanch

In the details for the dial pattern, a blank **SIP Domain** indicates the pattern matches any SIP 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 routes to this particular PBX. Specific originating locations could be denied access to this dial pattern (that is, the call would be denied).



SIP service providers

This case study depicts three SIP service providers: AT&T, Verizon, and Hypothetical. AT&T is connected through one session boarder controller (though it could be connected directly) while Verizon and Hypothetical are connected through a different, though shared SBC.

For connections to SIP service providers to be useful for outgoing as well as incoming traffic, each PBX must, in addition to routing their on-net 7-digit calls, route their PSTN calls to the Session Manager core. As seen before the 7-digit calls are routed to other PBXs while the PSTN numbers are converted to E.164 and routed to SIP service providers (as seen in this section).

SIP service provider adaptations

SIP service providers typically send in digit strings formatted for the calling area in which the service is provided. In North America they may be 10- or 7-digit called and calling party

numbers. For outgoing calls (relative to the Session Manager network) they 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.

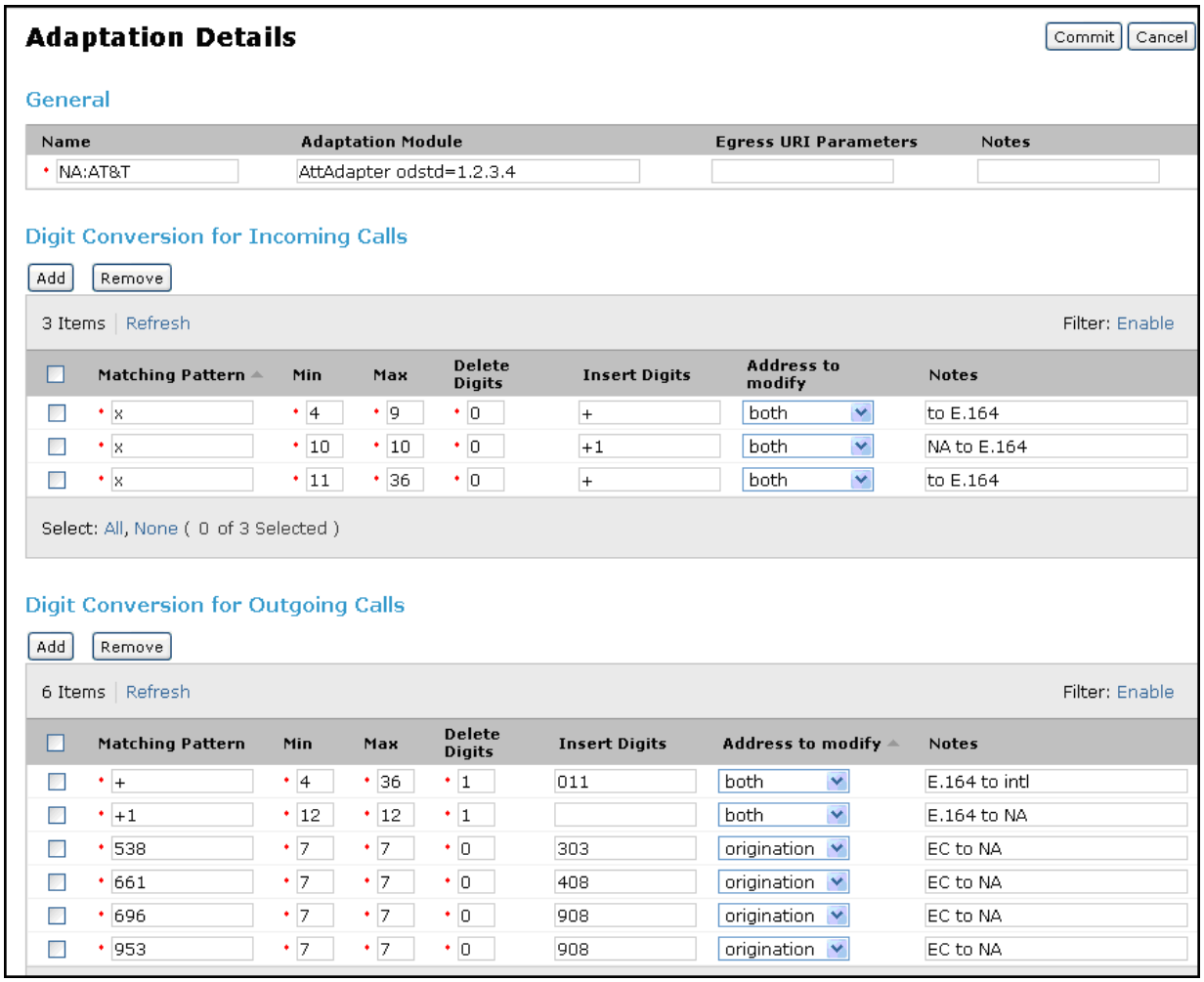
AT&T adaptation

When a request comes in from AT&T, the calling and called party numbers is 10 digits for calls originated from North America and E.164 for international calls. Session Manager converts the called party number to E.164 form.

When sending requests to AT&T, Session Manager has to convert calling and called party numbers. AT&T requires that the host part of the request-URI be their IP address (in this example, 135.9.43.69). The called party number must be sent in the request-URI as either 011+ digits for international calls or as a 10-digit North American number. The calling party number must be sent as a 10-digit number.

This adaptation uses the AttAdapter, which does digit conversion and strips the History-Info header from requests, as the AT&T network is not compatible with this header that is used by Communication Manager. The IP address supplied by AT&T must be specified as a parameter

to convert the host-part of the request-URI. Thus, the text to enter in the Adaptation Module box is AttAdapter odstd=135.9.43.69.



Adaptation Details Commit Cancel

General

Name	Adaptation Module	Egress URI Parameters	Notes
* NA:AT&T	AttAdapter odstd=1.2.3.4		

Digit Conversion for Incoming Calls

Add Remove

3 Items | Refresh Filter: Enable

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
* x	* 4	* 9	* 0	+	both	to E.164
* x	* 10	* 10	* 0	+1	both	NA to E.164
* x	* 11	* 36	* 0	+	both	to E.164

Select: All, None (0 of 3 Selected)

Digit Conversion for Outgoing Calls

Add Remove

6 Items | Refresh Filter: Enable

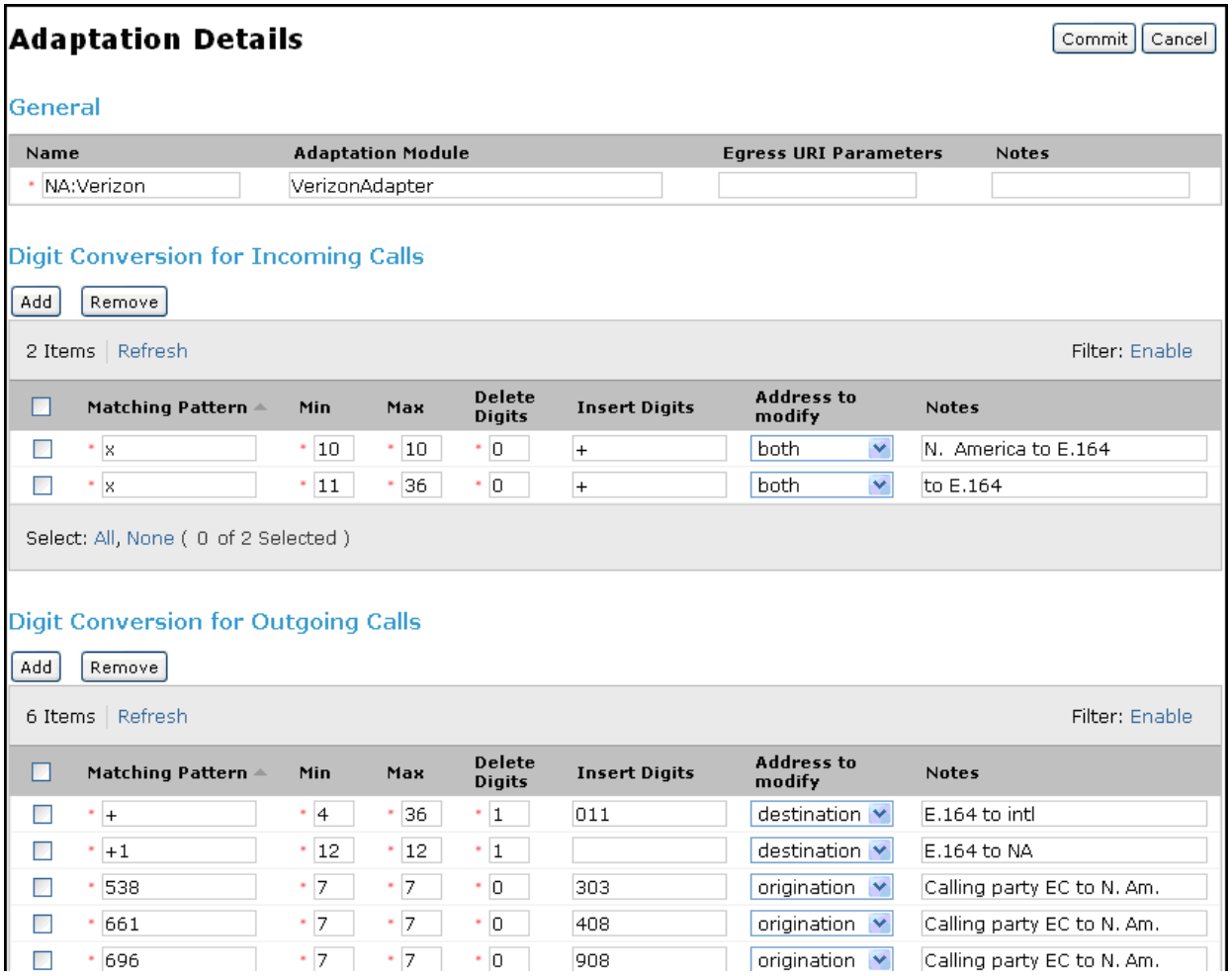
Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
* +	* 4	* 36	* 1	011	both	E.164 to intl
* +1	* 12	* 12	* 1		both	E.164 to NA
* 538	* 7	* 7	* 0	303	origination	EC to NA
* 661	* 7	* 7	* 0	408	origination	EC to NA
* 696	* 7	* 7	* 0	908	origination	EC to NA
* 953	* 7	* 7	* 0	908	origination	EC to NA

Verizon adaptation

Verizon adaptation is similar to AT&T adaptation, with these differences:

- Verizon uses the VerizonAdaptation adaptation module. This module does digit conversion and converts the History-Info header to a Diversion header and vice-versa.
- In this case study the Verizon connection and the following Hypothetical service provider connection is done through a common session border controller (SBC). The conversion of

the domain in the SIP message request URI to the IP address of the Verizon gateway is handled by the SBC.



Adaptation Details — Commit | Cancel

General

Name	Adaptation Module	Egress URI Parameters	Notes
* NA:Verizon	VerizonAdapter		

Digit Conversion for Incoming Calls

Add | Remove

2 Items | Refresh — Filter: Enable

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
* x	* 10	* 10	* 0	+	both	N. America to E.164
* x	* 11	* 36	* 0	+	both	to E.164

Select: All, None (0 of 2 Selected)

Digit Conversion for Outgoing Calls

Add | Remove

6 Items | Refresh — Filter: Enable

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
* +	* 4	* 36	* 1	011	destination	E.164 to intl
* +1	* 12	* 12	* 1		destination	E.164 to NA
* 538	* 7	* 7	* 0	303	origination	Calling party EC to N. Am.
* 661	* 7	* 7	* 0	408	origination	Calling party EC to N. Am.
* 696	* 7	* 7	* 0	908	origination	Calling party EC to N. Am.

Hypothetical adaptation

The basic DigitConversionAdapter may suffice for adapting connectivity to other SIP service providers. Alternatively, some adaptation functions could be provided by an external SBC which is used in this particular case study, leaving the DigitConversionAdapter to simply convert digit fields in the SIP message.

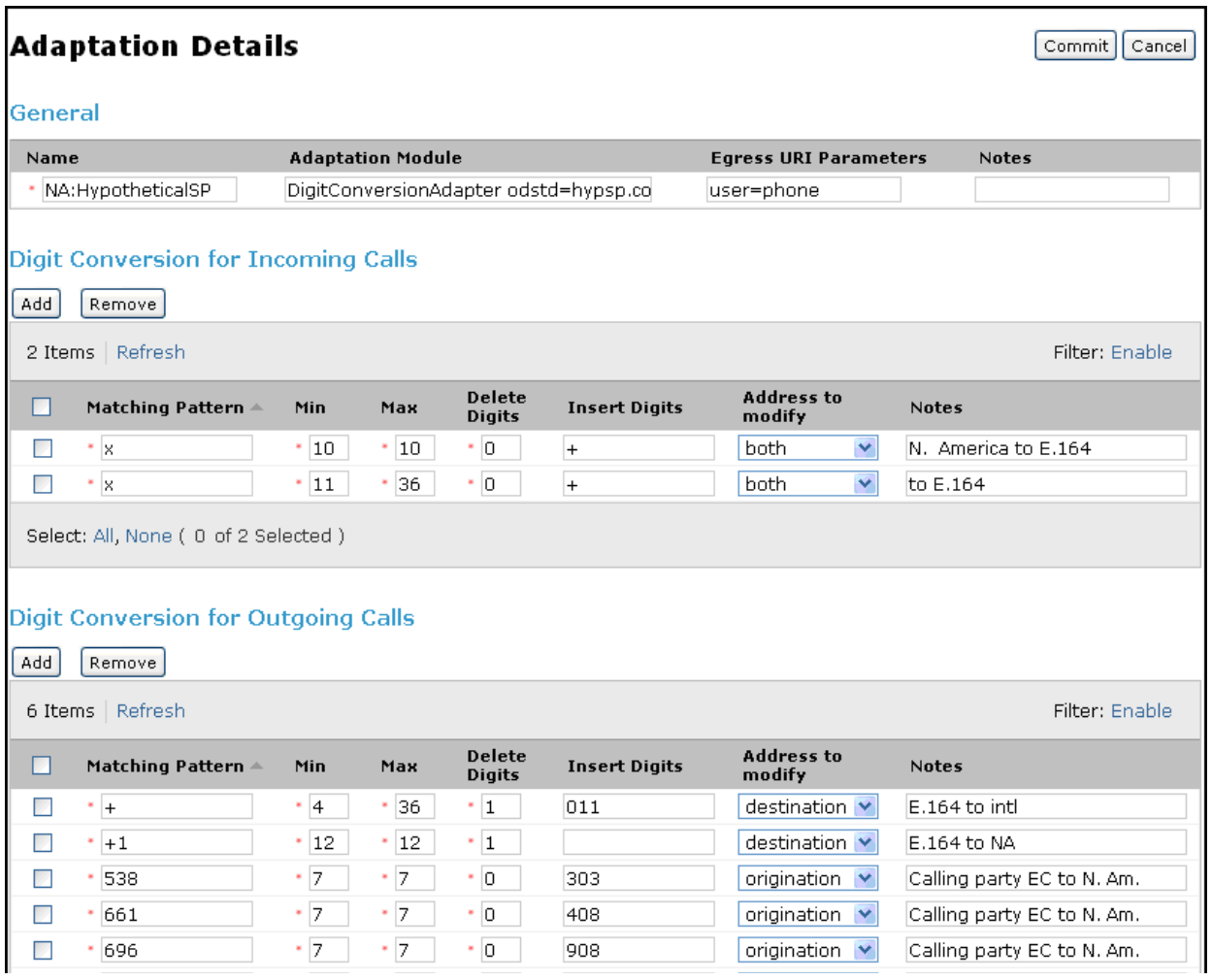
When a request comes in from Hypothetical, the calling and called party numbers are 10 digits for calls originated from North America and E.164 for international calls. Session Manager converts the called party number to the E.164 form.

When sending requests to Hypothetical, Session Manager has to convert calling and called party numbers. Hypothetical requires that the host part of the request-URI be "hyposp.com" and that DNS be used to locate the correct server. The called party number must be sent in the

request-URI as either 011+ digits for international calls or as a 1+10 digit North American number. The calling party number must be sent as a 10-digit number.

When calls originate from one of the PBXs, the calling party numbers are in the enterprise-canonical format. On egress to Hypothetical, these numbers must be converted to 10-digit North American numbers. The **Digit Conversion for Outgoing Calls** table below has been set up to do this. The choice of the origination address in the **Address to modify** column indicates that only calling party numbers (in the P-Asserted-Identity header) of the request is modified. The choice of the destination in the rule that converts E.164 to North American format indicates that only the Request-URI is modified.

This adaptation uses the DigitConversionAdapter. The "hyposp.com" domain must be specified as a parameter to convert the host-part of the request-URI. Also, Hypothetical requires the 'user=phone' parameter in the request-URI. This is entered in the **Egress URI Parameters** box on the form.



Adaptation Details

Commit Cancel

General

Name	Adaptation Module	Egress URI Parameters	Notes
* NA:HypotheticalSP	DigitConversionAdapter odstd=hypsp.co	user=phone	

Digit Conversion for Incoming Calls

Add Remove

2 Items | Refresh Filter: Enable

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
* x	* 10	* 10	* 0	+	both	N. America to E.164
* x	* 11	* 36	* 0	+	both	to E.164

Select: All, None (0 of 2 Selected)

Digit Conversion for Outgoing Calls

Add Remove

6 Items | Refresh Filter: Enable

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
* +	* 4	* 36	* 1	011	destination	E.164 to intl
* +1	* 12	* 12	* 1		destination	E.164 to NA
* 538	* 7	* 7	* 0	303	origination	Calling party EC to N. Am.
* 661	* 7	* 7	* 0	408	origination	Calling party EC to N. Am.
* 696	* 7	* 7	* 0	908	origination	Calling party EC to N. Am.

Note that the **Adaptation Module** and **Egress URI Parameters** fields allow free format text. These fields scroll horizontally so their complete values may not show on the form without

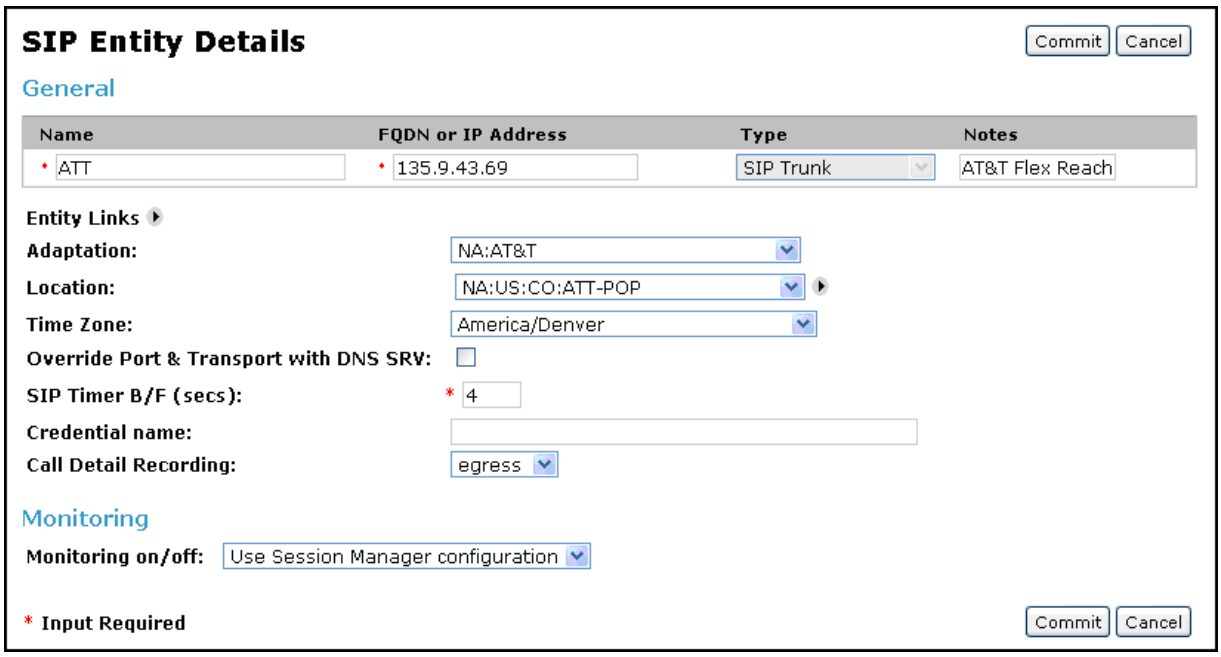
active selection and scrolling (as seen in this particular example). Additionally, the system does not validate the values in these fields, so enter these values carefully.

SIP entities for SIP service providers

SIP service provider connections differ from edge PBXs in various ways. Normally they are connected through session border controllers, and they require call detail recording. In this case study there are three SIP service provider connections: one, AT&T, is connected through a dedicated SBC while the other two, Hypothetical and Verizon, share an SBC. Other minor differences are highlighted.

Single SIP entity behind SBC

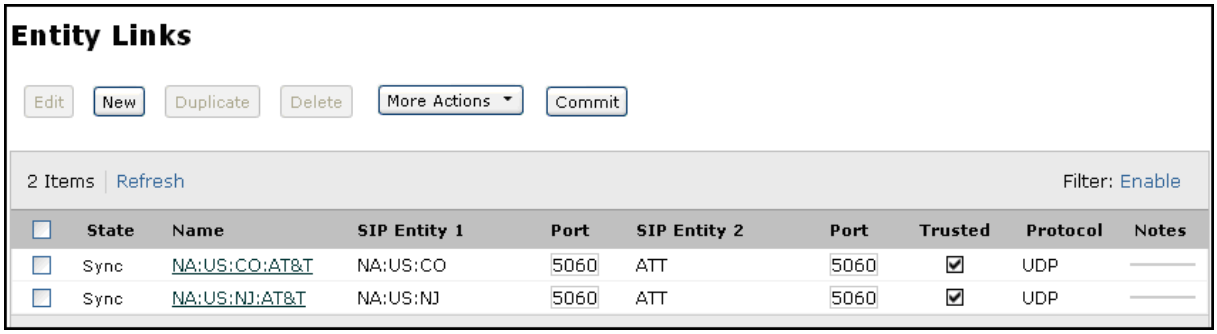
A single connection behind an SBC has the characteristic that the IP address of the SBC can be considered to represent the one and only SIP entity behind it. There is no reason to distinguish messages coming from the SBC from those intended for the SIP entity. The SIP entity configuration looks similar to that of any other SIP entity.



In this example the IP address of the SBC is used. The **Type** is marked SIP Trunk for categorization.

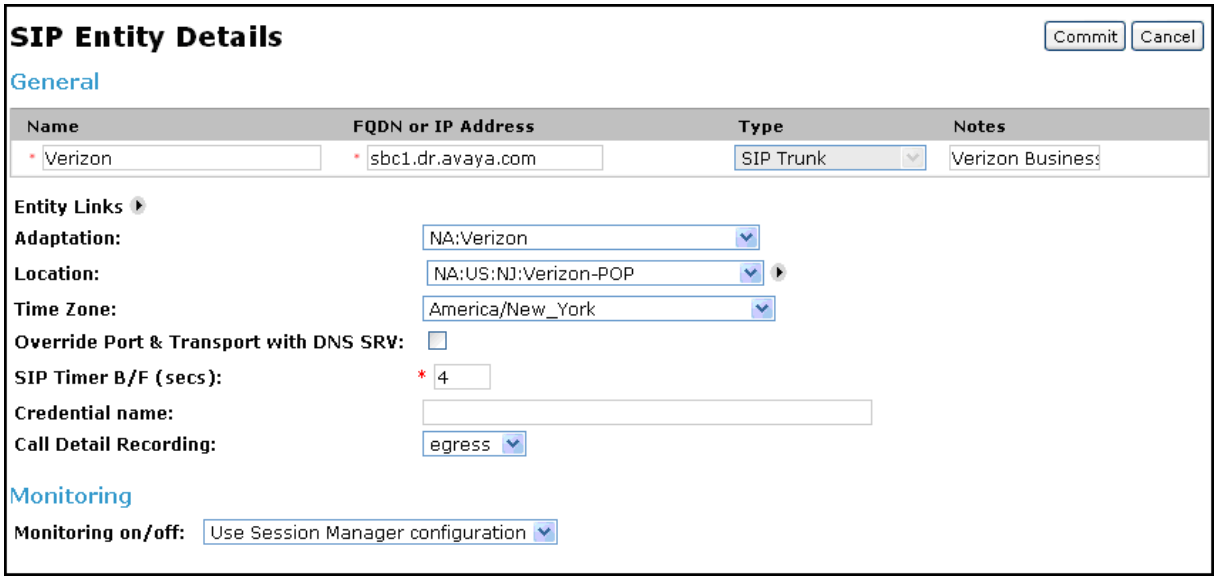
The **Call Detail Recording:** field is set at egress, meaning that all sessions established out to this SIP entity are recorded. Incoming sessions are not recorded, unless they route out to a SIP entity that is marked for **egress** or **both** CDR recording.

Again, an entity link must be created for each Session Manager to this SIP entity, in this case UDP is the Protocol used, though the SBC could be used to translate the UDP supported by AT&T to TCP. The SBC must also be willing to accept messages from each Session Manager and route messages to either Session Manager (in case of network or Session Manager failure).

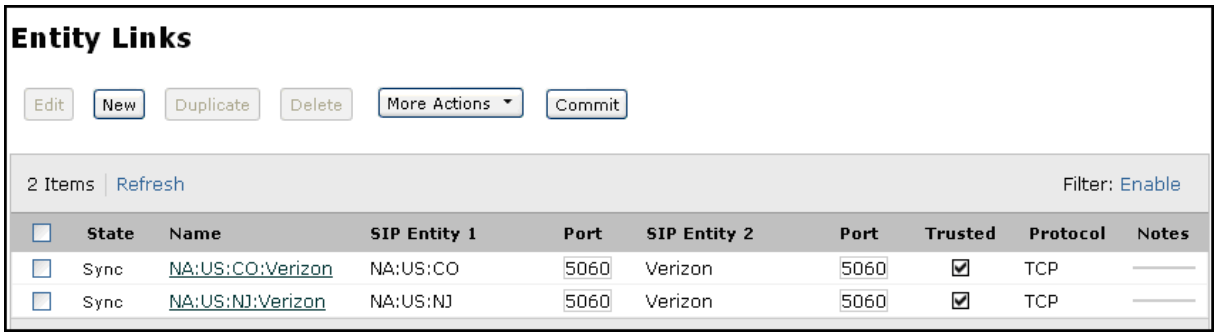


Multiple SIP entities behind SBC

In this example, both the Verizon and Hypothetical service providers are behind an SBC at an IP address specified by an FQDN. We do not have an entry in the Local Host Name Resolution table for this. The Session Manager goes to the network's DNS server to resolve the IP address.



The entity links specified for this SIP entity use the standard ports for TCP.



Entity Links

Edit | New | Duplicate | Delete | More Actions | Commit

2 Items | Refresh | Filter: Enable

	State	Name	SIP Entity 1	Port	SIP Entity 2	Port	Trusted	Protocol	Notes
☐	Sync	NA:US:CO:Verizon	NA:US:CO	5060	Verizon	5060	☑	TCP	
☐	Sync	NA:US:NJ:Verizon	NA:US:NJ	5060	Verizon	5060	☑	TCP	

The Hypothetical service provider's gateway, behind the SBC, is located in the same location as that of Verizon, so any bandwidth management for that location applies to both SIP entities. The time zone, used for time-of-day routing differs. Although this may sound strange (same location, but different time zone), it is an artifact of grouping them together for bandwidth management. Both, in this case study, are reached over the same physical communication link to the SBC, but behind that, their respective gateways are located in different time zones and the tariffs they specify have different rates depending upon the time zone in which the gateways are located. Additionally, Hypothetical does not support any form of SIP monitoring, so this is disabled on the SIP entity form.

SIP Entity Details Commit | Cancel

General

Name	FQDN or IP Address	Type	Notes
* HypotheticalSP	* sbc1.dr.avaya.com	SIP Trunk	

Entity Links

Adaptation: NA:HypotheticalSP

Location: NA:US:NJ:Verizon-POP

Time Zone: America/Chicago

Override Port & Transport with DNS SRV: ☑

SIP Timer B/F (secs): * 4

Credential name:

Call Detail Recording: egress

Monitoring

Monitoring on/off: Disable monitoring

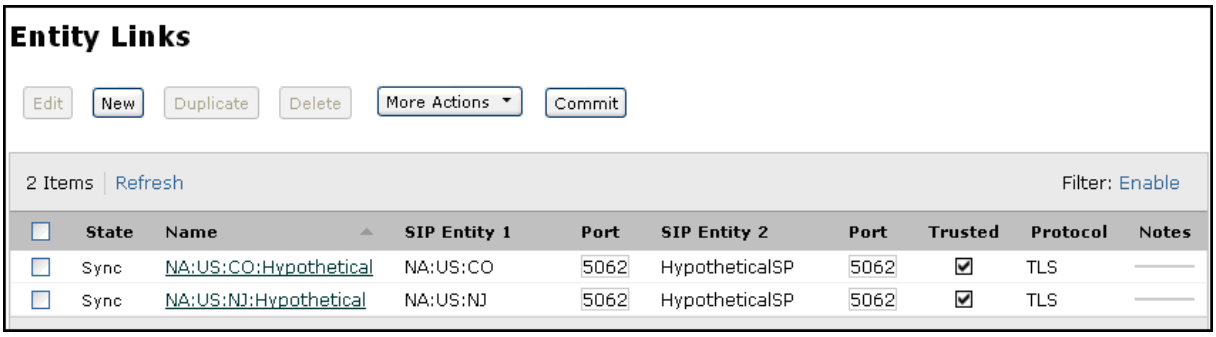
Proactive cycle time (secs): * 900

Reactive cycle time (secs): * 120

Number of Retries: * 1

The special entity link administration is what makes this configuration possible. Notice that the ports are different and nonstandard on both sides of the entity link. The SBC must be programmed to send messages from Hypothetical's gateway to port 5062 using the TLS

protocol and must be willing to accept connections to port 5062 and forward those messages to Hypothetical (the ports could have been different). Using the different ports is what allows the Session Manager to distinguish the traffic from the same SBC IP address to be from different SIP entities.



Entity Links

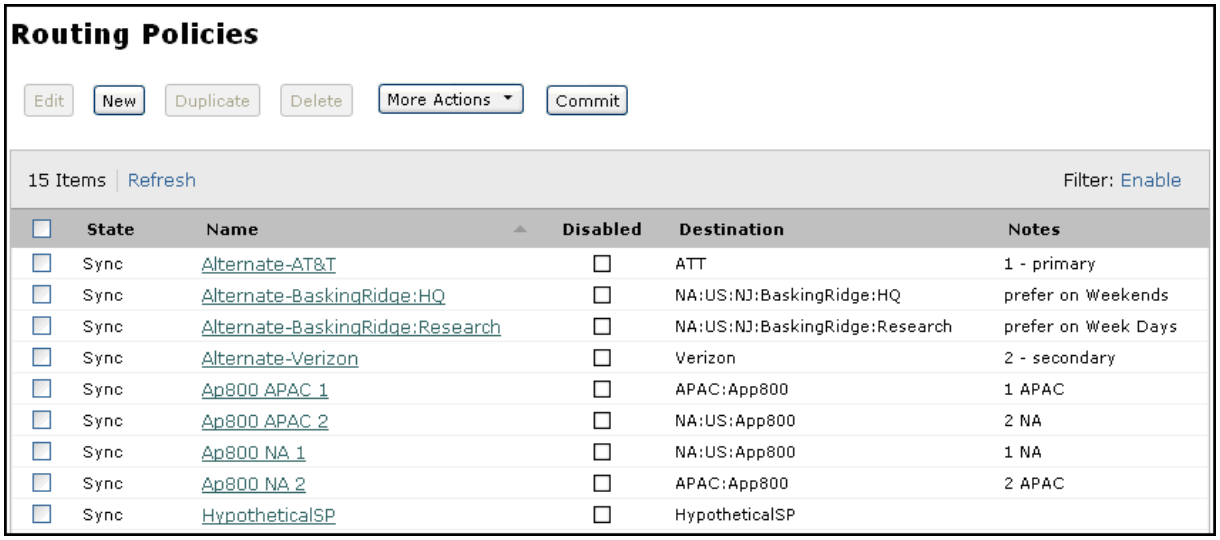
Edit | New | Duplicate | Delete | More Actions | Commit

2 Items | Refresh | Filter: Enable

State	Name	SIP Entity 1	Port	SIP Entity 2	Port	Trusted	Protocol	Notes
Sync	NA:US:CO:Hypothetical	NA:US:CO	5062	HypotheticalSP	5062	☑	TLS	
Sync	NA:US:NJ:Hypothetical	NA:US:NJ	5062	HypotheticalSP	5062	☑	TLS	

Routing policies for SIP service providers

The routing polices Alternate-AT&T, Alternate-Verizon, and HypotheticalSP are the primary policies that route to the SIP service providers. The Alternate-BaskingRidge polices are for tail-end hop-off (discussed later), and the Ap800 polices are for some SIP foundation servers (also discussed later).



Routing Policies

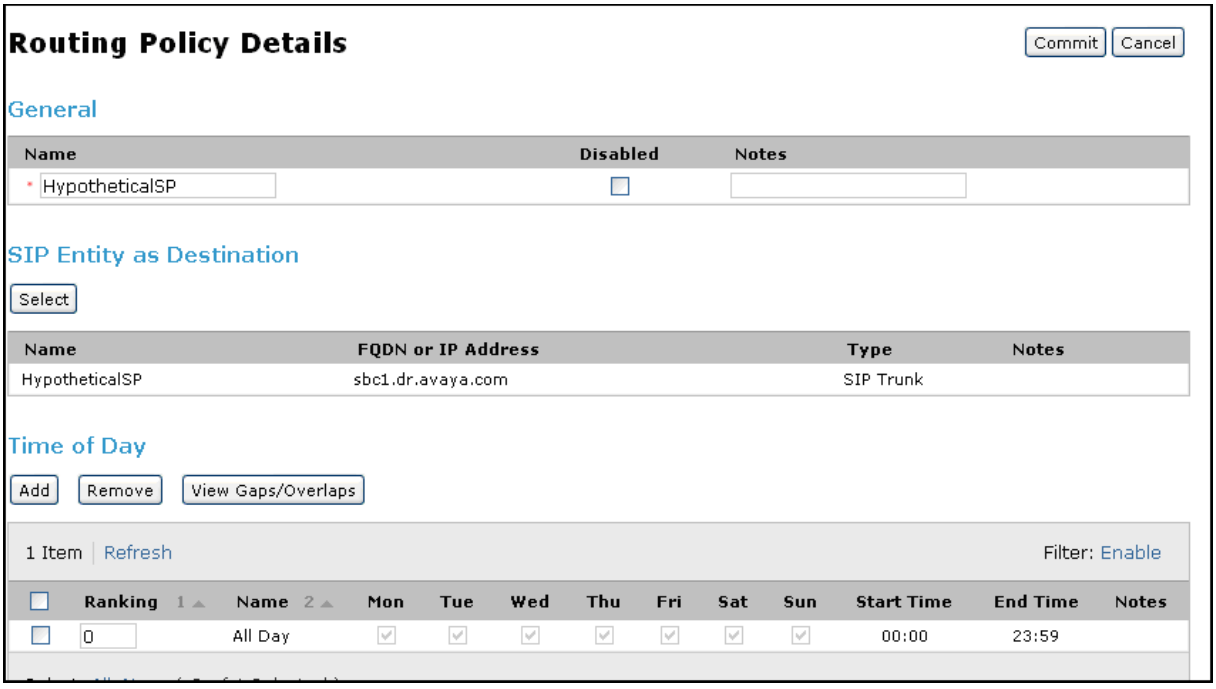
Edit | New | Duplicate | Delete | More Actions | Commit

15 Items | Refresh | Filter: Enable

State	Name	Disabled	Destination	Notes
Sync	Alternate-AT&T	☐	ATT	1 - primary
Sync	Alternate-BaskingRidge:HQ	☐	NA:US:NJ:BaskingRidge:HQ	prefer on Weekends
Sync	Alternate-BaskingRidge:Research	☐	NA:US:NJ:BaskingRidge:Research	prefer on Week Days
Sync	Alternate-Verizon	☐	Verizon	2 - secondary
Sync	Ap800 APAC 1	☐	APAC:App800	1 APAC
Sync	Ap800 APAC 2	☐	NA:US:App800	2 NA
Sync	Ap800 NA 1	☐	NA:US:App800	1 NA
Sync	Ap800 NA 2	☐	APAC:App800	2 APAC
Sync	HypotheticalSP	☐	HypotheticalSP	

Simple routing policy

The HypotheticalSP is a simple routing policy. No alternate routing to it is anticipated, so it has a single Rank 0 time of day entry. A unique dial pattern references this policy and no other.



Alternate routing policy

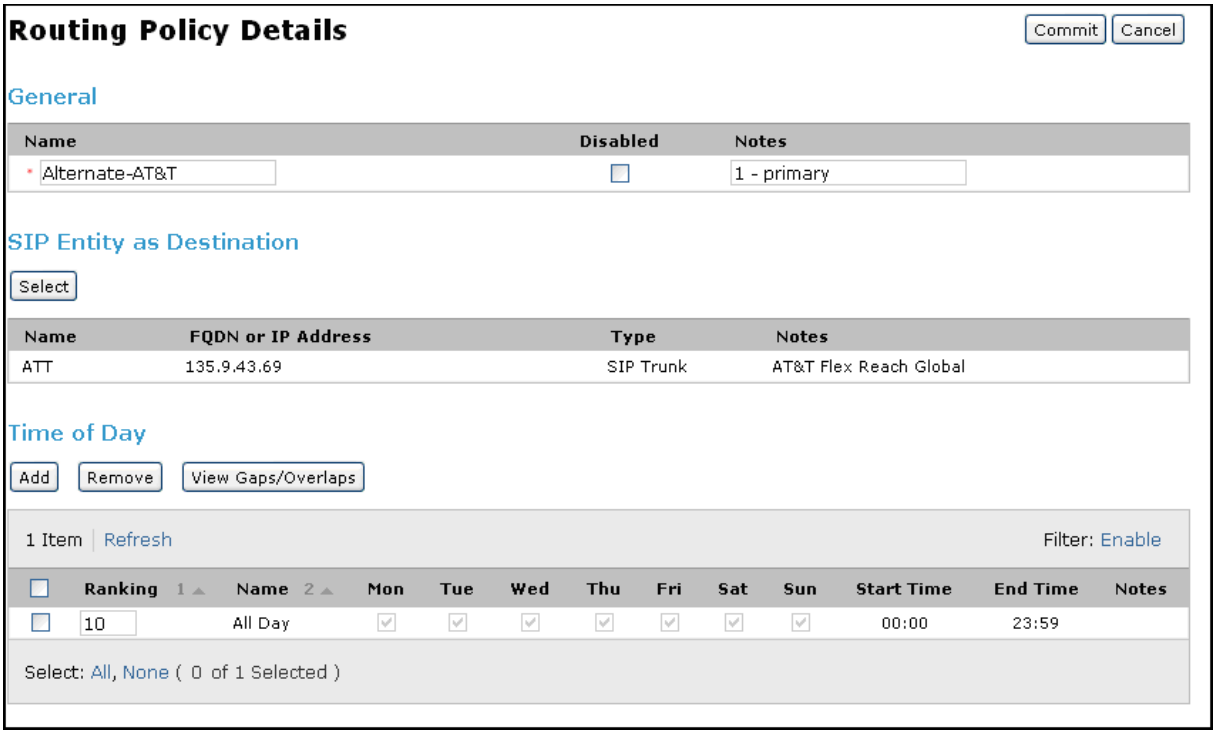
The Alternate-AT&T and Alternate-Verizon routing policies are meant to work in concert. The convention used here is to name such routing policies with the Alternate prefix and put their relative ranking in the **Notes** field. Here the Alternate-AT&T policy has a 10 ranking while the Alternate-Verizon has 20, so any dial pattern that references both of these routing policies prefers Alternate-AT&T.

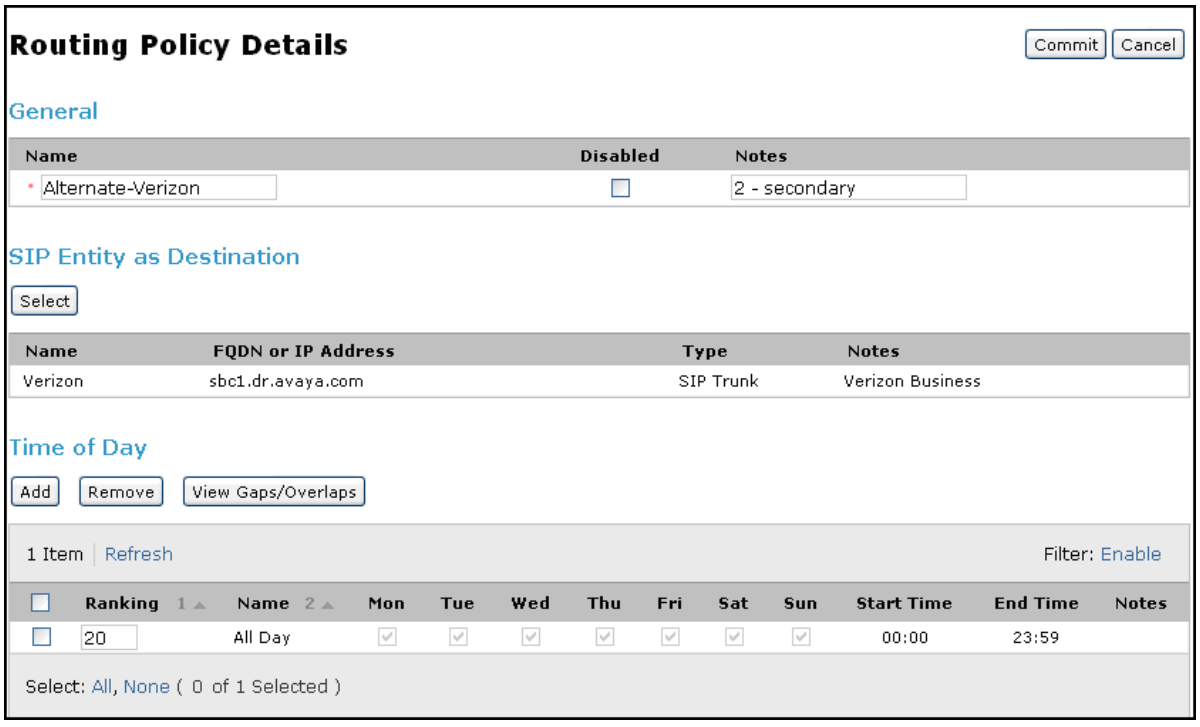
Another convention is to rank policies in increments of 10 at the start. This allows insertion of intermediately ranked policies without having to renumber all that would come later.

Note that when routing sessions, the Session Manager chooses the lower ranked routing policy for one of three reasons:

- SIP monitoring has declared all endpoints identified by the all higher ranked policies as down.
- This call fails to route (due to a bad return code or TimerB failure).

- This call fails to route due to managed bandwidth being exhausted to the destination location.





Dial patterns for SIP service providers

The E.164 dial pattern entries exist mainly because our case study network is connected to the PSTN through SIP service providers. They fall into four categories, marked in the **Notes** field:

- APP route directly to a SIP foundation server (see below). These are marked.
- TEHO for Tail-End Hop-Off (see below)
- E.164 route DID numbers from the SIP service provider to the proper PBX. The relatively low number of entries of this type result from the PBXs in question *owning* the full bank of DID numbers (for example, the Westminster PBX owns all numbers +13035380000 to +13035389999). If this were not the case, the discrepancy could be solved with more entries, either with a larger set of more explicit ones to route fewer numbers to the given PBX, or with more explicit ones that route exceptions elsewhere (like the +13035389077 entry).
- PSTN (the + entries) are very general patterns which essentially match any E.164 number not matched by a more explicit entry.

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

Note that the first + entry in the table below is distinct from the second, because it only applies if the destination has a domain of avayalabs.com, while the second pattern matches any other domain.

The four entries:

Dial Patterns

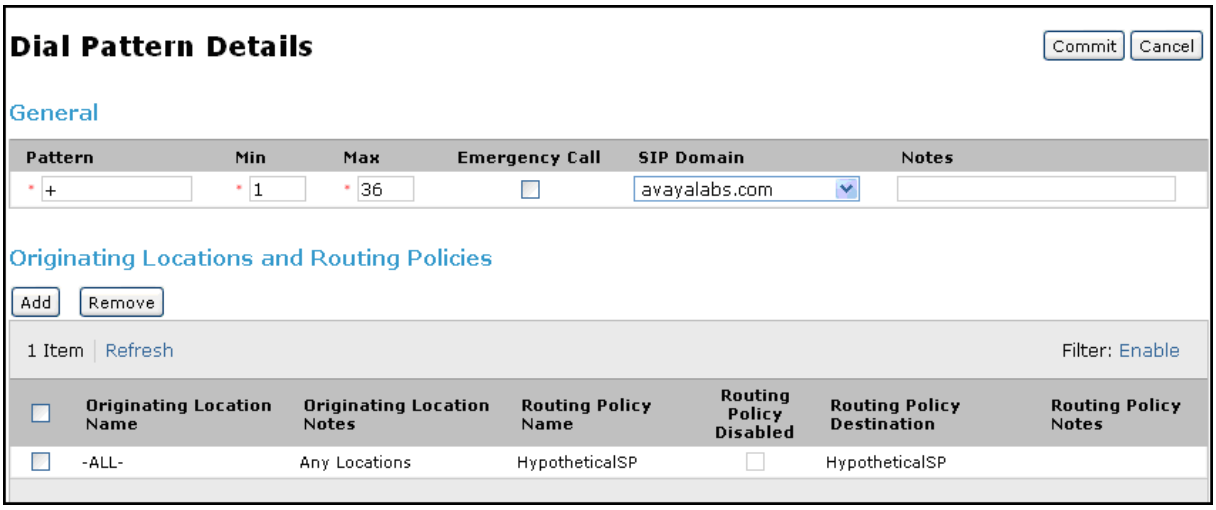
Edit | New | Duplicate | Delete | More Actions | Commit

16 Items | Refresh | Filter: Enable

	State	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
☐	Sync	+18664528292	12	12	☐	-ALL-	APP: GO AVAYA
☐	Sync	+13035389077	12	12	☐	-ALL-	APP: Modular Messaging
☐	Sync	+1908953	12	12	☐	-ALL-	E.164 to BaskingRidge:HQ
☐	Sync	+19086965	12	12	☐	-ALL-	E.164 to BaskingRidge:Research
☐	Sync	+1720444	12	12	☐	-ALL-	E.164 to HighlandsRanch
☐	Sync	+1408661	12	12	☐	-ALL-	E.164 to SanJose
☐	Sync	+1303538	12	12	☐	-ALL-	E.164 to Westminster
☐	Sync	+	1	36	☐	avayalabs.com	PSTN via SIP Service Providers
☐	Sync	+	1	36	☐	-ALL-	PSTN via SIP Service Providers
☐	Sync	+1908	12	12	☐	-ALL-	TEHO to BaskingRidge
☐	Sync	+1303	12	12	☐	-ALL-	TEHO to Westminster

Simple routing policy

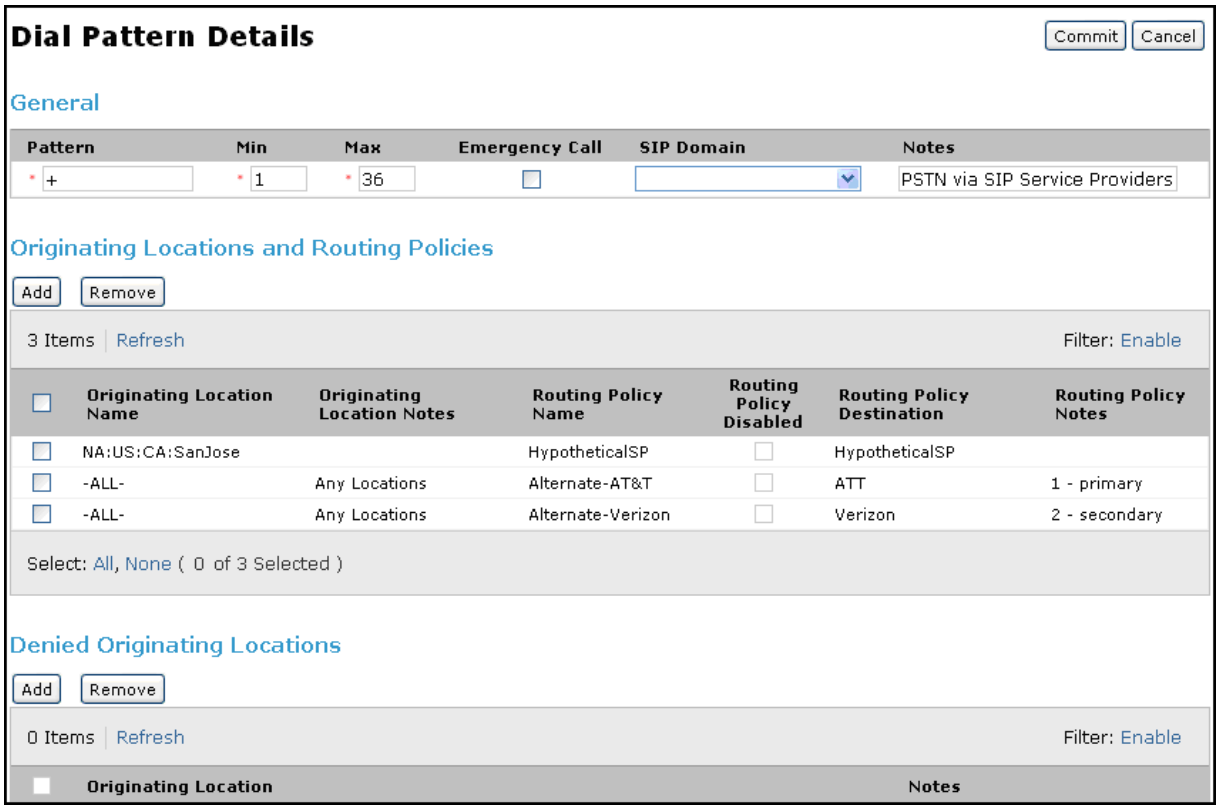
The simple case dictates that any session destined for any E.164 address with the domain avayalabs.com routes only using the HypotheticalSP routing policy. In this case study the avayalabs.com domain is used by the BaskingRidge:Research SIP entity. Therefore all E.164 numbers that do not match any of the other patterns are routed using the HypotheticalSP SIP service provider.



Alternate routing policy

This dial pattern entry performs two distinct route selections for all E.164 numbers (except those to the avayalabs.com domain). If the originating location is SanJose, then the HypotheticalSP

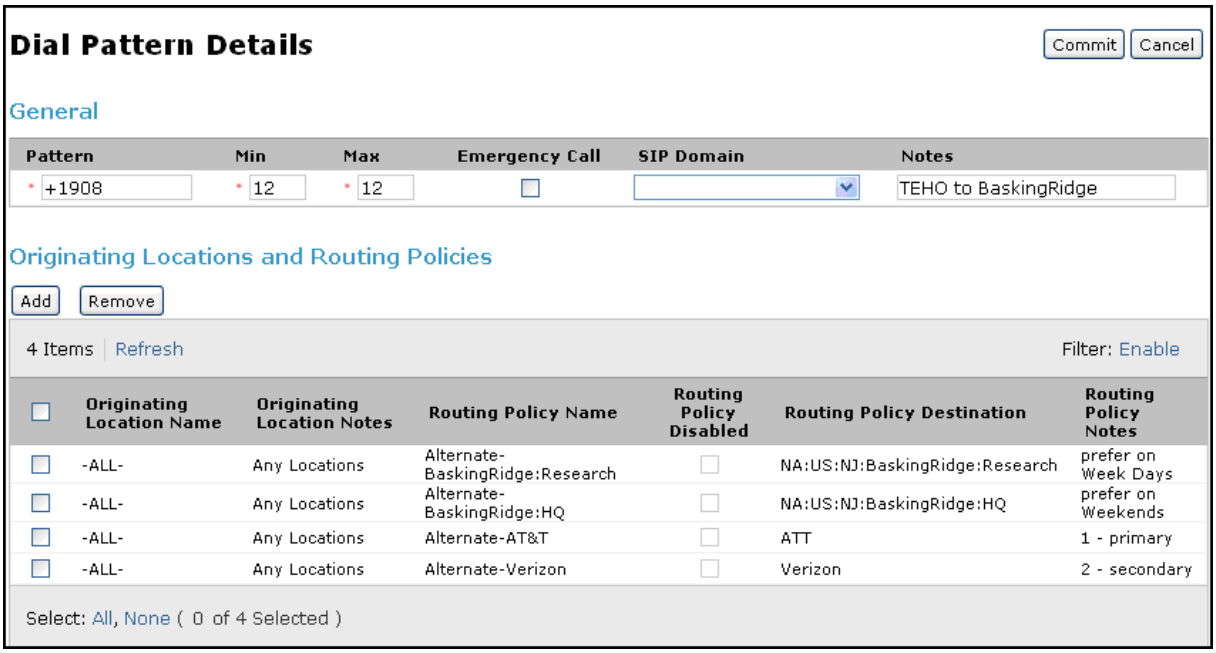
service provider is used. Any other originating location selects (using alternate routing) the Alternate-AT&T and Alternate-Verizon routing policies.



Tail-end hop-off

TEHO builds on the E.164 routing to the SIP service providers and relies on the same fundamental assumption that PBXs route their PSTN calls into the Session Manager core. Select E.164 patterns route first or exclusively to a PBX which has PSTN trunks of its own to

handle the call. In this case study both BaskingRidge PBXs can handle calls to the 908 area code. The dial pattern entry identifies one of four route policies.



Dial Pattern Details Commit Cancel

General

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
* +1908	* 12	* 12	☐		TEHO to BaskingRidge

Originating Locations and Routing Policies

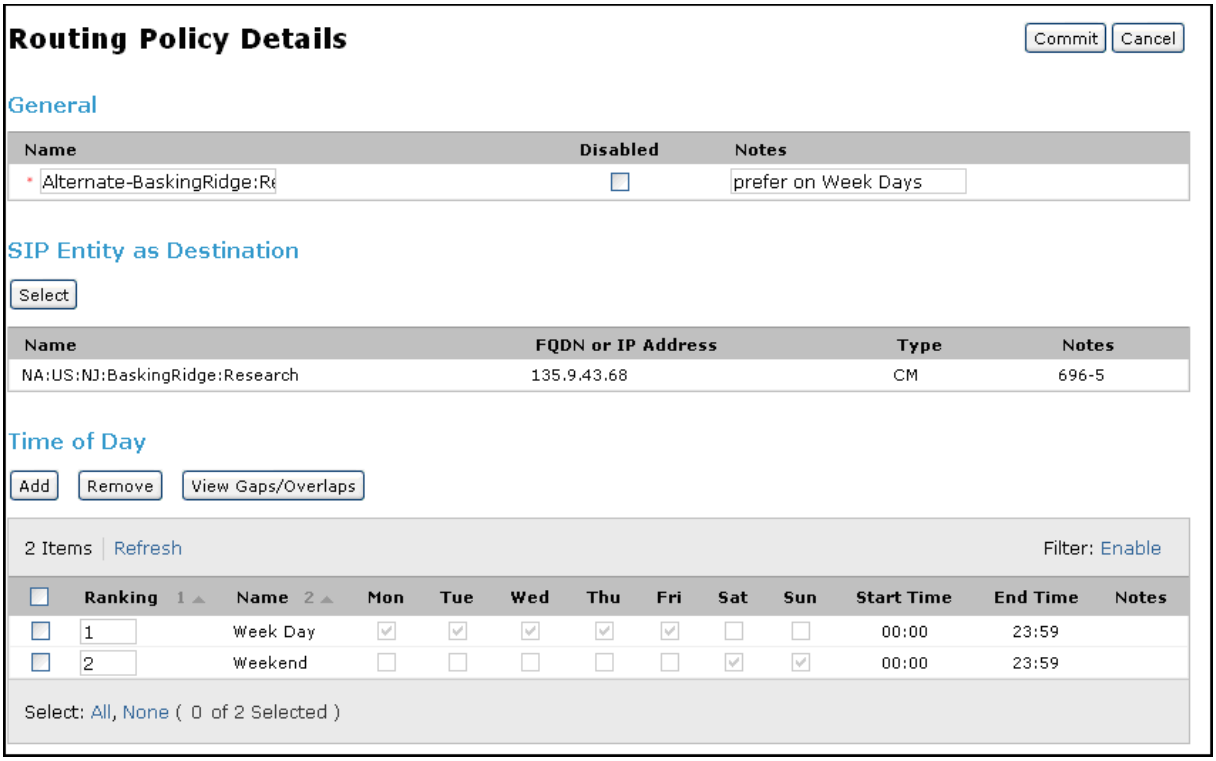
Add Remove

4 Items | Refresh Filter: Enable

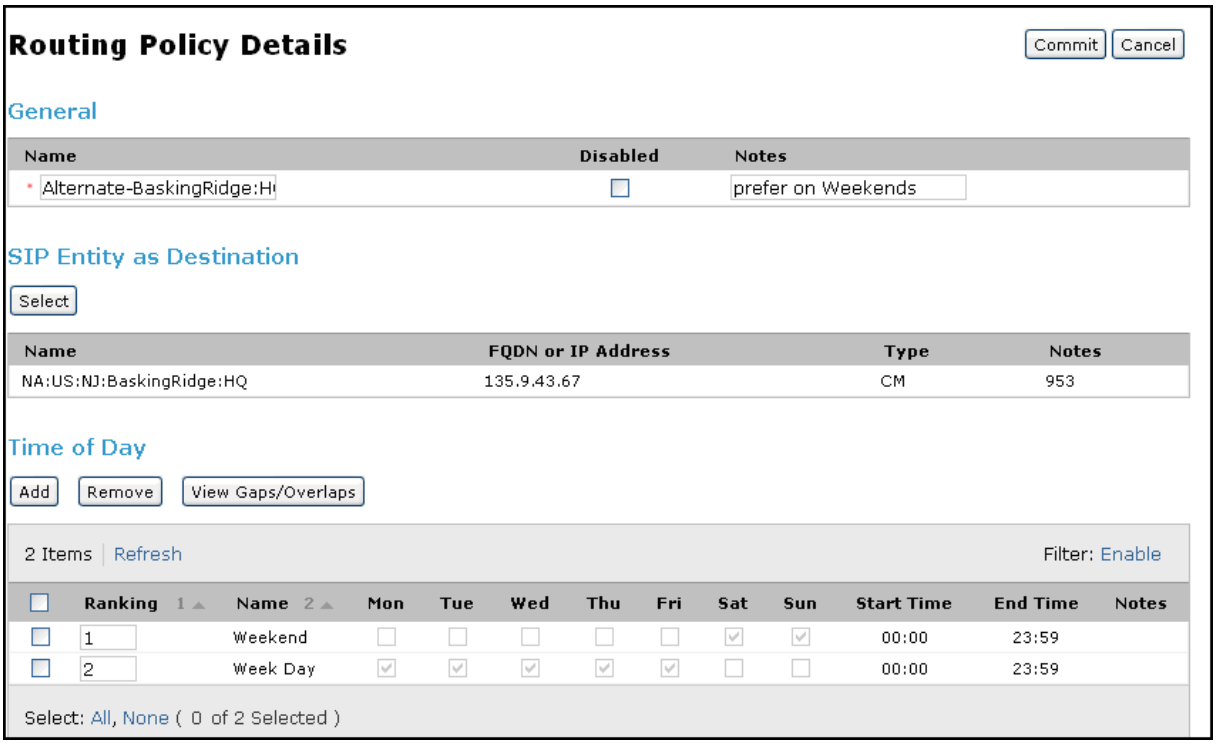
☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	Alternate-BaskingRidge:Research	☐	NA:US:NJ:BaskingRidge:Research	prefer on Week Days
☐	-ALL-	Any Locations	Alternate-BaskingRidge:HQ	☐	NA:US:NJ:BaskingRidge:HQ	prefer on Weekends
☐	-ALL-	Any Locations	Alternate-AT&T	☐	ATT	1 - primary
☐	-ALL-	Any Locations	Alternate-Verizon	☐	Verizon	2 - secondary

Select: All, None (0 of 4 Selected)

The Alternate-AT&T and Alternate-Verizon entries were shown before. They have ranks for 10 and 20, respectively. The other entries Alternate-BaskingRidge:Research and Alternate-BaskingRidge:HQ are shown below to have time-of-day varying ranks.



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.



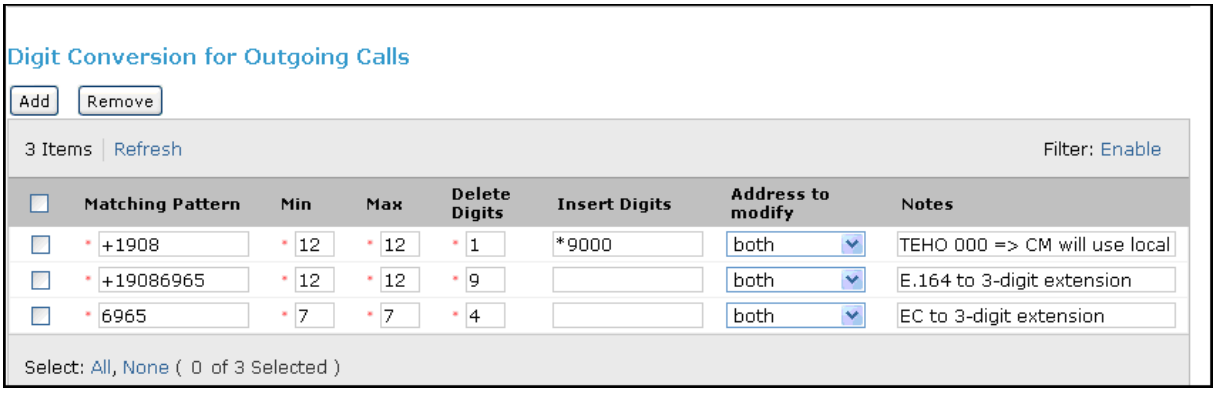
Thus the routing policy (and so SIP entity) ordering is as such:

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

It is desirable for the two BaskingRidge PBXs to be able to make use of the SIP service provider trunks even for 908 area code calls if their PSTN trunks are in use or out of service. To do this, and to make configuration of the PBXs routing simpler they route all their PSTN calls into the Session Manager core. A potential problem is when the 908 area code calls get routed back to them. If no consideration is made for this, the calls are simply routed back to the Session

Manager core only to potentially loop back into the very same PBX. To avoid this, adaptation for the PBXs changes the destination address so that the PBX can recognize it as needing routing out of its PSTN trunk rather than back into the Session Manager core.

Adaptation for BaskingRidge:Research:



The +1908 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 the case of this Communication Manager, the *9 is the ARS access code and the 000 is an otherwise nondialable digit string that can be used for this unique identification.

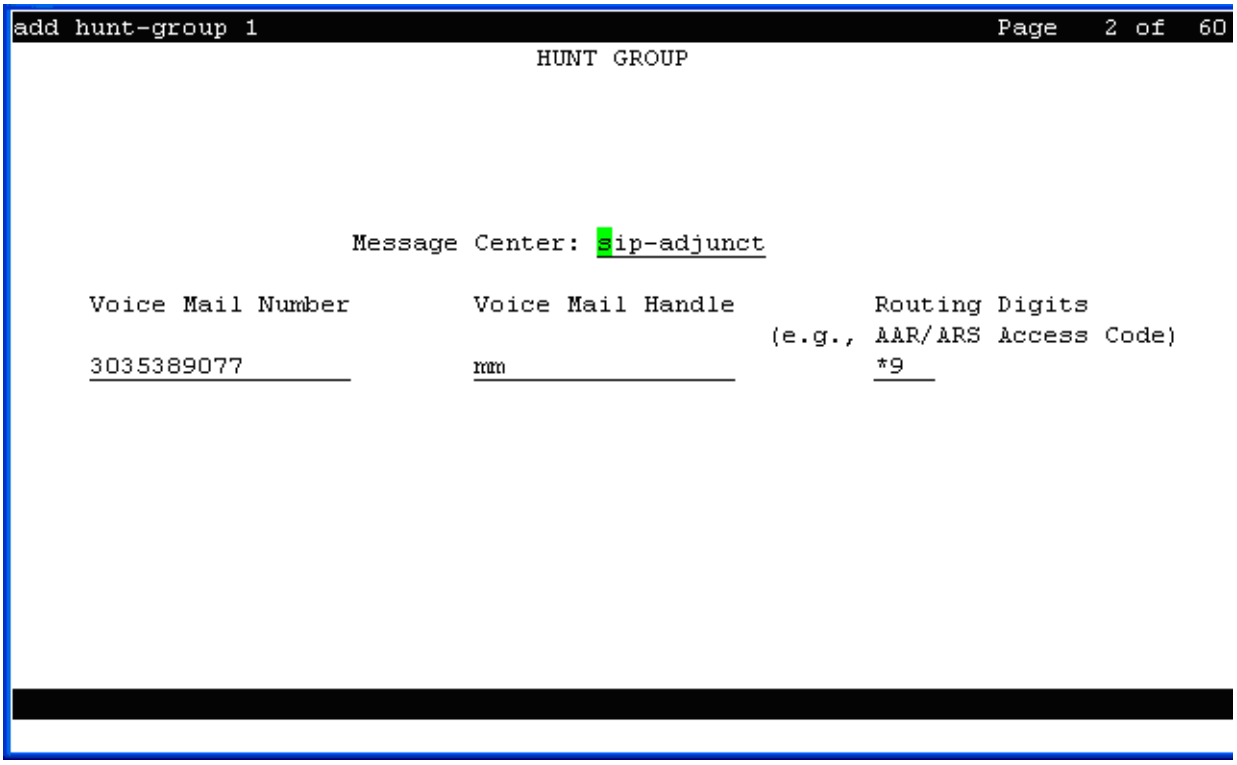
SIP foundation servers

The two SIP application types shown in this case study are Modular Messaging and Voice Portal. Both of these applications handle incoming and outgoing calls, although Modular Messaging primarily handles incoming calls. Like any SIP entity, adaptation for digit conversion can be used, but that is needed primarily for existing Modular Messaging or Voice 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.

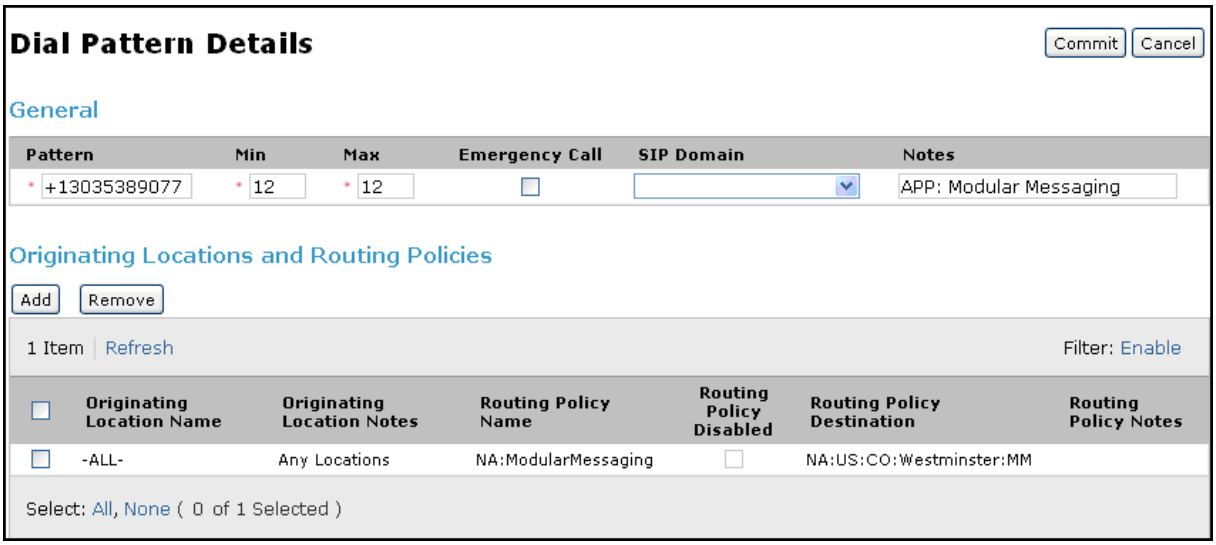
Modular Messaging

On each Communication Manager system, Modular Messaging is associated with a hunt group and assigned a routing digit string to route covered and direct sessions with media and a Voice Mail handle for message waiting indication subscriptions and notifications. Both types of sessions must be routed by Session Manager from each supported Communication Manager to the appropriate Modular Messaging system.

On the Communication Managers in this case study the following hunt group data is entered:

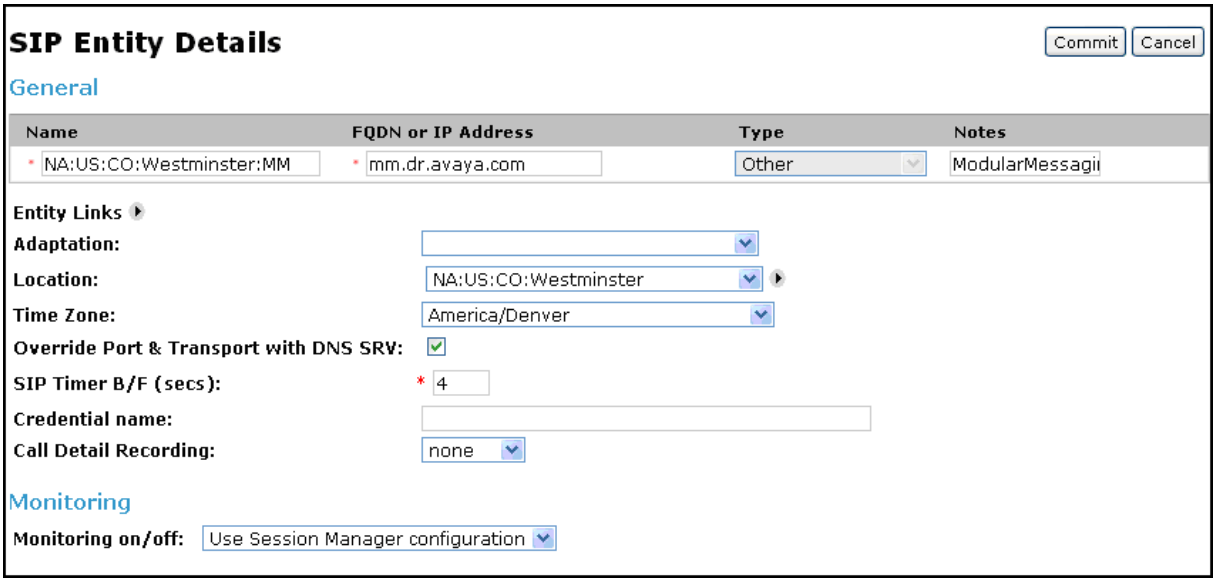


The number 3035389077 is routed through a dial pattern entry:

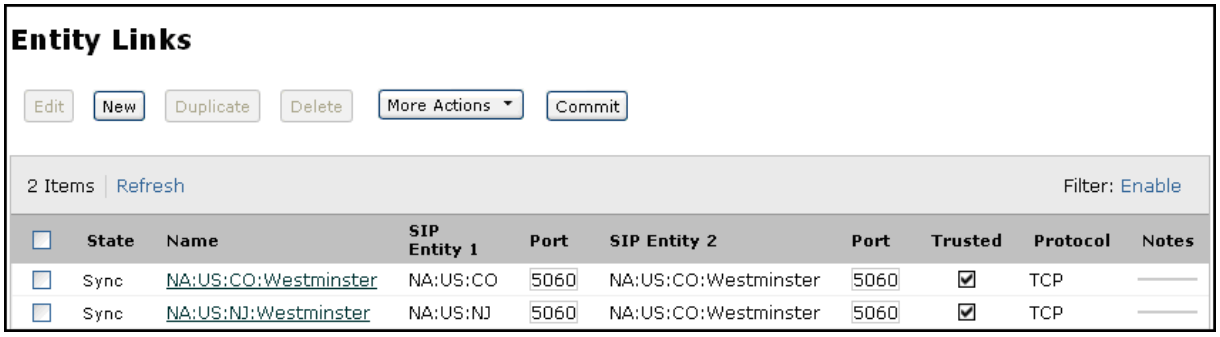


that identifies a SIP entity. CDR can be on, and it might be interesting to track calls into the Modular Messaging system, though the Modular Messaging system itself has an internal CDR capability. It may also be useful to implement bandwidth management on the Modular

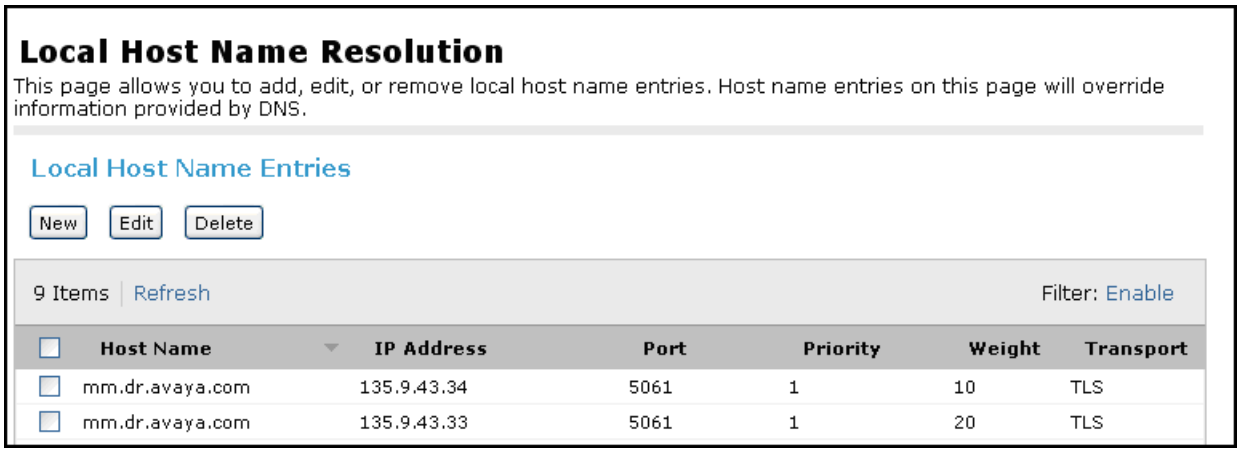
Messaging system in its own location, but it has also has a way of limiting calls. What is interesting is the load balancing between the multiple message access servers (MASs) within a Modular Messaging system. And in this particular case the local host name resolution table is used to provide the multiple IP addresses as well as the port and transport information needed to contact the MASs.



With entity links from both the Session Managers, checking the **Override Port & Transport with DNS SRV** on the SIP entity form indicates that both the Port and Protocol (aka Transport) on the SIP entity form are ignored. The convention used here is that a Port value of 1 indicates that both are ignored.

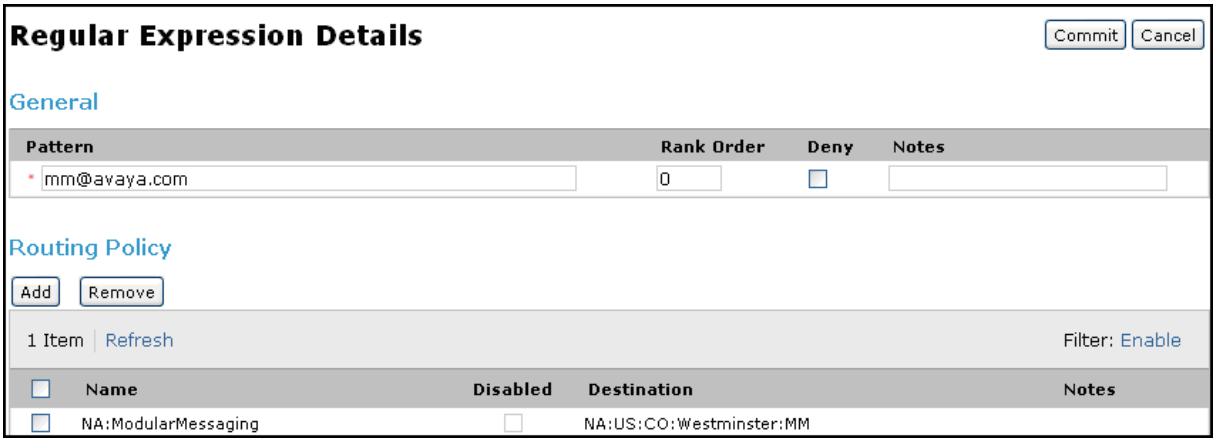


SRV records within the DNS server accessed by the Session Managers could be used to provide the necessary overridden information, but it is much easier to include this information in the **Local Host Name Resolution** table:



In this particular case TLS connections are made to port 5061 of both of the MASs at the indicated 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 given to the MAS at 135.9.43.34 while two-thirds of the calls go to the other. 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 message waiting indication subscribe and notify sessions are routed with the handle specified in Communication Manager (mm@avaya.com in this case). Handles are currently routed using the regular expressions table:

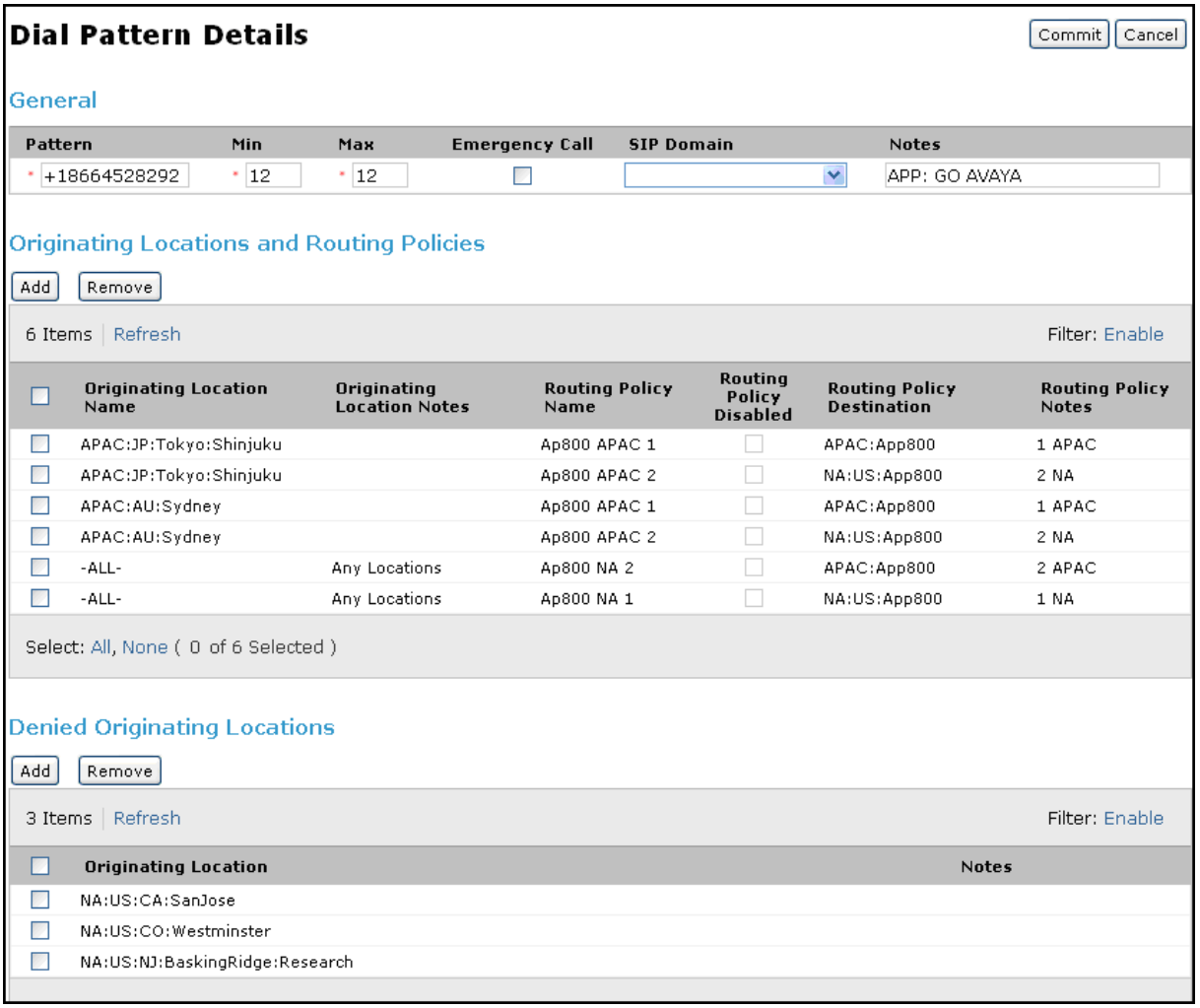


The pattern here is very precise with no meta character pattern matching symbols only because a specific handle needs to be matched. The fewer the meta characters, the more efficient the match. The routing policy selected by this match is the same one selected by the dial pattern of the number associated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

Voice Portal-like SIP application service

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

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



Dial Pattern Details Commit Cancel

General

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
* +18664528292	* 12	* 12	☐		APP: GO AVAYA

Originating Locations and Routing Policies

Add Remove

6 Items | Refresh Filter: Enable

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	APAC:JP:Tokyo:Shinjuku		Ap800 APAC 1	☐	APAC:App800	1 APAC
☐	APAC:JP:Tokyo:Shinjuku		Ap800 APAC 2	☐	NA:US:App800	2 NA
☐	APAC:AU:Sydney		Ap800 APAC 1	☐	APAC:App800	1 APAC
☐	APAC:AU:Sydney		Ap800 APAC 2	☐	NA:US:App800	2 NA
☐	-ALL-	Any Locations	Ap800 NA 2	☐	APAC:App800	2 APAC
☐	-ALL-	Any Locations	Ap800 NA 1	☐	NA:US:App800	1 NA

Select: All, None (0 of 6 Selected)

Denied Originating Locations

Add Remove

3 Items | Refresh Filter: Enable

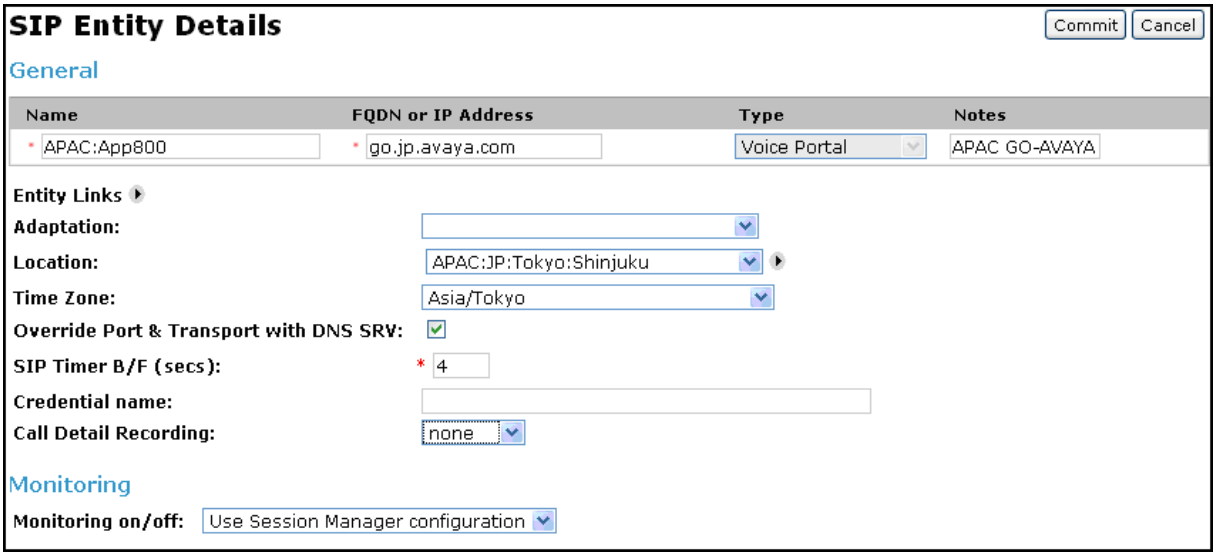
☐	Originating Location	Notes
☐	NA:US:CA:SanJose	
☐	NA:US:CO:Westminster	
☐	NA:US:NJ:BaskingRidge:Research	

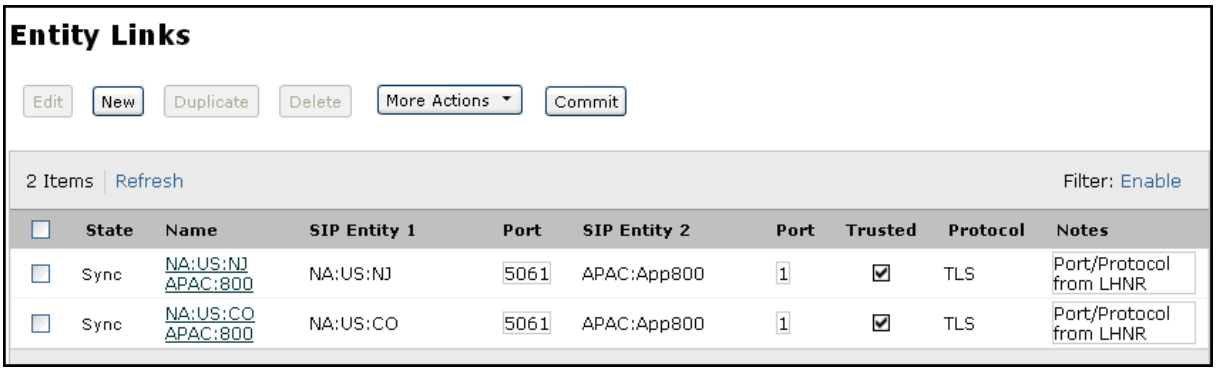
To paraphrase the routing policy selection, without actually listing the routing policies themselves:

- 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.

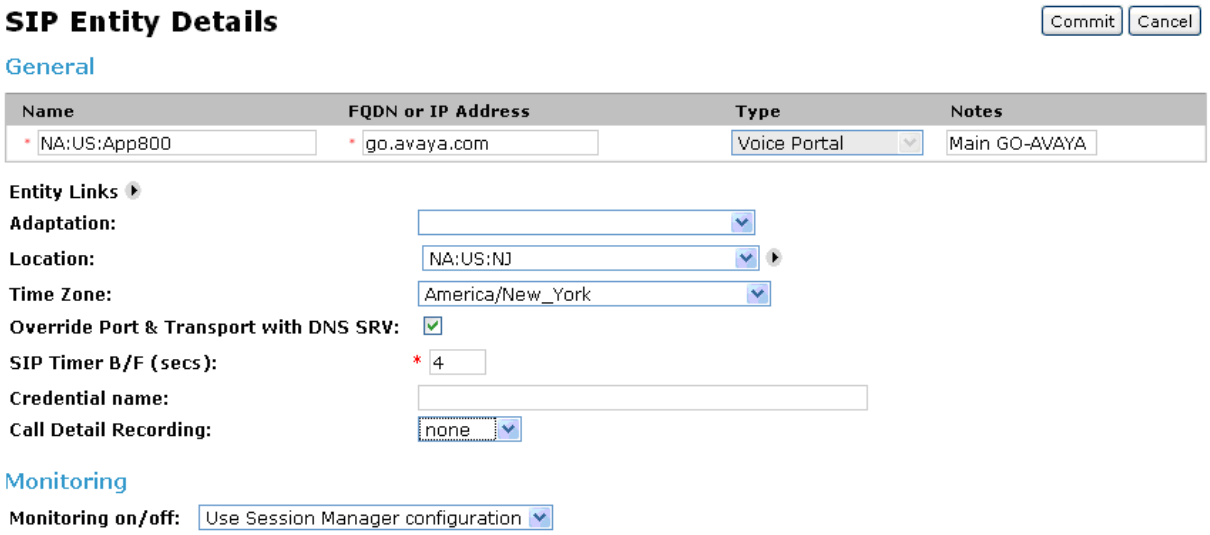
- All other SIP entities (including the ones defined in this case study PBX and SIP service provider alike) prefer the NA:US:App800 server.
- SIP entities in the SanJose, Westminster, and BaskingRidge:Research locations cannot route calls to this dial pattern. The calls are denied.

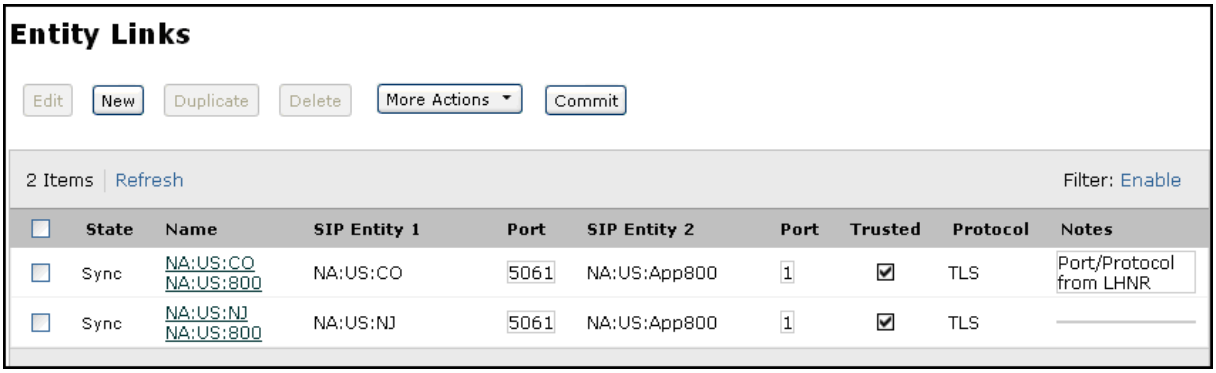
The SIP entities for the foundation servers are similar.



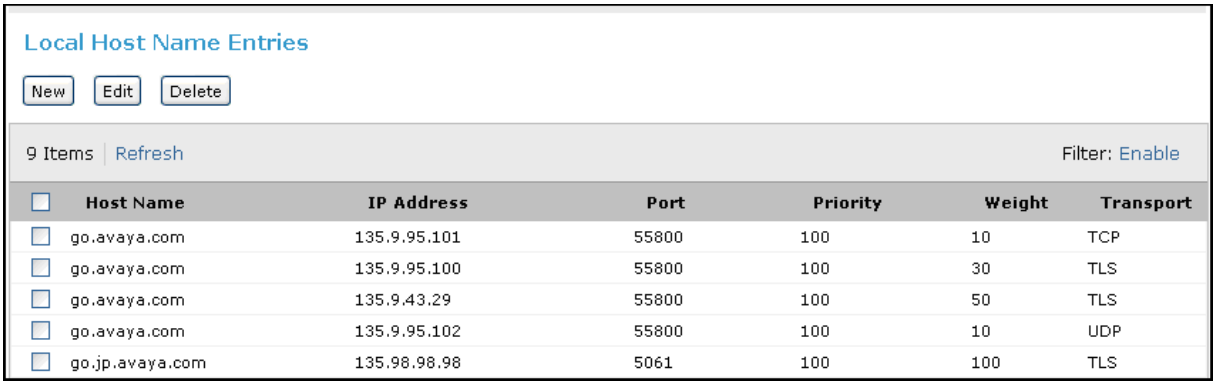


They have different FQDNs, are in different locations and time zones, but they both choose to override the port and transport specified in the entity link.





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.



Local Host Name Entries

New Edit Delete

9 Items | Refresh Filter: Enable

Host Name	IP Address	Port	Priority	Weight	Transport
go.avaya.com	135.9.95.101	55800	100	10	TCP
go.avaya.com	135.9.95.100	55800	100	30	TLS
go.avaya.com	135.9.43.29	55800	100	50	TLS
go.avaya.com	135.9.95.102	55800	100	10	UDP
go.jp.avaya.com	135.98.98.98	5061	100	100	TLS

The NA:US:App800 SIPentity chooses 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.

Index

R

S

T

U

W