Avaya Solution & Interoperability Test Lab

Configuring Cisco 7940/7960 SIP Telephones to connect to Avaya Aura® Session Manager 6.0 with Avaya Aura® Communication Manager 6.0 as a Feature Server - Issue 1.0

Abstract

These Application Notes describes the configuration steps necessary to connect Cisco 7940/7960 SIP Telephones to Avaya Aura® Session Manager with Avaya Aura® Communication Manager running as a Feature Server.

These Application Notes describe the necessary files needed in the TFTP directory and configuration settings to support loading the Cisco SIP firmware and configuration files, using the TFTP protocol, onto the Cisco SIP telephones. The sample configuration describes how the Cisco SIP telephones are configured to register with Avaya Aura® Session Manager. Administration of the Cisco SIP phones on the Avaya Aura® Session Manager is performed through the Avaya Aura® System Manager web interface. Administration of a SIP Trunk within Avaya Aura® Communication Manager Feature Server, to carry calls between Cisco SIP endpoints and Avaya SIP endpoints, is provided in the sample configuration.

Table of Contents

1. Introduction

1.1. Avaya Aura® Session Manager

Avaya Aura® Session Manager is a SIP routing and integration platform and the core component within the Avaya Aura® Enterprise Edition solution. It integrates all the SIP entities across the entire enterprise network within a company. Avaya Aura® Session Manager enables new distributed SIP-based system solutions featuring multi-vendor integration, centralized dial plans and user profiles, easier centralized SIP trunking, much easier "on-net" call routing, and greatly enhanced SIP scalability and security. This enhanced architectural flexibility allows enterprises to significantly reduce telecommunications and management costs, lower their TCO, and increase business agility by being able to more rapidly deploy appropriate Unified Communications capabilities to different user groups wherever they are.

1.2. Avaya Aura® System Manager

Central management of Avaya Aura® Session Manager is handled through the Avaya Aura® System Manager application. Avaya Aura® System Manager delivers a set of shared, secure management services and a common console across multiple products. Avaya Aura® System Manager includes the following central management services. User Management allows for the administration of users and user groups. Routing Policy is used for the administration of routing policy for all Avaya Aura® Session Manager instances within an Enterprise. Alarm Management supports alarm monitoring, acknowledgement, configuration, clearing, and retiring. The Logging Service receives log events formatted in the common log format. The Avaya Aura® Session Manager provides miscellaneous functions for Session Manager elements, including administering instances, configuring SIP firewalls, sequencing applications, monitoring SIP entities and the security module, and managing bandwidth usage. A central database that resides on the System Manager server stores all the Avaya Aura® System Manager central data, the Avaya Aura® Session Manager administration data, and the Central Data Distribution Service information. The last item is used to detect changes to the Avaya Aura® System Manager central database and then distribute these changes to the Avaya Aura® Session Manager instances.

1.3. Interoperability Testing

The objective of this interoperability test is to verify that Cisco 7940/7960 SIP telephones can interoperate with Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager 6.0 running as a Feature Server. These Application Notes reflects interoperability testing performed using the Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager 6.0 running as a Feature Server. It also includes procedures for upgrading SIP telephone firmware on Cisco 7940/7960 SIP Telephones.

Testing was performed between Cisco 7940/7960 SIP telephones and Avaya one-X® Deskphone 9630 SIP; both registered to Avaya Aura® Session Manager. Avaya Aura® Communication Manager acting as a Feature Server provided the feature services for the Avaya one-X® Deskphone 9630 SIP registered to Session Manager.

Expanded testing between Cisco 7940/7960 SIP telephones and Avaya 4621SW (H323), Avaya 6221 (Analog), and Avaya 2420 (Digital) telephones was perform by connecting the Session Manager via SIP trunk to Avaya Aura® Communication Manager acting as an Evolution Server, which supports H323, Analog, and Digital endpoints.

The interoperability testing focused on four main areas:

- The ability of the Cisco 7940/7960 SIP telephones to boot up with the correct SIP image, load the configuration files via TFTP, and register with the Session Manager.
- Basic calling using G.711 and G.729 codec's with and without shuffling. Additional test cases were executed in this area to test codec negotiation between G.711 and G.729. Interoperability between the Avaya SIP, Avaya H323, Avaya Analog, and Avaya Digital telephones with Cisco 7940/7960 SIP phones was tested using the G.711 and G.729 codec's where applicable.
- Interoperability testing between Avaya phone types and the Cisco SIP phones using the following Supplementary Calling Features:
  - Hold/Resume
  - Consultative Hold
  - Unattended Transfer
  - Attended Transfer
  - Call Forwarding All (CFA)
  - Conference Add/Drop
  - Call Waiting
  - DTMF
- Interoperability testing between the Cisco 7940/7960 SIP phones and Avaya Modular Messaging to be able to retrieve messages using the programmed Voice Mail button.

1.4. Configuration

The sample configuration consists of Avaya 96xx SIP phones and Cisco 7940/7960 SIP phones registered to Avaya Aura® Session Manager. Avaya Aura® Session Manager is connected to Avaya Aura® Communication Manager acting as a Feature Server via SIP trunk. See **Figure 1**. The Communication Manager acting as a Feature Server is used for PBX Off Station Mapping and is supplying feature sets to the Avaya SIP phones. The Communication Manager acting as a Feature Server is configured to support G.711MU, G.711A, and G.729 codec sets. The Avaya Aura® Session Manager and Avaya Aura® Communication Manager Acting as a Feature Server configuration allows Avaya SIP phones and Cisco SIP phones to call one another and function with their own call feature sets.

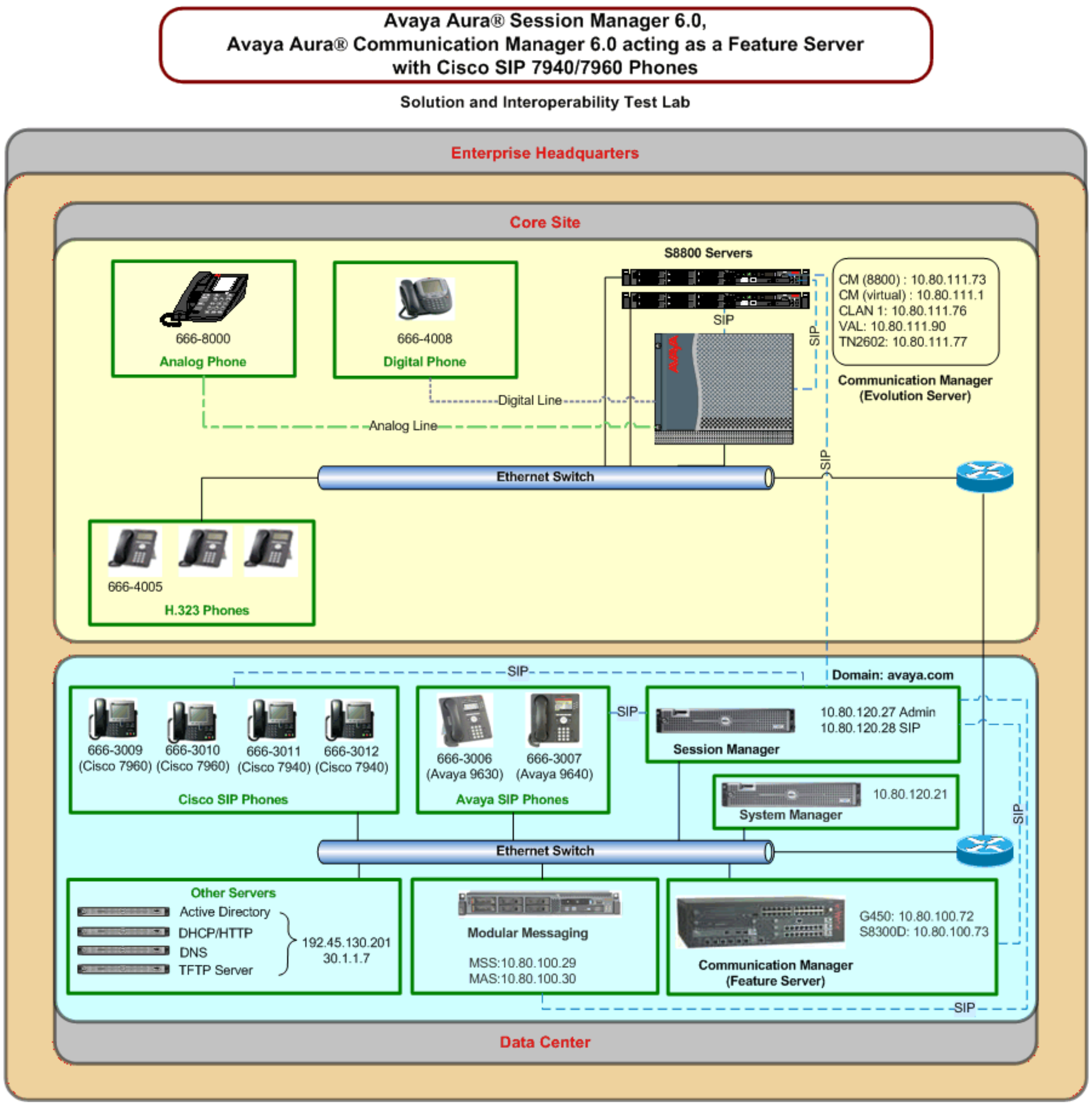


Figure 1: Sample Configuration

The test bed was extended to include Avaya Aura® Communication Manager acting as an Evolution Server connecting to Avaya Aura® Session Manager via SIP trunk to allow SIP phones (both Avaya and Cisco) to call other phone types (H323, Analog, and Digital). The H323, Analog, and Digital phones are configured and registered to Communication Manager acting as an Evolution Server. This additional configuration allows interoperability testing between the Cisco 7940/7960 SIP phones and the Avaya H323, Analog, and Digital phone sets. The additional configuration between Session Manager and Communication Manager acting as an Evolution Server is assumed to already be in place, setup and configuration for this section can be found in additional Application Notes referenced at the end of this document. The configuration of Session Manager working with Communication Manager acting as a Feature Server will be covered in this Application Note.

The Cisco 7940/7960 SIP phones are configured to boot using DHCP to configure their network addressing and receive Option 150 TFTP setting; allowing them to download the SIP phone image and configuration files from the designated TFTP server.

Station Number	Phone Type	First Name	Last Name	Location	Note
6663006	Avaya 9630 SIP	Avaya SIP	9630-1	HQ	
6663007	Avaya 9640 SIP	Avaya SIP	9640-1	HQ	
6663009	Cisco 7960 SIP	Cisco SIP	7960-1	Location 1 Subnet 10.80.60.x	Use Avaya Phone Type 9630 SIP MAC: 0003e311f2d1
6663010	Cisco 7940 SIP	Cisco SIP	7940-1	Location 1 Subnet 10.80.60.x	Use Avaya Phone Type 9630 SIP MAC : 000d28c20f7e
6663011	Cisco 7960 SIP	Cisco SIP	7960-2	Location 1 Subnet 10.80.60.x	Use Avaya Phone Type 9630 SIP MAC:
6663012	Cisco 7940 SIP	Cisco SIP	7940-2	Location 1 Subnet 10.80.60.x	Use Avaya Phone Type 9630 SIP MAC:

Table 1: SIP Phone Extensions

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Hardware Component	Software/Firmware Version
S8800 Media Server	Session Manager 6.0.0.0.600020
	System Manager 6.0 Build No. 6.0.0.0.556-3.0.6.1
S8300D Server with G450 Media Gateway	Avaya Aura® Communication Manager 6.0 acting as a Feature Server (R016x.00.0345.0) Patch 1002
S8800 Server with G650 Media Gateway	Avaya Aura® Communication Manager 6.0 acting as an Evolution Server (R016x.00.0.345.0) Patch 1002
Avaya Modular Messaging (MAS)	5.2, Build 9.2.150.0 (Patch 8 - 9.2.150.13)
Avaya Modular Messaging (MSS)	5.2, Build 5.2-11.0
Avaya one-X® Deskphone 9630 IP Telephones (SIP)	2.6.0
Avaya 4621SW IP Telephones (H.323)	S2.9.1
Avaya 6221 Analog Telephones	--
Avaya 2420 Digital Phones	--
Cisco 7940 (SIP)	P0S3-8-12-00
Cisco 7960 (SIP)	P0S3-8-12-00
Dell Servers: DHCP/HTTP DNS Active Directory TFTP	Windows Server 2008 R2 Standard

3. Configuration

The sample configuration used in these Application Notes will focus on configuring the Cisco 7940/7960 SIP phones to load the correct Cisco SIP firmware and download the configuration files necessary to register via SIP with the Session Manager. The sample configuration will also address the necessary administration used to configure the following components in the "Data Center" (**Figure 1**) including:

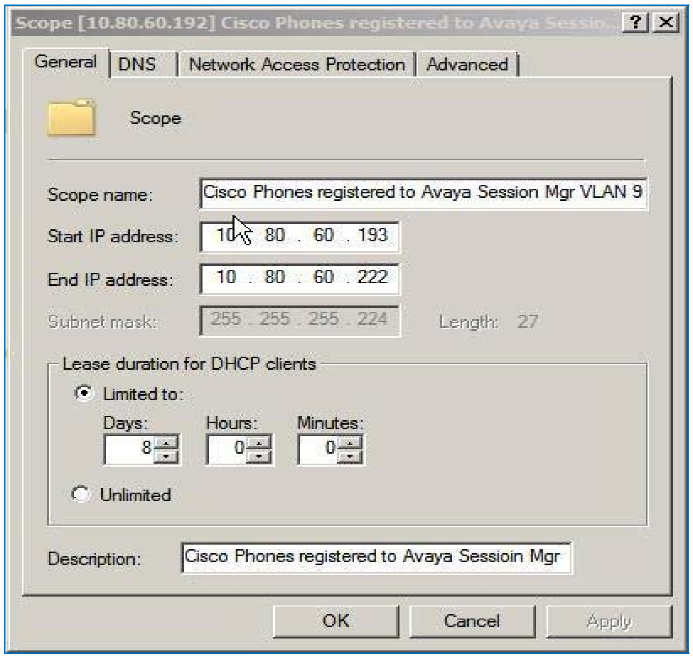
- DHCP Server
- TFTP Server
- Cisco 7940/7960 SIP telephones
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager acting as a Feature Server
- Avaya Aura® System Manager

The sample configuration used in these Application Notes assume the items within the Core Site have already been configured to operate together in an Avaya Aura® Architecture solution allowing calling between H.323 phones, Analog phones, and Digital phones. The references section of these Application Notes contain additional information on configuring Communication Manager as an Evolution Server supporting H.323, Analog, and Digital phones.

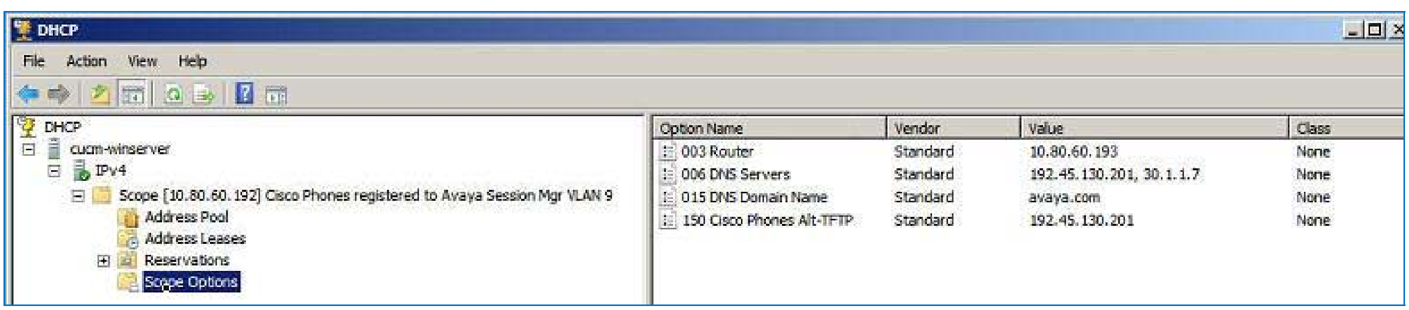
3.1. DHCP Server Configuration

The Cisco 7940/7960 SIP telephones were configured to DHCP their IP address, Network Mask, Gateway Address, Domain Name, DNS, and Option 150 (Alt-TFTP Address) from the network DHCP server. Microsoft DHCP server on Windows Server 2008 R2 was used to administrator the DHCP scopes for both the Cisco SIP telephones and the Avaya one-X® SIP Deskphones.

The scope range used for the sample configuration was configured as follows:



The Scope Options used for the Cisco phones are shown below:

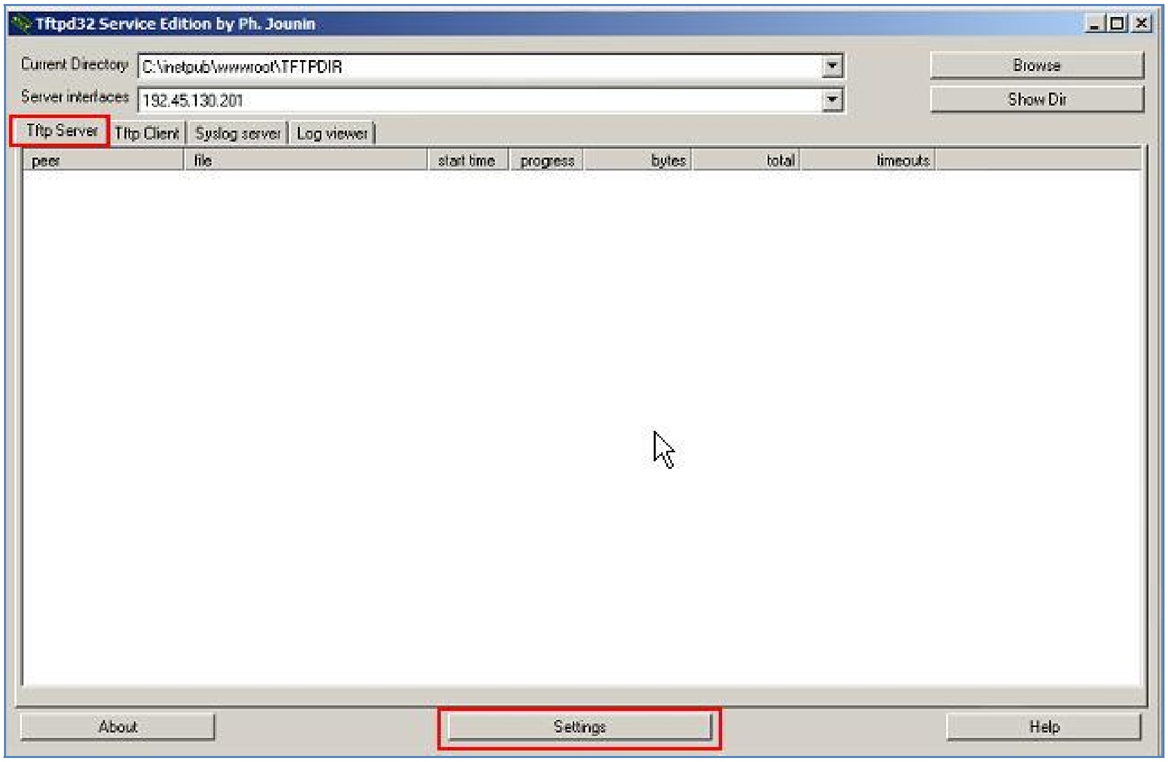


Option 150 has the IP Address of the TFTP Server that is used to download the Cisco SIP firmware and configuration files.

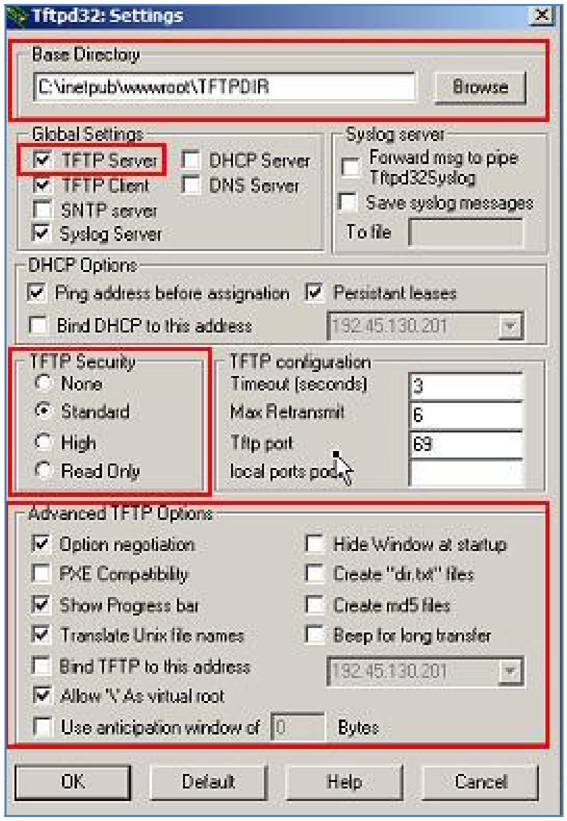
3.2. TFTP Server

The SIP firmware files are transferred to the Cisco 7940/7960 SIP phones using a TFTP Server. Tftpd32, an open source utility, providing an integrated TFTP Server, TFTP Client, DHCP Server, and Syslog Server, was used as the TFTP server.

Running Tftpd32 provides a tabbed interface where the **Tftp Server** tab is selected.



Clicking the **Settings** button at the bottom center application displays a configuration window.



Set the **Base Directory** path to a location where the Cisco SIP phone load and configuration files will be stored. In the sample configuration, **C:\inetpub\wwwroot\TFTPDIR** was created and used as the TFTP **Base Directory** for the TFTP server. Under **Global Settings** check the box next to **TFTP Server**, this will start the TFTP Server when applied. Under **TFTP Security** select the **Standard** radio button. Under **Advanced TFTP Options** for following selections were checked and activated:

- ☑ Option negotiation
- ☑ Show Progress bar
- ☑ Translate Unix file names
- ☑ Allow “\” As virtual root

Click **OK** button to accept the configuration.

3.3. Configure Cisco 7940/7960 SIP Telephone

This section describes steps needed to configure and connect Cisco SIP phones to Session Manager. The steps include downloading the current released Cisco SIP firmware for the 7940/7960 phones and unzipping the files to the TFTP root directory. It will also explain the configuration files and the settings needed to register the Cisco SIP phones with the Session Manager. Since this sample configuration uses the DHCP server, a section will describe how to clear the menu settings by setting the Cisco SIP phones to their factory default setting, allowing them to DHCP all their needed settings from the DHCP server. A section will document the boot/upgrade process as the Cisco 7940 SIP phone boots and registers with Session Manager.

3.3.1. Cisco SIP Firmware

The Cisco SIP firmware for the Cisco 7940/7960 phones can be downloaded from www.cisco.com and requires a support account. The Cisco SIP phone firmware used during testing and for this sample configuration was the latest available, P0S3-8-12-00. This file is downloaded as a zip file, P0S3-8-12-00.zip. The naming convention Cisco uses for their phone loads can be decoded as follows.

First Digit	Second Digit	Third Digit	Fourth Digit	Version x-yy-zz
P = Phone Device	0 = Combined Image (Application & DSP)	Phone Protocol 0 = SCCP (Skinny) S = SIP	3 = ARM Processor	Firmware Version x = major version yy = minor version zz = sub minor version

Table 2: Cisco Firmware Naming Decode

Unzip the contents of the P0S3-8-12-00.zip file to the root directory of the TFTP Server. **Table 3** below lists the zip file contents and the description for each of the files.

File	Description
OS79XX.TXT	This file tells the Cisco 7940/7960 which binary to download from the TFTP server. This file is case sensitive and must only contain the name of the file that you want to load, without the .bin extension. Without this file, the phone does not know which file it needs to retrieve, in order to replace its existing software.
P0S3-8-12-00.loads	File that contains the universal application loader and application image, where the third digit in the file name represents the protocol of the application image LOADS file: 0 = SCCP, and S = SIP.
P0S3-8-12-00.sb2	Application firmware image, where third digit in the file name represents the application firmware image: 0 = SCCP, and S = SIP.
P0S3-8-12-00.bin	A non-secure universal application loader for upgrades from images earlier than 5.x.
P003-8-12-00.sbn	A secure universal application loader for upgrades from images 5.x or later.

Table 3: Contents & Description Cisco Phone Firmware Image ZIP File

3.3.2. Cisco Configuration Files

In order for the Cisco SIP phones to boot correctly and register with the Session Manager a few configuration files must be created and/or edited. **Table 4** contains a list of the configuration files that will be needed to boot up the Cisco SIP phones and register with Session Manager.

Configuration File	Description
OS79XX.txt	File must be edited to contain the firmware version the phones are to load. This file is case sensitive and must only contain the name of the file that you want to load, without the .bin extension. Without this file, the phone does not know which file it needs to retrieve, in order to replace its existing software. Sample Configuration: Appendix 7.1 OS79XX.TXT
SYNCINFO.XML	Controls the image version and associated sync value to be used for remote reboots. Sample Configuration: Appendix 7.2 SYNCINFO.XML
DIALPLAN.XML	This file contains the dial plan used by the phones. Sample Configuration: Appendix 7.3 DIALPLAN.XML
SIPDEFAULT.CNF	This is the Phone-Common file. It contains parameters common to all phones. Sample Configuration: Appendix 7.4 SIPDEFAULT.CNF
SIP[*MAC Address*].cnf	This is the Phone-Specific file. It contains the parameters specific to the individual phone with the specific MAC address. An example file name is SIP0003E311F2D1.cnf. "SIP" must be uppercase, letters in the MAC address must be uppercase, and ".cnf" must be lowercase. Sample Configuration: Appendix 7.5 SIP0003E311F2D1.cnf
RINGLIST.DAT	Lists audio files that are the custom ring type options for the phones. Sample Configuration: Appendix 7.6 RINGLIST.DAT
SEP[*MAC Address*].cnf.xml	This is a Phone-Specific file. It contains the device protocol, phone model, and load information to be used. Sample Configuration: Appendix 7.7 SEP0003E311F2D1.cnf.xml
CTLSEP[*MAC Address*].tlv	This is a Phone-Specific file. It contains security certificate information is needed. This file will be edited to be blank, since certificates are not being used in this sample configuration. The Cisco SIP phone boot process still looks for this file in the TFTP directory.

Table 4: Configuration Files

Several of the files contain generic configurations used by all Cisco SIP phones. Please refer to the Appendix of this document to view the configuration samples used in these Application Notes. Three specific configuration files are needed for each phone and will contain the phones MAC address in part of the naming convention of each of these files. These files are: SEP[*MAC_Address*].cnf, SEP[*MAC_Address*].cnf.xml, and CTLSEP[*MAC_Address*].tlv.

The Cisco SIP 7960 phone with MAC address **0003E311F2D1** was used in this sample configuration for User **Cisco SIP 7960-1** with phone extension **6663009**. Three configuration files were created using this phones MAC address, **SIP0003E311F2D1.cnf**, **SEP0003E311F2D1.cnf.xml**, and **CTLSEP0003E311F2D1.tlv**.

The following parameters must be set to match settings used on the Session Manager.

- proxy1_address: "10.80.120.28" — This must match the IP address of the SIP virtual interface assigned in the Session Manager.
- line1_authname: "6663009" — This must match the username of this user created in Session Manager.
- line1_password: "123456" — This must match the password of this user created in Session Manager.
- messages_uri: "6664999" — This must match the extension assigned on the Feature Server for retrieving messages.

To discover all available parameters supported in this file, refer to the Cisco Phone reference section of these Application Notes.

3.3.3. Cisco 7940/7960 Menu Settings

In order to clear any settings programmed into the Cisco SIP phones, it is recommended to factory reset the phone. This can be accomplished by pressing the *****, **6**, and **Settings** buttons all at the same time to reset the phone. Immediately press and hold the **#** key until the screen shows **Reset key sequence detected**, then release the **#** key and enter the **123456789*0#**. Lights on the **Headset**, **Mute**, and **Speaker** buttons will start flashing with alternating Green, Red, Green across these buttons, this is normal. The screen will ask to "**Save network cfg? 1=yes 2=no**". Press **2** to select **no**, not to save the phone's current configuration, this will clear all configuration values currently on the phone. The phone will now show **Factory reset initiated** in the display and will reload.

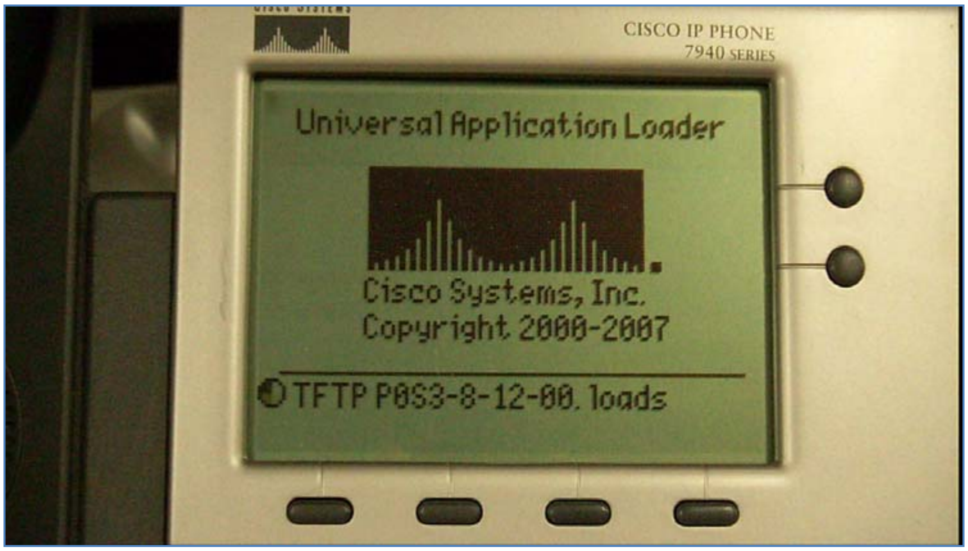
3.3.4. Booting/Upgrading Cisco Phone

The following is the Cisco SIP phones normal boot sequence.

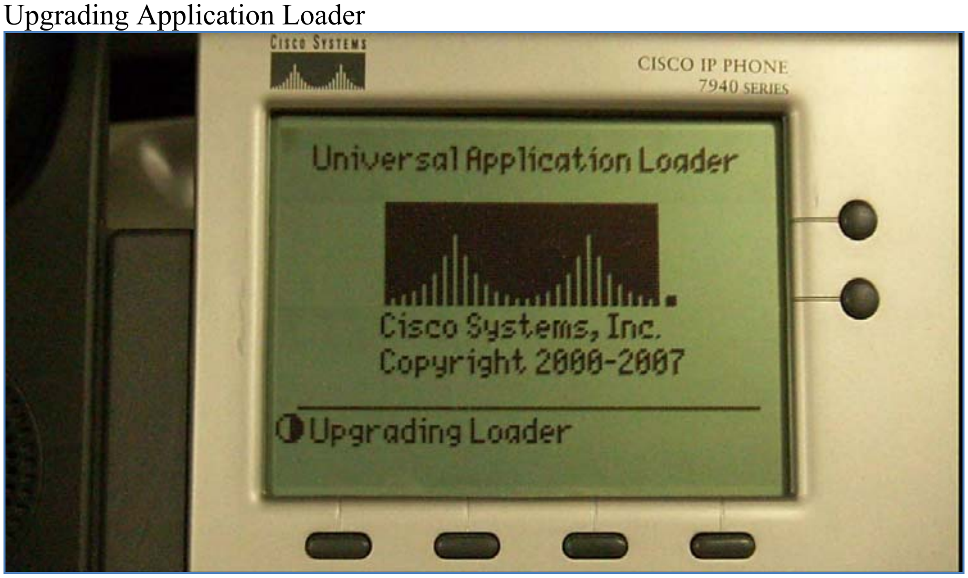
1. Each phone requests the initial setup file OS79XX.TXT.
   Note: Ensure that you use exactly the same name, because the file names on the TFTP server and the SIP image name in OS79XX.TXT are case sensitive.

2. Each phone loads the firmware binary file listed in the OS79XX.TXT file. After the proper BIN file is downloaded, it replaces the software that it runs with this new image.

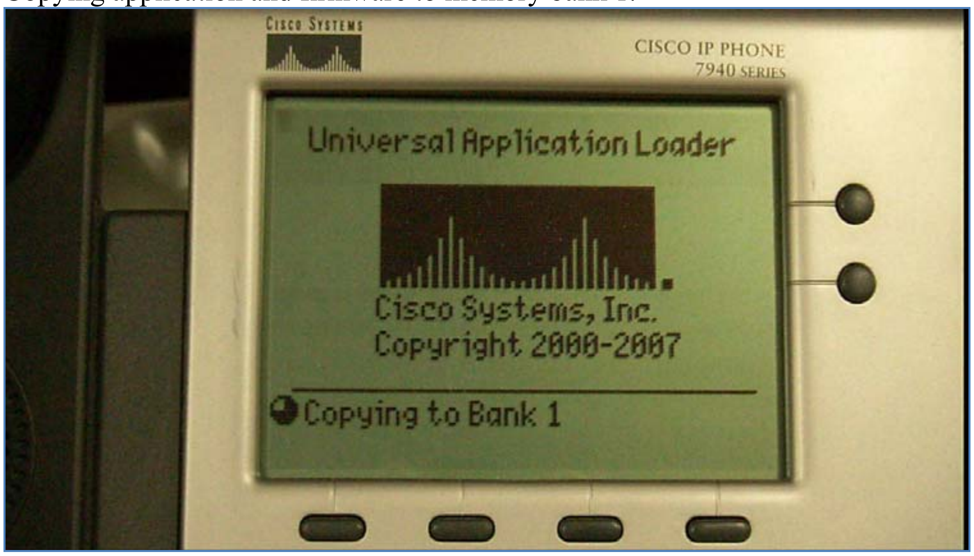
3. Each phone loads the SIP image that is indicated in the initial setup file. In this case, the P0S3-8-12-00.bin file is loaded.



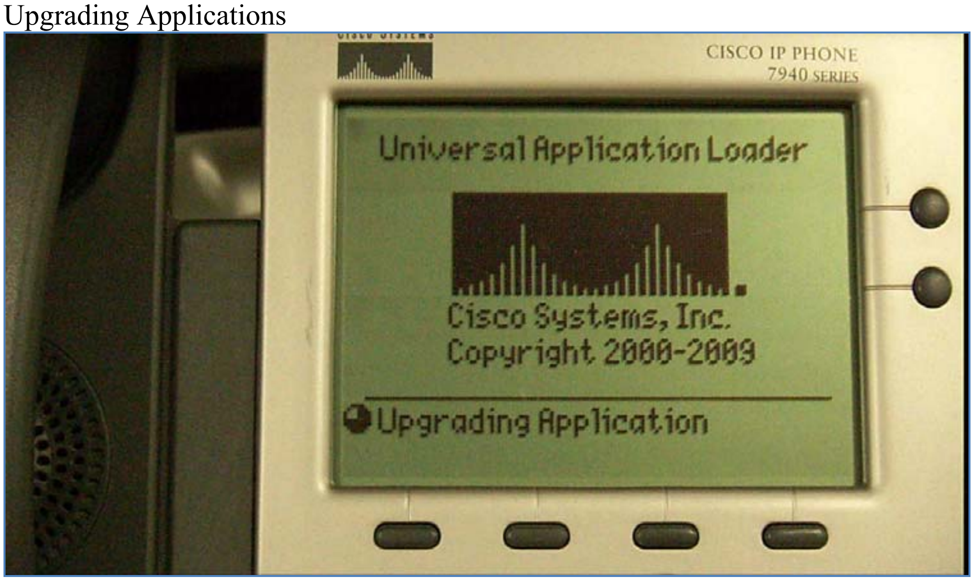
4. Upgrading Application Loader



5. Copying application and firmware to memory bank 1.



6. Upgrading Applications



7. Each phone loads the SIPDefault.cnf file. This file contains basic configuration settings that are common for all phones.

8. Each phone loads its specific configuration information from the file SIP*mac_address*.cnf. The MAC address must be specified in capital letters.

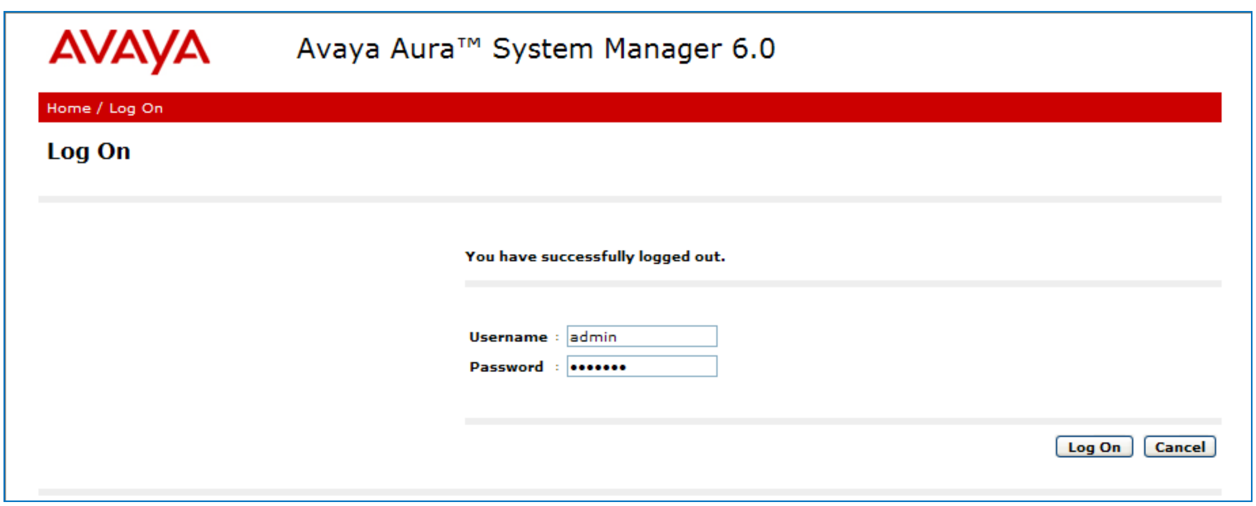
3.4. Administer Avaya Aura® Session Manager

The following steps describe configuration of Session Manager for use with Cisco 7940 and 7960 SIP telephones. The following section describes administering SIP Entities between Session Manager and the Communication Manager Feature Server in order to establish a SIP Entity link between Session Manager and the Communication Manager Feature Server. Administering the Cisco SIP telephones to register to Session Manager is also discussed.

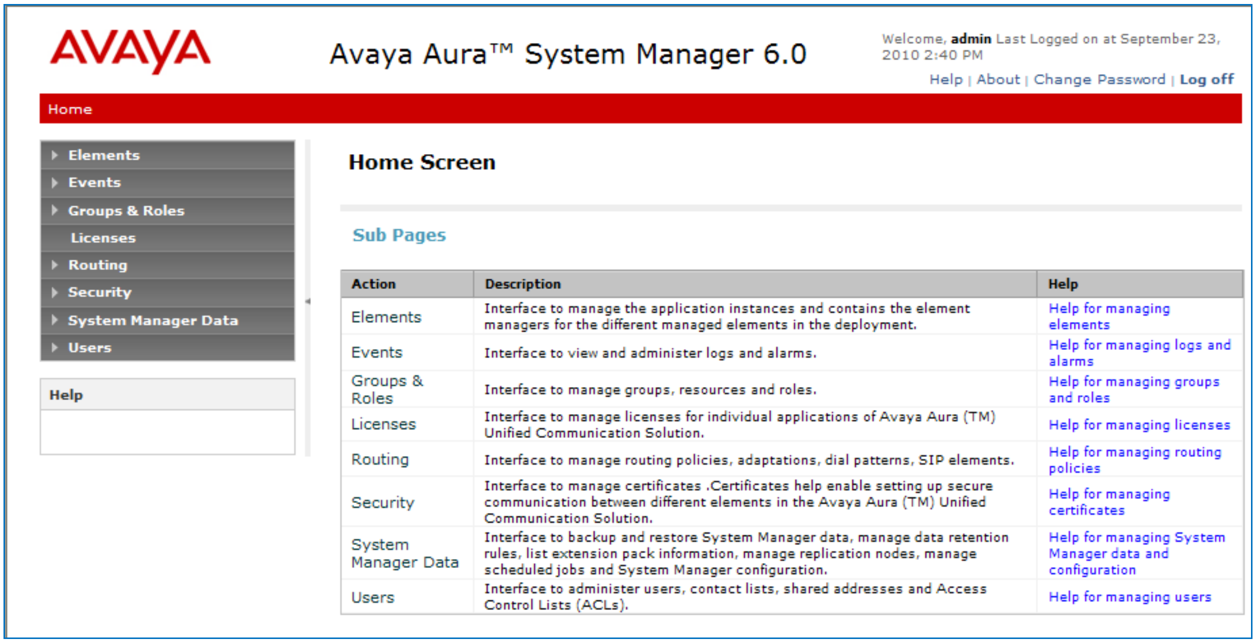
- Access Avaya Aura® Session Manager
- Add SIP Domain
- Add Location
- Administer Avaya Aura® Session Manager SIP Entity
- Administer Avaya Aura® Communication Manager Feature Server SIP Entity
- Administer Modular Messaging SIP Entity
- Administer SIP Entity Link
- Administer Avaya Aura® Session Manager
- Administer Avaya Aura® Communication Manager as a Feature Server
- Administer Avaya Aura® Communication Manager Feature Server Application
- Administer Avaya Aura® Communication Manager Feature Server Application Sequence
- Synchronize CM Data
- Add SIP User

3.4.1. Access Avaya Aura® Session Manager

Access the System Manager web interface, by entering **http://<ip-addr>/SMGR** as the URL in an Internet browser, where *<ip-addr>* is the IP address of the server running System Manager graphical user interface. Log in with the appropriate **Username** and **Password** and press the **Log On** button to access Session Manager.

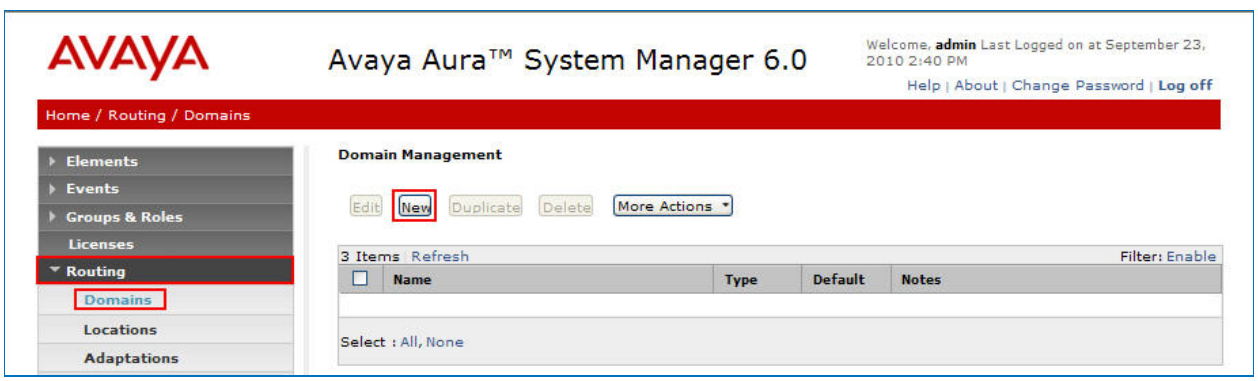


The **main menu** of the **System Manager Graphical User Interface** is displayed in the following screenshot.

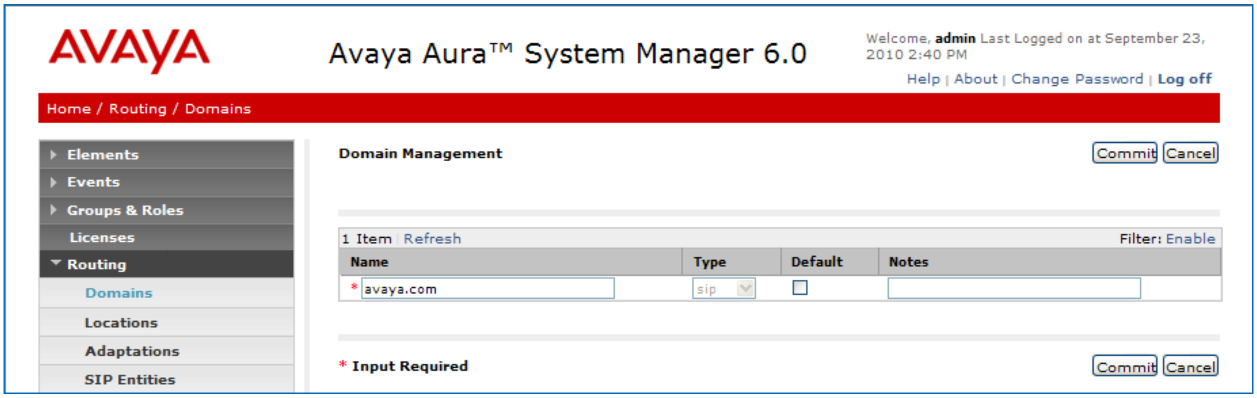


3.4.2. Administer SIP Domain

Select **Routing → Domains** and click on the **New** button to add a new domain.



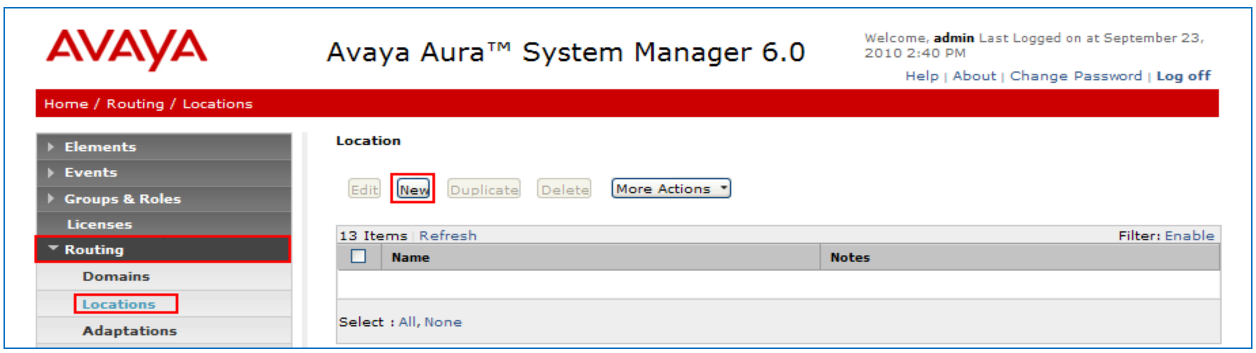
The name of the SIP Domain used in Session Manager **avaya.com** was added. The type was set to **sip**. Press the **Commit** button to add the SIP Domain.



3.4.3. Add Location

Locations are used to identify logical and physical locations where SIP entities reside for the purposes of bandwidth management or location based routing.

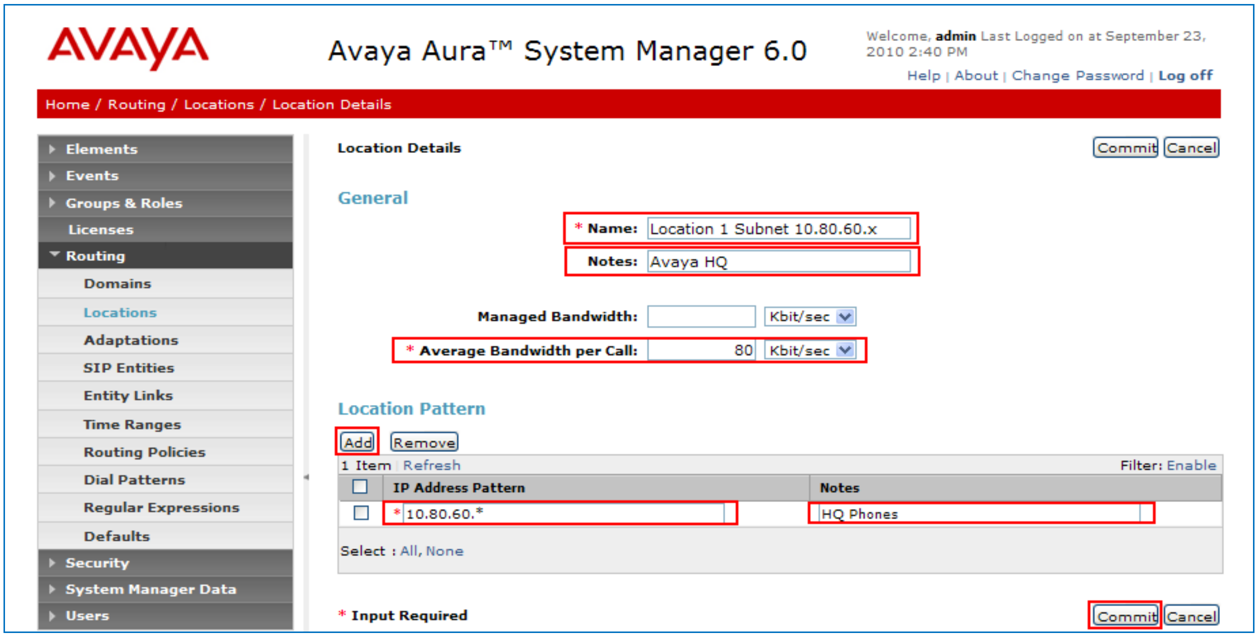
To add a new Location, click on **Routing** → **Locations** and click on the **New** button.



In the **General** section, enter the location **Name** "Location 1 Subnet 10.80.60.x". In the **Notes** field enter "Avaya HQ". The **Average Bandwidth per Call** was set to the default value of **80 Kbit/sec**.

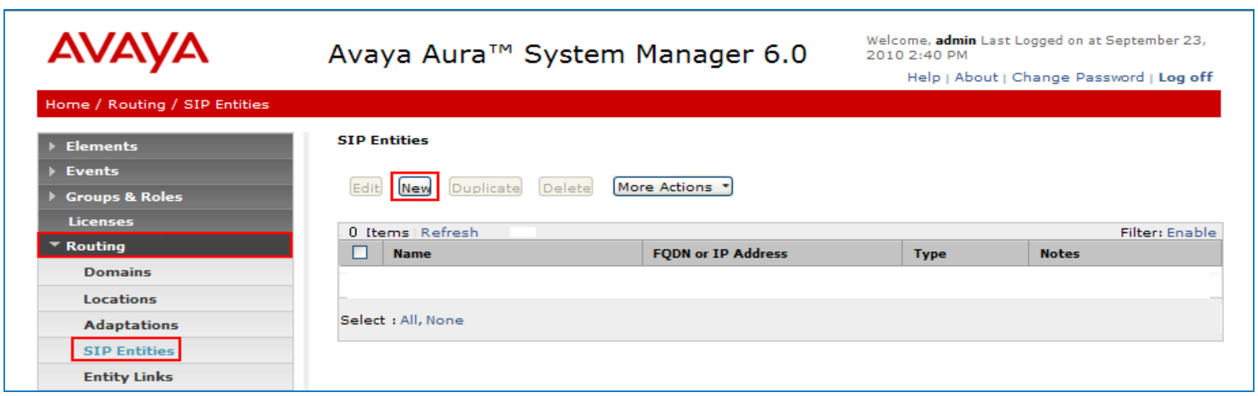
Under the **Location Pattern** section, click on the Add button and then enter the **IP Address Pattern** "10.80.60.*". In the **Notes** field enter a short description for the location, "HQ Phones" was used for this sample configuration.

Click the **Commit** button to confirm changes.



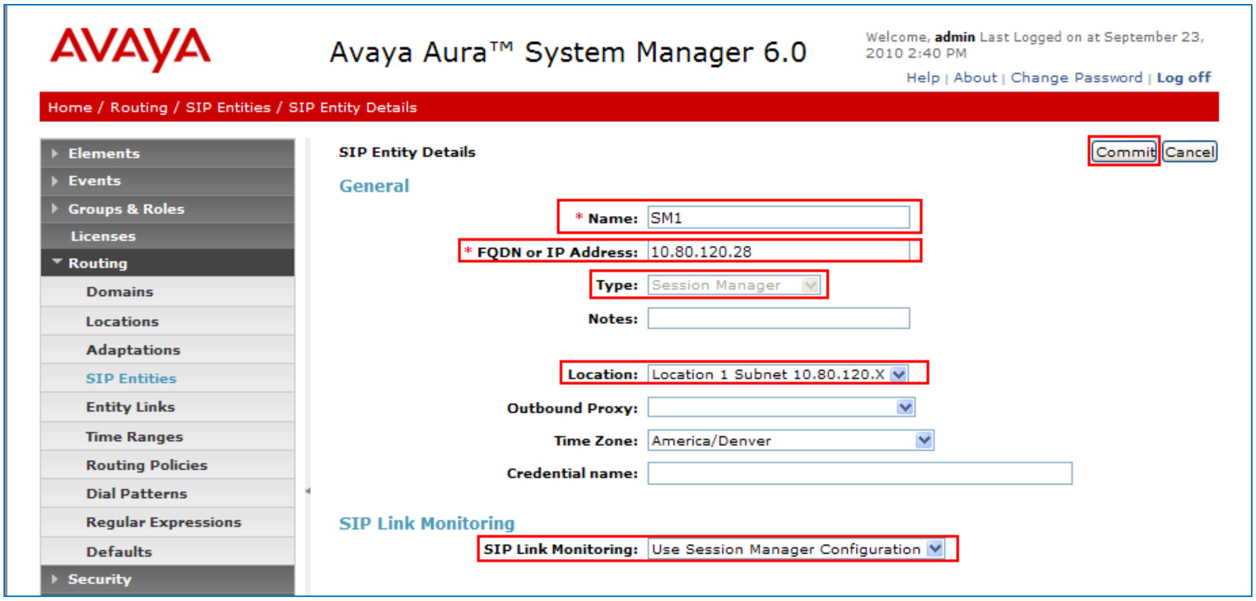
3.4.4. Administer Avaya Aura® Session Manager SIP Entity

The Session Manager SIP Entity is the first part of establishing a connection between Session Manager and the Communication Manager Feature Server. Create a SIP Entity for the Session Manager by selecting **Routing** → **SIP Entities** and then click on the **New** button.

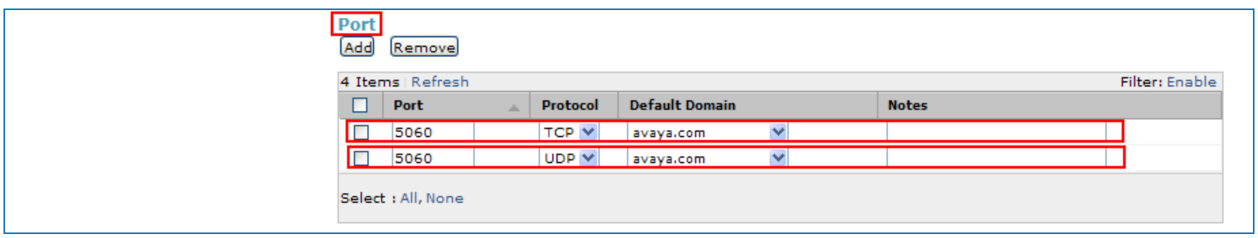


The **Name** of the SIP Entity was **SM1.** The **FQDN or IP Address** was set to **10.80.120.28**. This is the IP Address of the SM100 card in the Session Manager Server. The **Type** was set to **Session Manager.** The **Location** was set to **Location 1 Subnet 10.80.120.X**. The **Time Zone** should be set to the proper selection from the drop down list. The **SIP Link Monitoring** was set to **Use Session Manager Configuration**.

Click the **Commit** button to confirm changes.



The following screenshot shows what port settings need to be configured for the SIP Entity. With the signaling protocol being set to **TCP** port **5060** was used in the SIP Entity SIP trunk. The Cisco SIP telephones use **UDP** port **5060** to register to the Session Manager. UDP port 5060 must be created on the Session Manager SIP Entity.

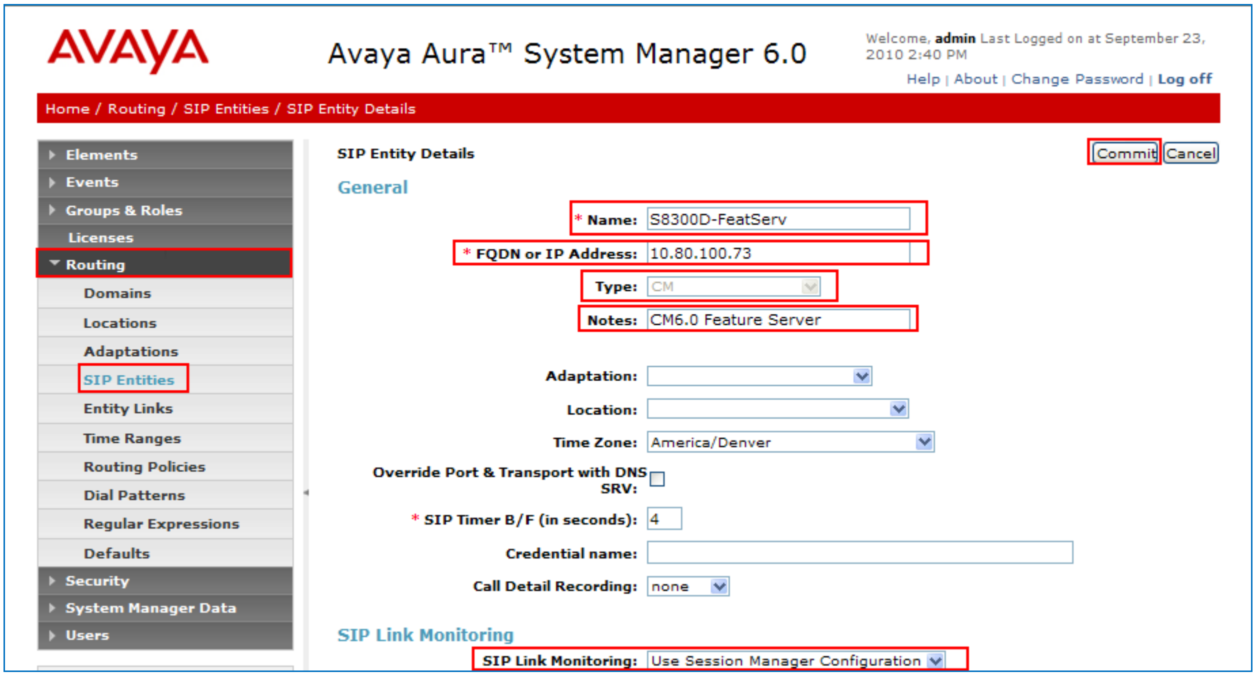


Click the **Commit** button to confirm changes.

3.4.5. Administer Communication Manager Feature Server SIP Entity

The Feature Server SIP Entity is the second part of the link between the Session Manager and the Communication Manager Feature Server. Create a SIP Entity for the Feature Server by selecting **Routing** → **SIP** Entities and then click on the **New** button. The **Name** of the SIP Entity was **S8300D-FeatServ**. The **FQDN or IP Address** was set to **10.80.100.73** which was the IP Address of the CLAN card in the G450 Media Gateway. The G450 Media Gateway is linked to the Communication Manager Feature Server through the IPSI card in the G450 Media Gateway. The **Type** was set to **CM** for Communication Manager. The **SIP Link Monitoring** was set to **Use Session Manager Configuration**.

Click the **Commit** button to confirm changes.



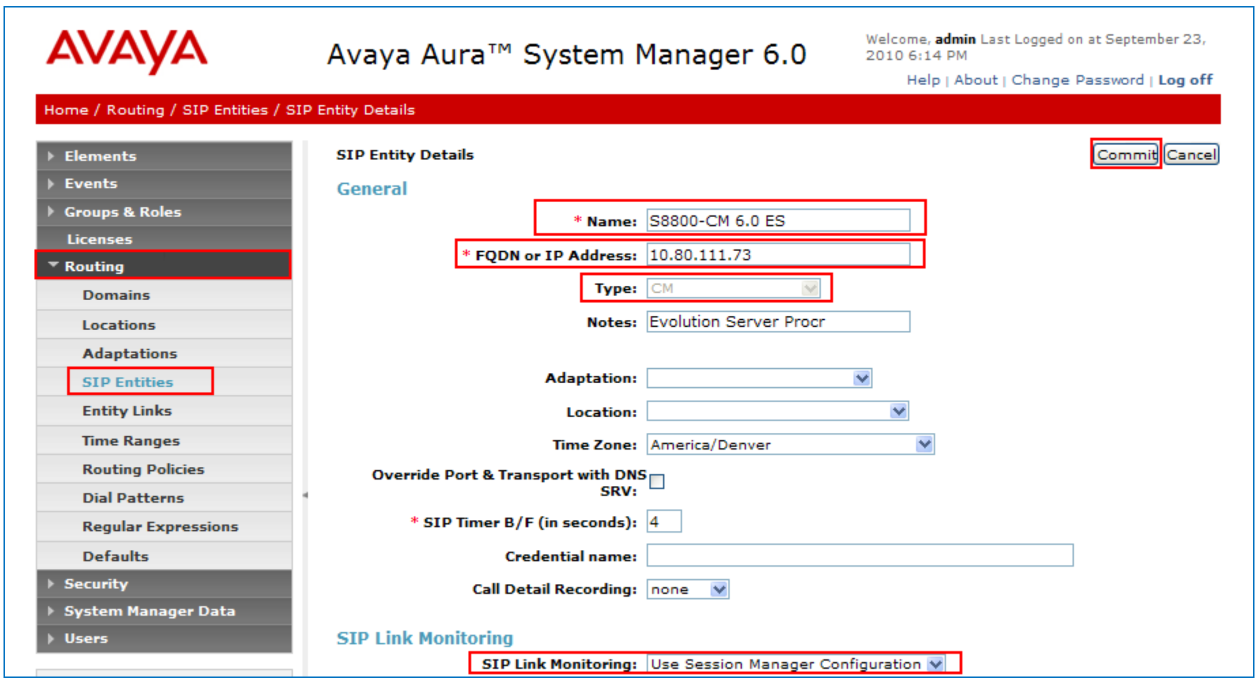
3.4.6. Administer Communication Manager Evolution Server SIP Entity

The Evolution Server SIP Entity is created to provide the far side SIP Entity allowing a SIP Trunk connection between Session Manager and Communication Manager acting as an Evolution Server. Once the SIP Entity Link is created in the next section, SIP communication between the SIP telephones registered to the Session Manager and the H323, Analog, and Digital telephones connected to the Evolution Server will be possible.

Create a SIP Entity for Communication Manager acting as an Evolution Server by selecting **Routing** → **SIP Entities** and then click on the **New** button.

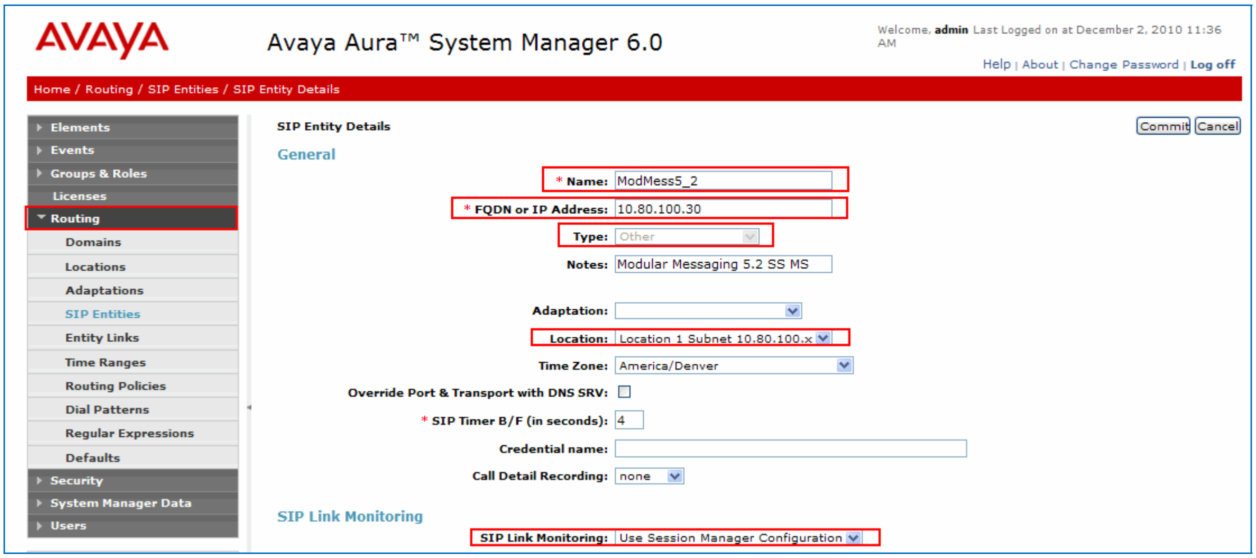
The **Name** of the SIP Entity was **S8800-CM 6.0 ES**. The **FQDN or IP Address** was set to **10.80.111.73** was the IP Address of the CLAN card in the G650 Media Gateway. The G650 Media Gateway is linked to Communication Manager Evolution Server through the IPSI card in the G650 Media Gateway. The **Type** was set to **CM** for Communication Manager. The **SIP Link Monitoring** was set to **Use Session Manager Configuration**.

Click the **Commit** button to confirm changes.



3.4.7. Administer Modular Messaging SIP Entity

The Modular Messaging SIP Entity is the link between the Session Manager and the Modular Messaging Application Server. The **Name** of the SIP Entity was **ModMess5_2.** The **FQDN or IP Address** was set to **10.80.100.30** which was the IP Address of the Messaging Application Server. The **Type** was set to **Other**. The **Location** was set to **Location 1 Subnet 10.80.100.X**. The **SIP Link Monitoring** was set to **Use Session Manager Configuration**. Click the **Commit** button to save changes.



3.4.8. Administer SIP Entity Links

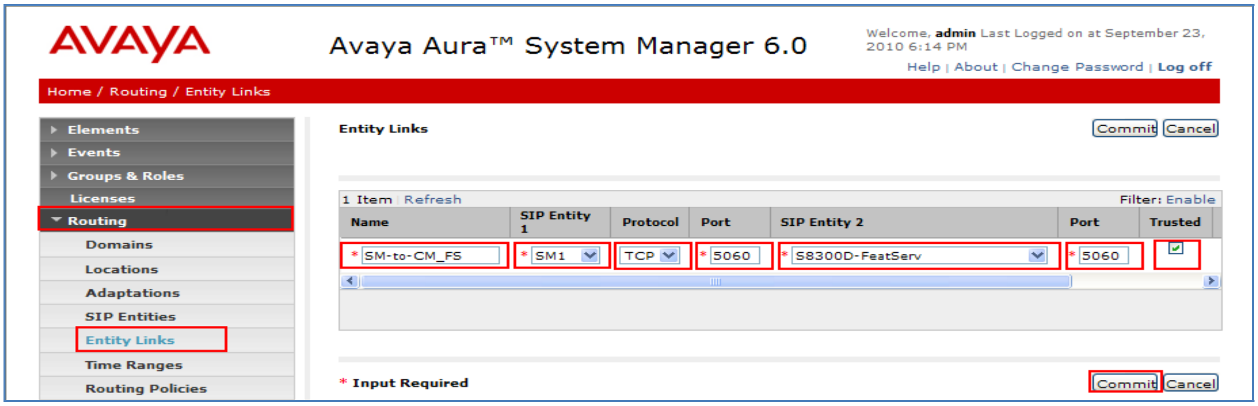
The SIP Entity Links provide a point to point link between the SIP Entities. Three SIP Entity Links are needed:

- SM-to-CM_FS   SIP Entity Link between Session Manager and Communication Manager Feature Server.
- SM1_ModMess5_2_5060_TCP   SIP Entity Link between Session Manager and Avaya Modular Messaging.
- S8800-CM_6.0   SIP Entity Link between Session Manager and Communication Manager Evolution Server.

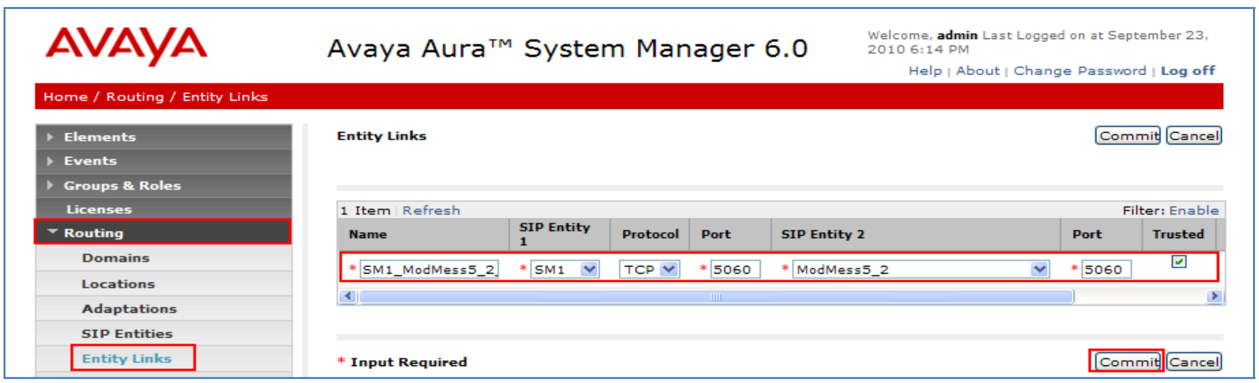
Create the SIP Entity Link by selecting **Routing** → **Entity Links** and clicking on the **New** button.

The **Name** was set to **SM-to-CM_FS**, representing the SIP Entity Link between the Session Manager and Communication Manager Feature Server. **SIP Entity 1**, the Session Manager SIP Entity was called **SM1**. **Protocol** is set to **TCP** and the **Port** is set to **5060**. **SIP Entity 2**, the

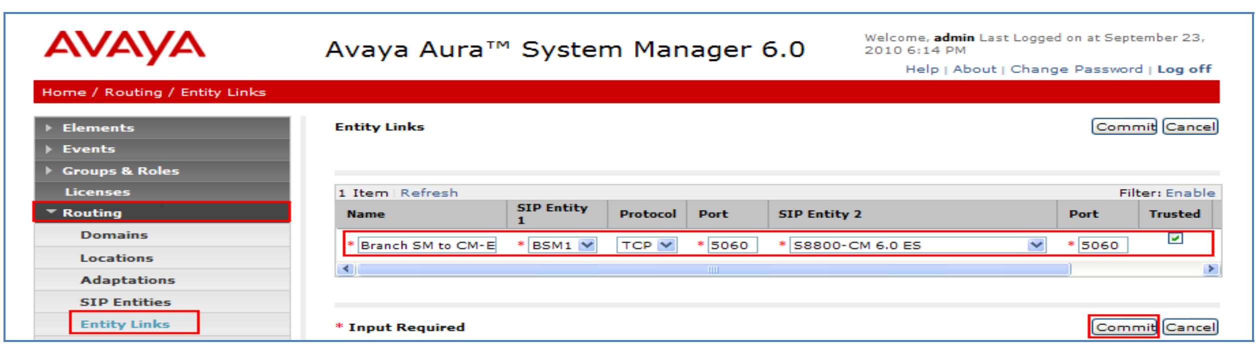
Feature Server SIP Entity was called **S8300D-FeatServ**. The signaling **Port** was **5060**. Check the box under **Trusted**, allowing SIP Entity 2 using the specified port to be a trusted connection.



Repeat the steps to create a SIP Entity Link for the link between the Session Manager and the Modular Messaging Server using the settings shown below.

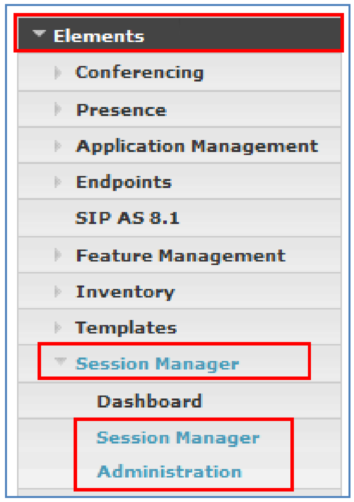


Create the last SIP Entity Link for the link between the Session Manager and Communication Manager Evolution Server using the settings show below.

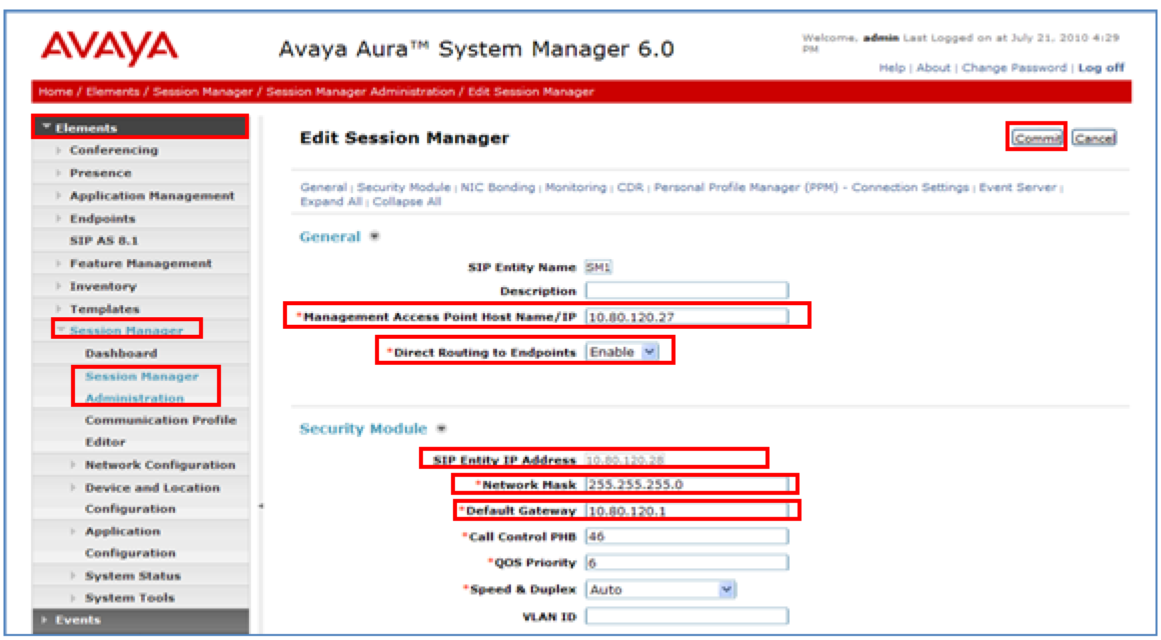


3.4.9. Administer Avaya Aura® Session Manager

In order to provide the link between Session Manager and System Manager, Session Manager must be added to the configuration. Under the **Elements → Session Manager** heading on the left hand side of the Session Manager GUI click on the **Session Manager Administration** sub heading**.**



The SIP Entity **Name** was set to **SM1**. The **Management Access Point Host Name / IP** was set to 10.80.120.27. This is the IP Address for the server running Session Manager. **Direct Routing to Endpoints** was **Enabled**. The **SIP Entity IP Address** was to 10.80.120.28. This was the IP Address of the SM100 card in Session Manager. The **Network Mask** was set to 255.255.255.0 and the **Default Gateway** was set to 10.80.120.1.



3.4.10. Administer Avaya Aura® Communication Manager as a Feature Server

In order for Communication Manager to provide configuration and feature support to Avaya SIP telephones when they register to Session Manager, Communication Manager Feature Server must be added as an application for Session Manager. This is a four step process.

Step 1

Select **Elements → Inventory → Manage Elements** on the left. Click on **New** (not shown). Enter the following fields, and use defaults for the remaining fields:

- **Name**: A descriptive name
- **Type**: Select "CM"
- **Node**: Select "Other.." and enter IP address for Communication Manager SAT access

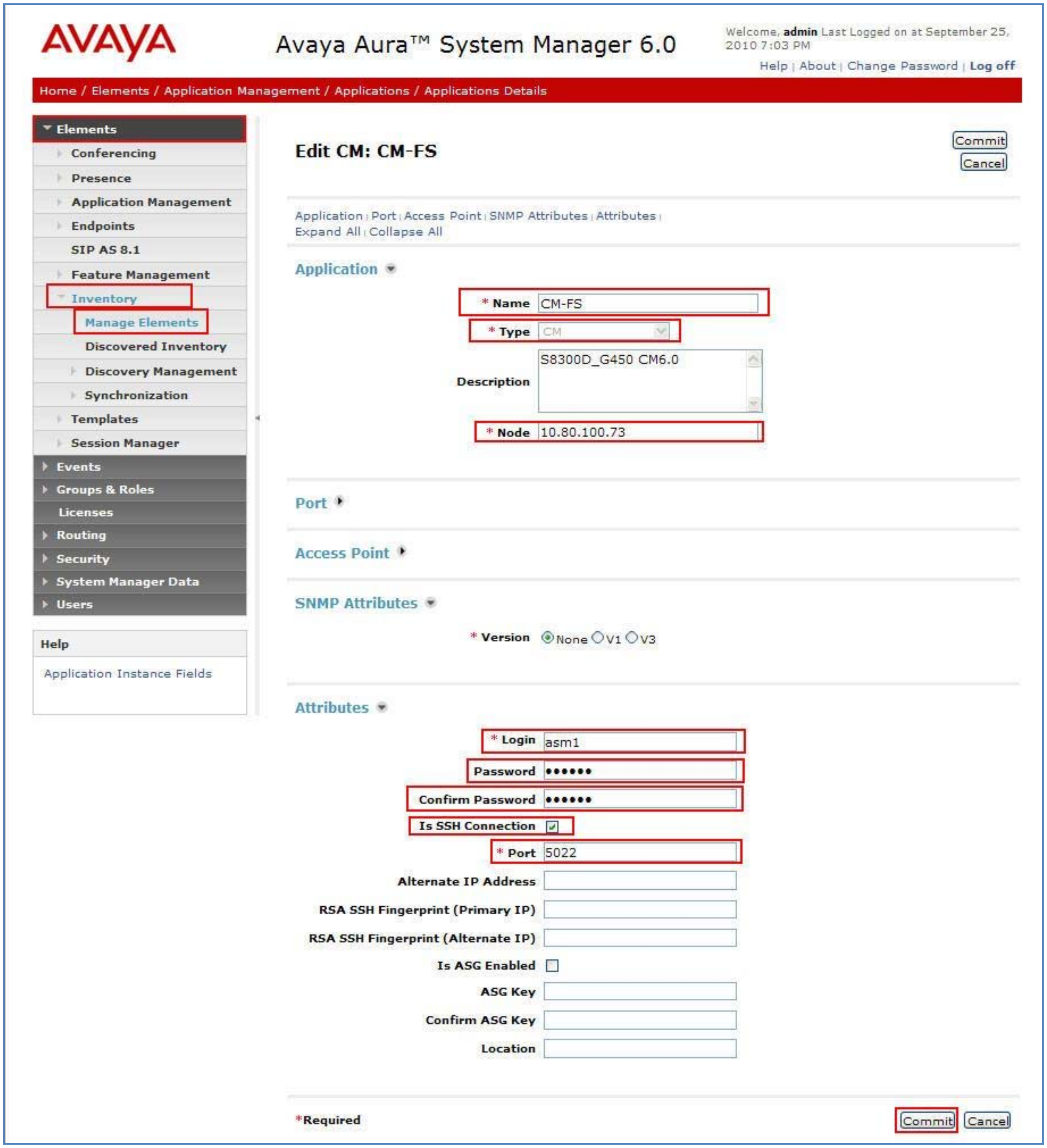
Under the *Attributes* section, enter the following fields, and use defaults for the remaining fields:

- **Login**: Login used for SAT access
- **Password**: Password used for SAT access
- **Confirm Password**: Password used for SAT access
- **Is SSH Connection:** ☑
- **Port:** 5022

Click on **Commit**.

This will set up data synchronization with Communication Manager to occur periodically in the background.

The screen shown below is the Edit screen since the Application Entity has already been added.


AVAYA
Avaya Aura™ System Manager 6.0
Welcome, admin Last Logged on at September 25, 2010 7:03 PM
Help | About | Change Password | Log off
Home / Elements / Application Management / Applications / Applications Details
Elements
Conferencing
Presence
Application Management
Endpoints
SIP AS 8.1
Feature Management
Inventory
Manage Elements
Discovered Inventory
Discovery Management
Synchronization
Templates
Session Manager
Events
Groups & Roles
Licenses
Routing
Security
System Manager Data
Users
Help
Application Instance Fields
Edit CM: CM-FS
Commit
Cancel
Application | Port | Access Point | SNMP Attributes | Attributes |
Expand All | Collapse All
Application
* Name CM-FS
* Type CM
Description S8300D_G450 CM6.0
* Node 10.80.100.73
Port
Access Point
SNMP Attributes
* Version None V1 V3
Attributes
* Login asm1
Password ••••••
Confirm Password ••••••
Is SSH Connection
* Port 5022
Alternate IP Address
RSA SSH Fingerprint (Primary IP)
RSA SSH Fingerprint (Alternate IP)
Is ASG Enabled
ASG Key
Confirm ASG Key
Location
*Required
Commit
Cancel

Step 2

Select **Elements → Session Manager → Application Configuration → Applications** on the left. Click on **New** (not shown). Enter the following fields, and use defaults for the remaining fields:

- **Name:** A descriptive name
- **SIP Entity:** Select the Communication Manager SIP Entity
- **CM System for SIP Entity** Select CM System

Click on **Commit**.

The screen shown below is the Edit screen since the Application has already been configured.

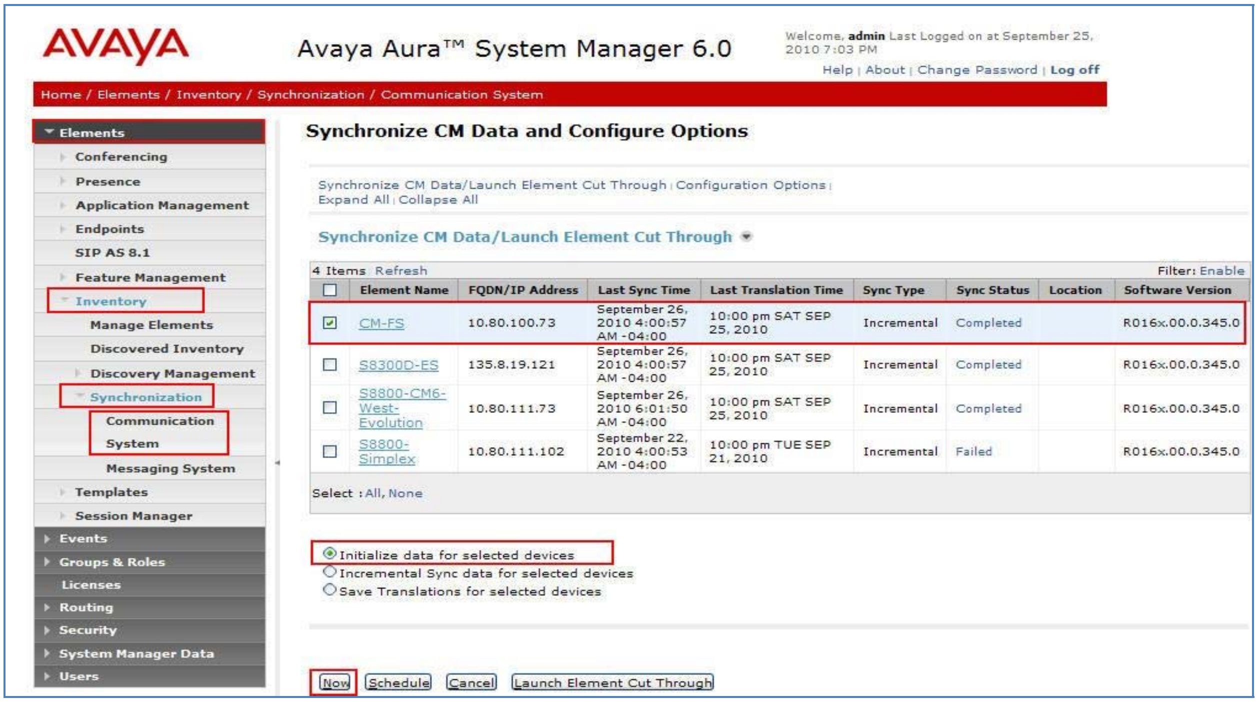
Step 3

Select **Elements → Session Manager → Application Configuration → Application Sequences** on the left. Click on **New** (not shown). Enter a descriptive name in the **Name** field. Click on the "+" sign next to the appropriate *Available Applications*, and the selected available application will be moved up to the *Applications in this Sequence* section. In this sample configuration, "CM-FS-Seq-App" was shown in the screen below (which is the Edit screen since the Application Sequence has already been configured).

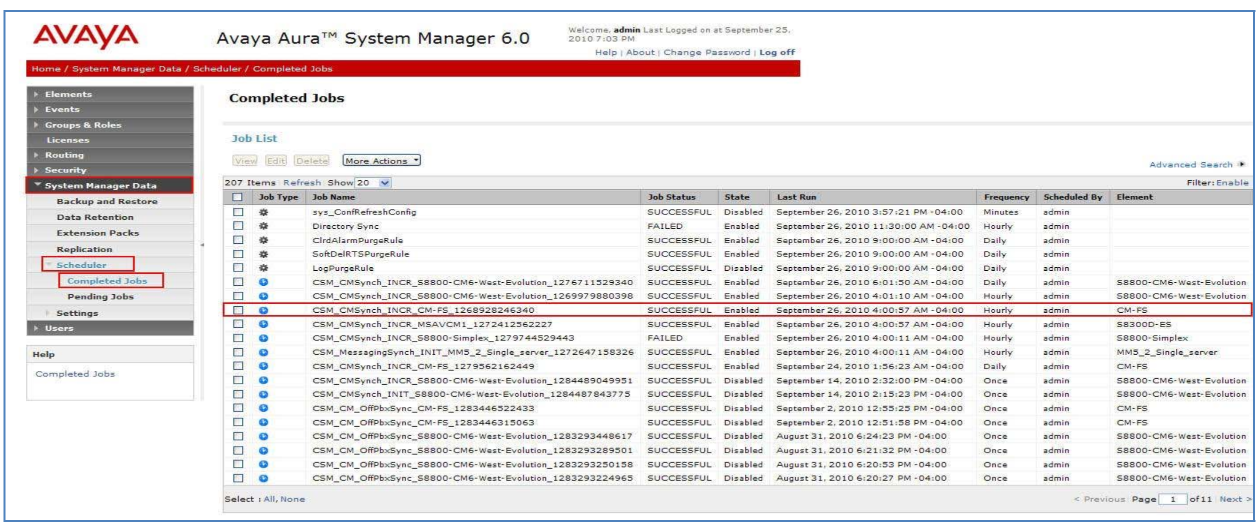
Click on **Commit**.

Step 4

Select **Elements → Inventory → Synchronization → Communication System** on the left. Select the appropriate Element Name ("CM-FS" in this case). Check the **Initialize data for selected devices** checkbox. Then click on **Now**. This will cause a data synchronization task to start. This may take some time to complete.



Use the menus on the left under **System Manager Data → Scheduler → Completed Jobs** to determine when the task has completed, as shown below (see entry with embedded Communication Manager name "CM-FS" for the sample configuration).



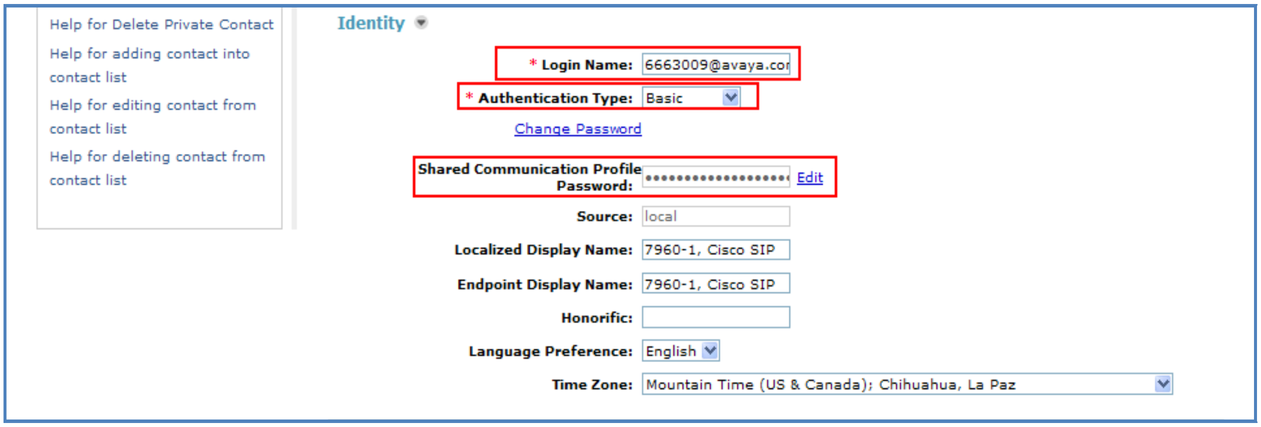
3.4.11. Add SIP Users

Refer to **Table 1** for adding SIP Users for this sample configuration. The administration for adding a single user for the Cisco SIP phones will be covered first and then a user for the Avaya SIP phones will be covered second. Use the listing in **Table 1** and repeat the steps for each user of the remaining SIP phones used in this sample configuration.

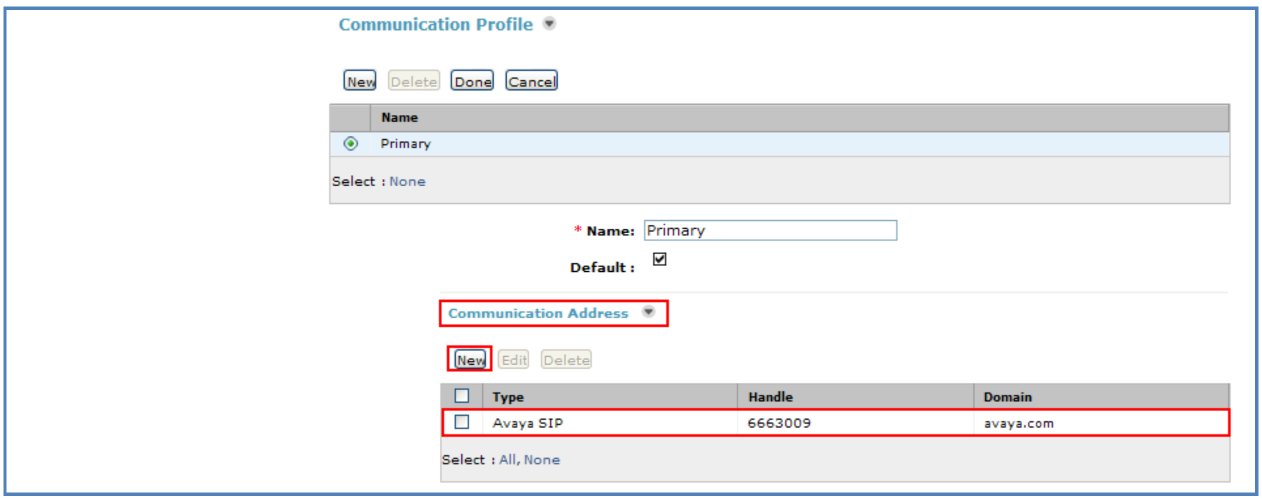
3.4.11.1 Cisco SIP Users

To add a SIP User for a Cisco SIP phone to Session Manager, access the **Users → Manage Users** on the left hand side of the Session Manager GUI. Then click on **New** (not shown) to open the New User Profile page. Referring to **Table** 1, Station Number 6663009 has a user with a **Last Name** of **7960-1** and a **First Name** of **Cisco SIP**.

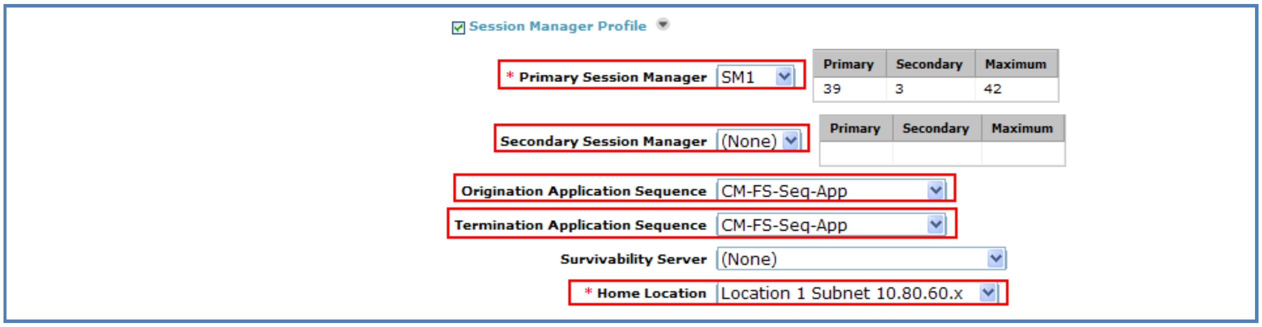
Under the **Identity** settings for the SIP User in the following screenshot the **Login Name** was set to the <phone extension>@avaya.com or for this user **6663009@avaya.com**. The **Authentication Type** was set to **Basic.** The **SMGR Login Password** was set to the login and password of the Session Manager. The **Shared Communication Profile Password** was set to **123456** to match the value set for "line1_password" in the **SEP0003e311f2d1.cnf** configuration file.



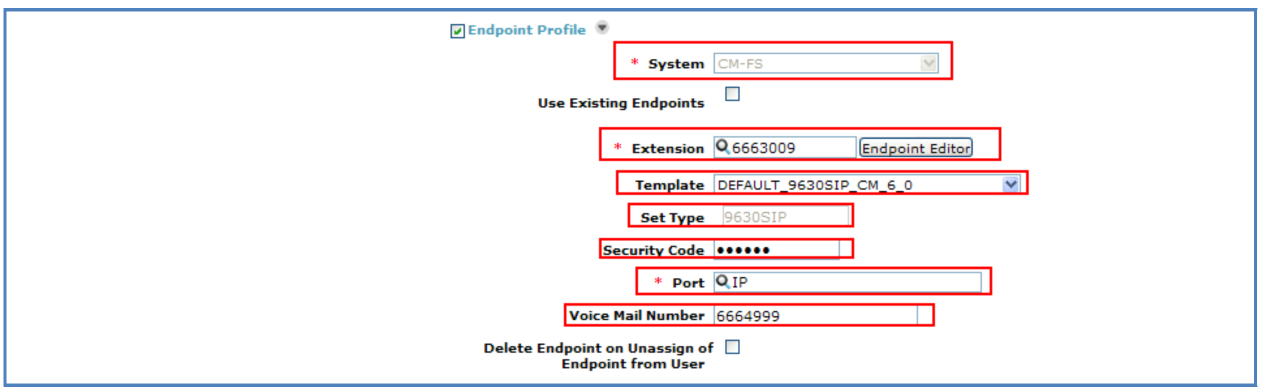
Under the **Communication Profile** heading set the **Name** of the Communication Profile to **Primary** and enable the **Default** setting. In the **Communication Address** the **Type** was set to **Avaya SIP** and the **SubType** was set to **username**. The **Fully Qualified Address** was set as **6663009@avaya.com**.



Under the **Session Manager Profile** heading set the **Primary Session Manager** to **SM1**. The **Secondary Session Manager** will be set to **None**. Both the **Origination Application Sequence** and **Termination Application Sequence** will be set to **CM-FS-Seq-App**. This is the Communication Manager Feature Server Application Sequence name. The **Survivability Server** is set to **None**. The **Home Location** will be set to **Location 1 Subnet 10.80.60.x**.



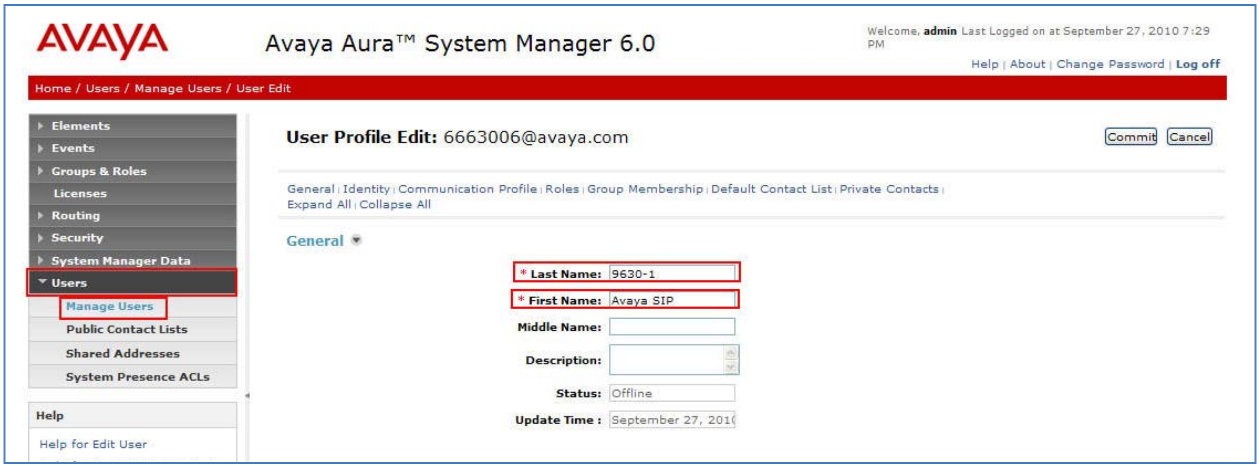
In order for the Endpoint Profile template information to be pushed from the Session Manager down to Communication Manager Feature Server, **enable** the **Endpoint Profile** box. The **System** was set to **CM-FS**. This is the Communication Manager Feature Server Entity Name. The **Extension** was set to **6663009** and the **Template** was set to **DEFAULT_9630SIP_CM_6_0**. The **Security Code** was set to **123456**. The **Port** was set to **IP**.



Repeat this section to add the remaining Cisco SIP Users assigned to station numbers in **Table 1**.

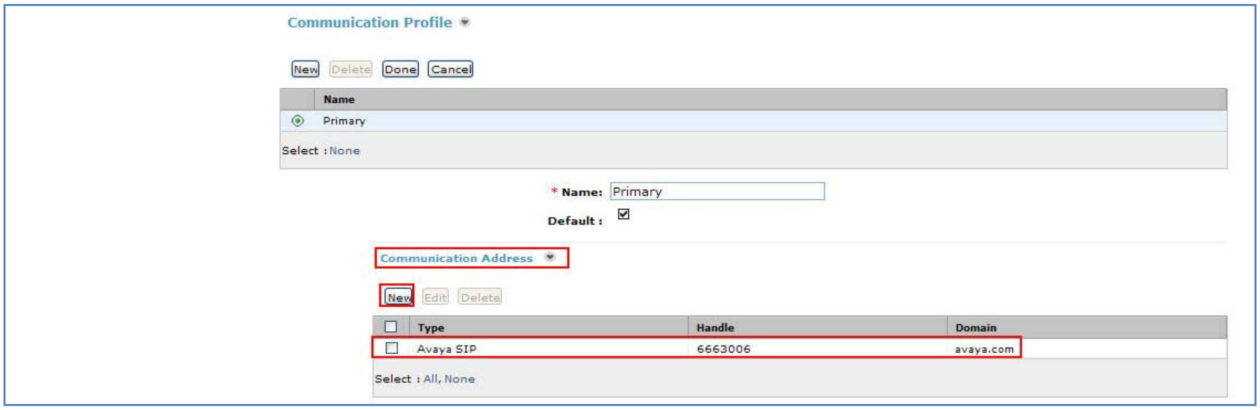
3.4.11.2 Avaya SIP Users

To add SIP User for Avaya SIP phone to Session Manager, access the **Users → Manage Users** on the left hand side of the Session Manager GUI. Then click on **New** (not shown) to open the New User Profile page. Referring to **Table 1**, Station Number 6663006 has a user with a **Last Name** of **9630-1** and a **First Name** of Avaya SIP.

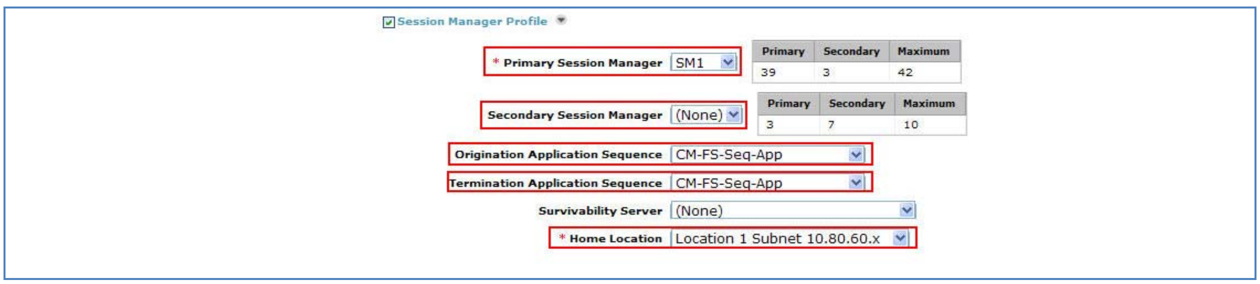


Under the **Identity** settings for the SIP User in the following screenshot the **Login Name** was set to the <phone extension>@avaya.com or for this user **6663006@avaya.com**. The **Authentication Type** was set to **Basic**. The **SMGR Login Password** was set to the login and password of the Session Manager. The **Shared Communication Profile Password** was set to **123456**.

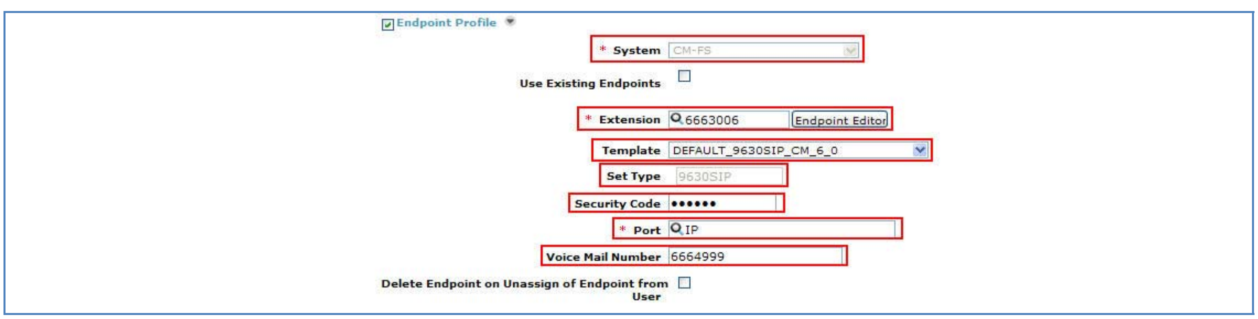
Under the **Communication Profile** heading set the **Name** of the Communication Profile to **Primary** and enable the **Default** setting. In the **Communication Address** the **Type** was set to **Avaya SIP** and the **SubType** was set to **username**. The **Fully Qualified Address** was set as **6663006@avaya.com**.



Under the **Session Manager Profile** heading set the **Primary Session Manager** to **SM1**. The **Secondary Session Manager** will be set to **None**. Both the **Origination Application Sequence** and **Termination Application Sequence** will be set to **CM-FS-Seq-App**. This is the Communication Manager Feature Server Application Sequence name. The **Survivability Server** is set to **None**. The **Home Location** will be set to **Location 1 Subnet 10.80.60.x**.



In order for the Endpoint Profile template information to be pushed from the Session Manager down to Communication Manager Feature Server, **enable** the **Endpoint Profile** box. The **System** was set to **CM-FS**. This is the Communication Manager Feature Server Entity Name. The **Extension** was set to **6663006** and the **Template** was set **to DEFAULT_9630SIP_CM_6_0**. The **Security Code** was set to **123456**. The **Port** was set to **IP**.



Repeat this section to add the remaining Avaya SIP Users assigned to station numbers in **Table 1**.

3.5. Administer Avaya Aura® Communication Manager Feature Server

This section highlights the important commands for defining Cisco SIP telephone as an Off-PBX Station (OPS) and administering a SIP Trunk and Signaling Group to carry calls between Cisco SIP and Avaya SIP endpoints in Communication Manager Feature Server.

3.5.1. Verify OPS Capacity

Use the **display system-parameters customer-options** command to verify that **Maximum Off-PBX Telephones – OPS** in has been set to the value that has been licensed, and that this value will accommodate addition of the SIP telephones. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to obtain additional capacity.

```
display system-parameters customer-options                     Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V16                              Software Package: Enterprise
       Location: 2                                 System ID (SID): 1
       Platform: 28                                Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 6400  62
                                      Maximum Stations: 2400  22
                              Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 9600  0
                    Maximum Off-PBX Telephones -   OPS: 9600  18
                    Maximum Off-PBX Telephones - PBFMC: 9600  0
                    Maximum Off-PBX Telephones - PVFMC: 9600  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   0
```

Verify that there are sufficient licenses to administer the SIP Trunk. This is the **Maximum Administered SIP Trunk** value on **Page 2** of System Parameter Customer-Options.

```
display system-parameters customer-options                     Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  0
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  2
                   Maximum Video Capable IP Softphones: 2400  7
                       Maximum Administered SIP Trunks: 4000  40
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
```

3.5.2. Administer Dial Plan Analysis

This section describes the **Dial Plan Analysis** screen**.** This is Communication Manager's way of translating digits dialed by the user. The user can determine the beginning digits and total length for each type of call that Communication Manager needs to interpret. The **Dialed String** beginning with the number 6663 and with a **Total Length** of 7 digits will be used to administer the **extension** range used for the SIP Telephones.

```
display dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 3

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   0            1   attd
   2            5   ext
   333          6   ext
   522          7   ext
   555          7   ext
   662          7   ext
   6663         7   ext
   6664         7   ext
   6665         7   ext
   777          7   ext
   778          7   ext
   *            2   fac
   *7           3   fac
   #            3   dac
```

3.5.3. Administer IP Node-Name

This section describes **IP Node-Name.** This is where Communication Manager assigns the IP Address and node-name to the SIP virtual interface of the Session Manager. The node-name of the Session Manager's SIP virtual interface is A**SM1-R6** and the IP Address is **110.80.120.28**. Communication Manager Feature Server automatically populates a processor node name to the IP Address of Communication Manager Feature Server. This node name is **procr** with IP Address 10.80.100.73.

```
list node-names all

                        NODE NAMES

Type      Name                 IP Address
IP        ASM1-R6              10.80.120.28
IP        ASM2-R6              10.80.120.30
IP        IPOR6                33.1.1.104
IP        default              0.0.0.0
IP        gateway1             10.80.100.1
IP        procr                10.80.100.73
IP        procr6               ::
```

3.5.4. Administer Signaling Group

This section describes the **Signaling Group** screen. The **Group Type** was set to **sip** and the **Transport Method** was set to **tcp**. Since the Cisco and Avaya SIP telephones are using a Communication Manager Feature Server for Off Pbx Station Mapping the **IMS Enabled** setting must be set to **yes**. Since the sip trunk is between Communication Manager Feature Server and Session Manager the **Near-end Node Name** is the node name of **procr** in the G450 Media Gateway for the Communication Manager Feature Server. The **Far-end Node Name** is the node name Session Manager's virtual SIP interface. This is **ASM1-R6**. The **Near-end Listen Port** and **Far-end Listen Port** are both set to port number **5060**. The **Far-end Network-Region** was set to **1.**

```
display signaling-group 10
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? y        Transport Method: tcp
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                    Far-end Node Name: ASM1-R6
 Near-end Listen Port: 5060                   Far-end Listen Port: 5060
                                           Far-end Network Region: 1

Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 10                      IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

3.5.5. Administer Trunk Group

This section describes **Trunk Group** used to carry calls between the Cisco 7960/7941 SIP telephones and the Avaya 9630 SIP telephones. Trunk Group 10 was configured as a SIP Trunk with the **Group Type** set as **sip.** The trunk **Group Name** was set to **SIP-IMS to ASM 1**. The **Direction** of the calls was set to **two-way** as there will be calls to and from the Cisco SIP telephones and Avaya SIP telephones. The **Service Type** was set to **tie** as the trunk is and internal trunk between Communication Manager Feature Server and Session Manager. The **Signaling Group** number assigned to this trunk is **10**. The **Number of Members** assigned to this trunk group is **20**. All other fields on this page are left as default.

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

Group Number: 10                   Group Type: sip          CDR Reports: y
  Group Name: SIP-IMS to ASM 1             COR: 1        TN: 1        TAC: #10
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 10
                                                     Number of Members: 20
```

3.5.6. Administer IP Network Region

This section describes **IP Network Region** screen**.** It was decided to place all SIP endpoints in the one network region. The **Authoritative Domain** must mirror the domain name of Session Manager. This was **avaya.com**. The codecs used on the SIP endpoints were placed in **Codec Set 3**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** were set to **yes.**

```
display ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name: SIP calls for ASM1
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 16535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

3.5.7. Administer IP Codec Set

This section describes the **IP Codec Set screen**. IP Codec **G.711MU, G.711A** and **G.729** were used for testing purposes with the Cisco and Avaya SIP endpoints.

```
display ip-codec-set 3                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 3

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.711A            n          2        20
 3: G.729             n          2        20
 4:
 5:
 6:
 7:


     Media Encryption
 1: none
 2:
 3:
```

3.5.8. Administer Off PBX Telephone Station Mapping

This section show the **off-pbx-telephone station-mapping**. The Cisco SIP telephone extensions 6663009 - 6663012 use off pbx **Application OPS** which is used for SIP enabled telephones. The SIP **Trunk Selection** is set to **aar**. The **Config Set** which is the desired call treatment was set to **1**.

```
display off-pbx-telephone station-mapping                       Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 666-3006         OPS         -       6663006          aar        1
 666-3007         OPS         -       6663007          aar        1
 666-3008         OPS         -       6663008          aar        1
 666-3009         OPS         -       6663009          aar        1
 666-3010         OPS         -       6663010          aar        1
 666-3011         OPS         -       6663011          aar        1
 666-3012         OPS         -       6663012          aar        1
```

The **Call Limit** is set to **6** as shown below. This is the maximum amount of simultaneous calls for extensions 6663009 - 6663012. The **Mapping Mode** field was set to **both** in this configuration setup. This is used to control the degree of integration between SIP telephones. The **Calls Allowed** field was set to **all**. This identifies the call filter type for a SIP Phone. The **Bridged Calls** field was set to **none** as it was not needed for testing purposes.

```
display off-pbx-telephone station-mapping                          Page   2 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station        Appl     Call        Mapping     Calls        Bridged        Location
 Extension      Name     Limit       Mode        Allowed      Calls
 666-3006       OPS       3        both        all          none
 666-3007       OPS       3        both        all          none
 666-3008       OPS       3        both        all          none
 666-3009       OPS       6        both        all          none
 666-3010       OPS       6        both        all          none
 666-3011       OPS       6        both        all          none
 666-3012       OPS       6        both        all          none
```

3.5.9. Administer Hunt Group

Hunt Group number **1** was administered and was assigned Group Name **Coverage to MM5.2**. Group Extension 666-4999 was assigned to hunt group 1. **UCD-MIA** was assigned as the Group Type.

```
display hunt-group 1                                               Page   1 of  60
                                  HUNT GROUP

            Group Number: 1                             ACD? n
              Group Name: Coverage to MM5.2           Queue? n
         Group Extension: 666-4999                   Vector? n
              Group Type: ucd-mia             Coverage Path:
                      TN: 1           Night Service Destination:
                     COR: 1                    MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display: grp-name
```

Select **sip-adjunct** for **Message Center.** The **Voice Mail Handle** was set to 6664999 the same value as the **Group Extension** on Page 1. The **Voice Mail Handle** was set to 6664999**.** The **Routing Digits *8** is used in the **Voice Mail Number** field as a Feature Access Code to access the SIP trunk the hunt group number goes out across.

```
display hunt-group 1                                               Page   2 of  60
                                  HUNT GROUP




                      Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle        Routing Digits
                                                 (e.g., AAR/ARS Access Code)
     6664999                   6664999                  *8
```

3.5.10. Add Coverage Path

Configure a coverage path for the Message Application Subscriber. Use the command **add coverage path n** where **n** is the coverage path number to be assigned. Configure a coverage point, using value **hx** where **x** is the hunt group number defined in **Section 3.5.9**. In this case its **hunt-group 1** or **h1** as shown below.

```
add coverage path n
                                 COVERAGE PATH

                   Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?            n               n
               Busy?            y               y
       Don't Answer?            y               y         Number of Rings: 2
                All?            n               n
 DND/SAC/Goto Cover?            y               y
   Holiday Coverage?            n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1               Rng: 2  Point2:
  Point3:                          Point4:
  Point5:                          Point6:
```

3.5.11. Administer Station Screen

This screen describes the **station** form setup for the Cisco SIP telephone on Communication Manager. Use the **change station xxxxxxx**, where xxxxxxx is the phone extension of the phone. In the sample configuration station **6663009** was used. Since the user was created and a phone type was assigned with an extension in **Section 3.4.11.1**, most of the fields should already be filled in with information. Use this form to set **Coverage Path 1** to **1**. Also, verify on page 6 of the station form that **SIP Trunk** is set to **aar**.

```
change station 6663009                                          Page   1 of   6
                                     STATION

Extension: 666-3009                      Lock Messages? n               BCC: 0
     Type: 9630SIP                       Security Code: 123456           TN: 1
     Port: S00030                      Coverage Path 1: 1               COR: 1
     Name: 7960-1, Cisco SIP           Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                Location:                  Time of Day Lock Table:
              Loss Group: 19
                                                 Message Lamp Ext: 666-3009

        Display Language: english                  Button Modules: 0

          Survivable COR: internal
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n
```

```
change station 6663009                                          Page   6 of   6
                                     STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: None
                    SIP Trunk: aar
```

Refer to **Table 1** and change the **Coverage Path 1** to **1** and check that **SIP Trunk** is set to **aar** for all stations created during the user administration in **Section 3.4.11**.

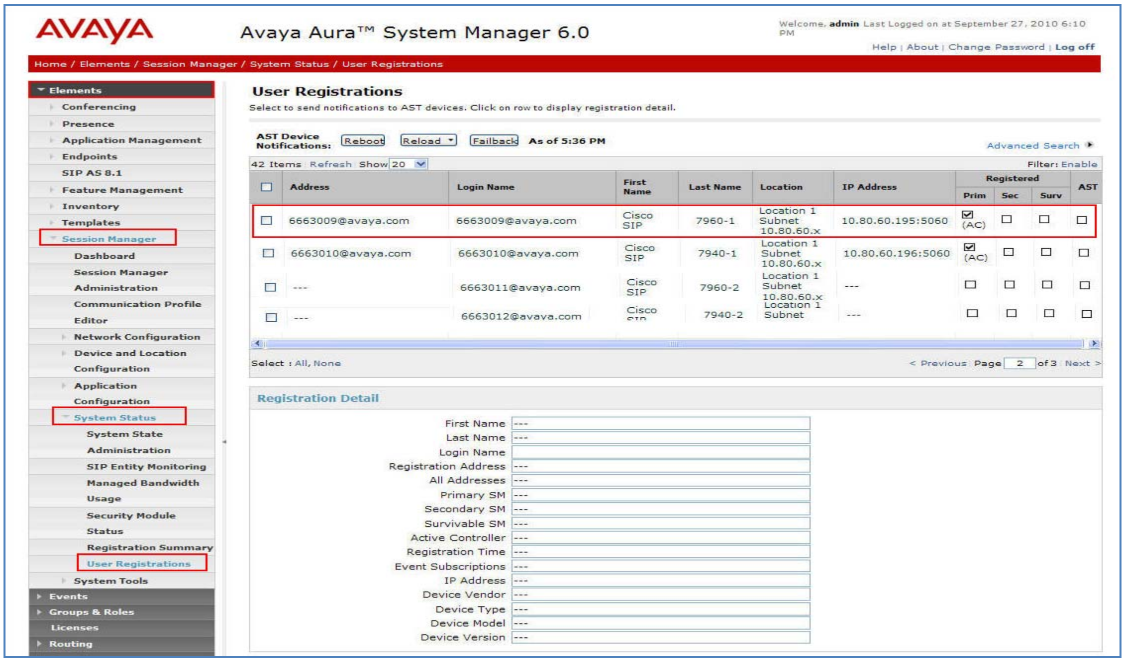
4. Verification

The following five verification steps were tested using the sample configuration. The following steps can be used to verify installation in the field.

1. Verified the Cisco 7940/7960 SIP Telephones were registered to the Session Manager.
2. Verified a call could be made with clear audio between the Cisco 7940 SIP Telephone and Cisco 7960 SIP Telephone. Verified the call was seen to be active on the SIP Trunk within Communication Manager. This was successful.
3. Verified a call could be made with clear audio from both the Cisco 7940/7960 SIP Telephones to the Avaya 9630 SIP Telephone. Verified the call was seen to be active on the SIP Trunk within Communication Manager. This was successful.
4. Verified supplementary features such as Call Hold, Call Forward, Conference and Transfer could be completed between the Cisco endpoints and the Avaya endpoints. This was successful.
5. Verified message could be retrieved and heard using message button on Cisco 7940/7960 SIP telephones. Note: Cisco 7940/7960 phones use the unsolicited notify method to turn on/off the MWI lamp. MM5.2 supports the unsolicited notify method, but the Session Manager released used in this application note does not currently support unsolicited notify messages and cannot pass them to the Cisco phones to turn on/off the MWI lamp.

4.1. Session Manager Registered Users

The following screen shows Session Manager registered users. This screen can be accessed from the left navigation menu **Elements → Session Manager → System Status → User Registrations** on System Manger GUI. If the the Cisco SIP phones are registered with Session Manager they will show up in the list with a checked box as being **Registered** on the **Prim** (Primary) with an **(AC)** (Active Controller) showing below. The AST box will not be checked as this is not an Avaya SIP phone.



5. Conclusion

These Application Notes have described the administration steps required to register Cisco 7940 and 7960 SIP Telephones to Avaya Aura® Session Manager with Avaya Aura® Communication Manager running as a Feature Server. SIP telephones that support IETF RFC 3842 (Subscribe/Notify method) will illuminate/extinguish the MWI lamp when voice messages are left/read for that extension. Cisco 7940/7960 SIP Phones do not support this standard, but support an unsolicited Notify method for MWI. The unsolicited Notify is not currently supported in this version of Session Manager. MM5.2 supports the unsolicited notify method, but the Session Manager release used in these application notes do not currently support unsolicited notify messages and cannot pass them to the Cisco phones to turn on/off the MWI lamp.

6. References

The following references are relevant to these Application Notes:

Avaya one-X Deskphone Edition 9600 Series SIP IP Telephones

[1] ***Avaya one-X™ Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.6***, Doc ID: 16-601944, Issue 6, June 2010, available at http://support.avaya.com.

Avaya Aura® Session Manager

[2] ***Avaya Aura™ Session Manager Overview***, Doc ID 03-603323, Issue 3, Release 6.0, June 2010, available at http://support.avaya.com.

[3] ***Installing and Configuring Avaya Aura™ Session Manager,*** Doc ID 03-603473, Issue 1.0, June 2010, available at http://support.avaya.com.

[4] ***Installing and Upgrading Avaya Aura™ System Manager***, Release 6.0, June 2010, available at http://support.avaya.com.

[5] ***Maintaining and Troubleshooting Avaya Aura™ Session Manager***, Doc ID 03-603325, Issue 1.0, Release 6.0, June 2010, available at http://support.avaya.com.

Avaya Aura® Communication Manager 6.0

[6] ***Administering Avaya Aura™ Communication Manager***, Doc ID 03-300509, Issue 6.0, Release 6.0, June 2010, available at http://support.avaya.com.

Cisco System Phones

[7] ***Cisco7940 and 7960 IP Phone Fireware Upgrade Matrix***, Cisco IOS Release 12.3(8)T, November 13, 2006, available at http://www.cisco.com.

[8] ***Converting a Cisco 7940/7960 Call Manager Phone to a SIP Phone***, Doc ID: 5455, March 20, 2009, available at http://www.cisco.com.

[9] ***Cisco Unified IP Phone 7960G and 7940G Administration Guide for Release 8.0 (SIP)***, Text Part Number: OL-7890-01, February 2007, available at http://www.cisco.com.

7. Appendix

7.1. OS79XX.TXT

```
P003-8-12-00
```

7.2. SYNCINFO.XML

```
<IMAGE VERSION="*" SYNC="1">
```

7.3. DIALPLAN.XML

```
<DIALTEMPLATE>
        <TEMPLATE MATCH="666...." TIMEOUT="0"/> <!-- Avaya HQ & Remote Branch -->
        <TEMPLATE MATCH="555...." TIMEOUT="0"/> <!-- Cisco 5.x, 6.x, 7.x Clusters -->
        <TEMPLATE MATCH="777...." TIMEOUT="0"/> <!-- Nortel/Avaya Heritage Phones -->
        <TEMPLATE MATCH="*"       TIMEOUT="5"/> <!-- Anything else -->
</DIALTEMPLATE>
```

7.4. SIPDEFAULT.CNF

```
image_version: "P0S3-8-12-00"

# Proxy Server
proxy1_address: "10.80.120.28"
# proxy2_address: "xxx.xxx.xxx.xxx"
# proxy3_address: "xxx.xxx.xxx.xxx"
# proxy4_address: "xxx.xxx.xxx.xxx"

# Proxy Server Port
proxy1_port:"5060"
# proxy2_port:"5060"
# proxy3_port:"5060"
# proxy4_port:"5060"
```

```
proxy_emergency: ""
proxy_emergency_port: "5060"
proxy_backup: ""
proxy_backup_port: "5060"
outbound_proxy: ""
outbound_proxy_port: "5060"

nat_enable: "0"
nat_address: ""
voip_control_port: "5060"
start_media_port: "16348"
end_media_port:  "20134"
nat_received_processing: "1"
dyn_dns_addr_1: "192.45.130.201"
dyn_dns_addr_2: "30.1.1.7"
dyn_tftp_addr: "192.45.130.201”
tftp_cfg_dir: "./"

proxy_register: "1"
timer_register_expires: "120"
preferred_codec: g711ulaw
tos_media: "5"
enable_vad: "0"
dial_template: "dialplan"
network_media_type: "auto"
autocomplete: "1"
telnet_level: "1”

cnf_join_enable: "1"
semi_attended_transfer: "1"
call_waiting: "1"
anonymous_call_block: "0"
callerid_blocking: "0"
dnd_control: "0"
transfer_onhook_enabled: "0"
call_hold_ringback: "0"
stutter_msg_waiting: "0"
cfwd_url: ""
call_stats: "0"
auto_answer: "0"
```

```
dtmf_inband: "1"
dtmf_outofband: "avt"
dtmf_db_level: "3"
dtmf_avt_payload: "101”
timer_t1: "500"
timer_t2: "4000"
sip_retx: "10"
sip_invite_retx: "6"
timer_invite_expires: "180"

sntp_mode: "directedbroadcast"
sntp_server: "xxx.xxx.xxx.xxx"
time_zone: "MST"
time_format_24hr: "1"
dst_offset: "1"
dst_start_month: "April"
dst_start_day: ""
dst_start_day_of_week: "Sun"
dst_start_week_of_month: "1"
dst_start_time: "2"
dst_stop_month: "Nov"
dst_stop_day: "1"
dst_stop_day_of_week: "Sunday"
dst_stop_week_of_month: ""
dst_stop_time: "2"
dst_auto_adjust: "1"

messages_uri: "6664999"
mwi_status: "1"


services_url: "http://example.domain.ext/services/menu.xml”
directory_url: "http://example.domain.ext/services/directory.php"
logo_url: "http://192.45.130.201/PhoneLogo/AvayaPhoneLogo.bmp”

http_proxy_addr: ""
http_proxy_port: 80
remote_party_id: 0
```

7.5. SIP0003E311F2D1.cnf

```
proxy1_address: "10.80.120.28"
proxy2_address: "xxx.xxx.xxx.xxx"
proxy3_address: "xxx.xxx.xxx.xxx"
proxy4_address: "xxx.xxx.xxx.xxx"

line1_name: "6663009"
line1_shortname: "Cisco SIP 6663009"
line1_displayname: "Cisco SIP 6663009"
line1_authname: "6663009"
line1_password: "123456"

line2_name: ""
line2_shortname: ""
line2_displayname: ""
line2_authname: "6663009"
line2_password: "123456"

line3_name: ""
line3_shortname: ""
line3_displayname: ""
line3_authname: "UNPROVISIONED"
line3_password: "UNPROVISIONED"

line4_name: ""
line4_shortname:
line4_displayname: ""
line4_authname: "UNPROVISIONED"
line4_password: "UNPROVISIONED"

line5_name: ""
line5_shortname: ""
line5_displayname: ""
line5_authname: "UNPROVISIONED"
line5_password: "UNPROVISIONED"

line6_name: ""
line6_shortname: ""
line6_displayname: ""
line6_authname: "UNPROVISIONED"
line6_password: "UNPROVISIONED"

proxy_emergency: ""
proxy_emergency_port: "5060"
proxy_backup: ""
proxy_backup_port: "5060"
outbound_proxy: ""
outbound_proxy_port: "5060"
```

```
nat_enable: "0"
nat_address: ""
voip_control_port: "5060"
start_media_port: "16348"
end_media_port:  "20134"
nat_received_processing: "0"
messages_uri: "6664999"

phone_label: "Registered To Avaya  "
time_zone: CST
logo_url: "http://192.45.130.201/PhoneLogo/AvayaPhoneLogo.bmp"

telnet_level: "2"
phone_prompt: "Cisco7960"
phone_password: "cisco"
enable_vad: "0"
network_media_type: "auto"
user_info: phone
```

7.6. RINGLIST.DAT

```
FlintPhone      FlintPhone.raw
HarpSynth       HarpSynth.raw
Jamaica         Jamaica.raw
Klaxons         Klaxons.rar
KotoEffect      KotoEffect.raw
MusicBox        MusicBox.raw
Ohno            Ohno.raw
Piano 1         Piano1.raw
Piano 2         Piano2.raw
```

7.7. SEP0003E311F2D1.cnf.xml

```
<device>
<deviceProtocol>SIP</deviceProtocol>
<loadInformation model="IP Phone 7960G">P0S3-8-12-00</loadInformation>
</device>
```

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com