Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Cisco Unified Communications Manager Release 6.0 – Issue 1.0

Abstract

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager and Cisco Unified Communications Manager Release 6 using SIP trunks.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, Avaya Aura™ Communication Manager runs on an Avaya S8300 Server with an Avaya G430 Media Gateway, and Cisco Unified Communications Manager runs on a Cisco network appliance. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager.

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager and Cisco Unified Communications Manager (Cisco UCM) Release 6 using SIP trunks. These Application Notes supplement previously published Application Notes [6] that illustrate a similar configuration using Cisco UCM Release 7 with an earlier version of Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager.

2. Overview

The sample network is shown in **Figure 1**. Avaya Aura™ Communication Manager is supporting the Avaya 9630 IP Telephone (H.323) and 6408D+ Digital Telephone. Cisco UCM supports the Cisco 7960G IP Telephone (SCCP) and the Cisco 7961G IP Telephone (SIP). SIP trunks are used to connect Avaya Aura™ Communication Manager and Cisco UCM to Avaya Aura™ Session Manager. All inter-system calls are carried over the SIP trunks to Avaya Aura™ Session Manager, allowing Session Manager to perform "adaptations" to improve the interoperability profile. For example, Session Manager will extract display information that Cisco UCM places in the "Remote-Party-ID" of a SIP message and relocate the information so that Communication Manager will process and display the information. Similarly, Session Manager will extract display information received from Communication Manager and populate the display information in the Remote-Party-ID for consumption by Cisco UCM. Further information on this adaptation can be found in Section 8.

Avaya Aura™ Session Manager is managed by a separate Avaya Aura™ System Manager, which can manage multiple instances of Avaya Aura™ Session Managers. The initial configuration of Avaya Aura™ System Manager and Avaya Aura™ Session Manager are not the focus of these Application Notes. These Application Notes focus on the aspects of the configuration related to the SIP Trunk interoperability with Avaya Aura™ Communication Manager and Cisco UCM.

3. Configuration

Figure 1 illustrates the configuration used in these Application Notes. The telephones controlled by Avaya Aura™ Communication Manager have extensions of the form 143xx. The telephones controlled by Cisco UCM have extensions in the range 55xxx. A five-digit Uniform Dial Plan (UDP) is used for dialing between systems. A single SIP trunk is provisioned from Avaya Aura™ Communication Manager and Cisco UCM to Avaya Aura™ Session Manager to manage call control for calls between the two systems.

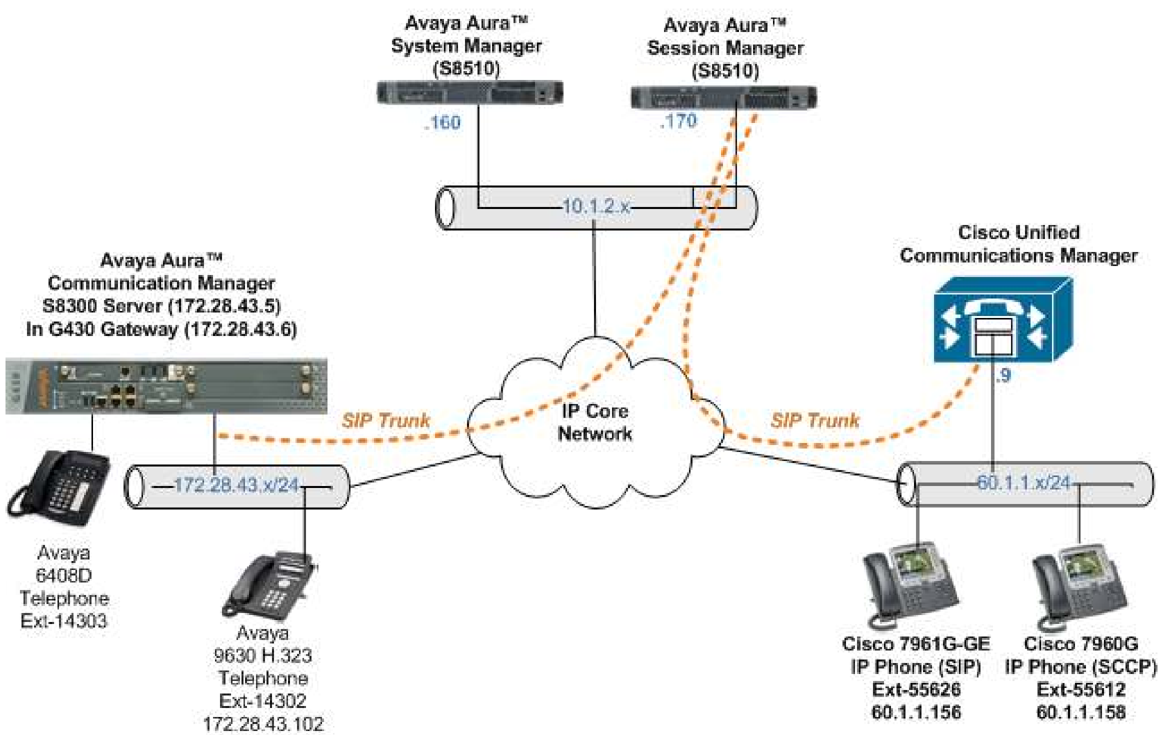


Figure 1: Sample Network Configuration

4. Equipment and Software Validated

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

DEVICE DESCRIPTION	VERSION TESTED
Avaya Aura™ Communication Manager - Running on an Avaya S8300 Server with an Avaya G430 Media Gateway	R 5.2 (R015x.02.0.947.3) SP1 (02.0.947.3-17294)
Avaya Aura™ System Manager - Running on an Avaya S8510 Server	1.1.4.0.111013
Avaya Aura™ Session Manager - Running on an Avaya S8510 Server	1.1.4.0.111013
Avaya 9630 IP Telephone (H.323)	3.0
Avaya 6408D Digital Telephone	-
Cisco Unified Communications Manager	6.0.1-2000-3
Cisco 7960G Unified IP Phone (SCCP)	Version 8.0(5.0) P00308000500 (App Load)
Cisco 7961G-GE Unified IP Phone (SIP)	SIP41.8-3-1S (Load file) Jar41sp.8-3-050.sbn (App Load)

5. Configure Avaya Aura™ Communication Manager

This section illustrates relevant configuration for Communication Manager SIP Trunking to Session Manager. The configuration in this section uses the System Access Terminal (SAT) interface, and screens may be abridged for brevity in presentation. For further information on Communication Manager, please consult references [4] and [5].

A license file controls availability of Communication Manager features and capacities. It is assumed that appropriate licensing is in place to support the configuration of SIP Trunking. Reference [6] provides a procedure for verifying license capacity.

5.1. Node Names

Node names are mappings of names to IP Addresses that can be used in various screens. The following abridged screen shows the relevant node-names used in the sample configuration. **Name** "ASM" and **IP Address** "10.1.2.170" are entered for Avaya Aura™ Session Manager. The IP Address of the S8300 processor Ethernet named "procr" is configured via the Web administration of the S8300 Server. Here, it can be observed that "procr" and "172.28.43.5" are the **Name** and **IP Address** for Avaya Aura™ Communication Manager running on the Avaya S8300 Server. For other system types, where an Avaya C-LAN card is used as the SIP signaling interface, the node name and IP Address of the C-LAN card would be entered here.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM                 10.1.2.170
procr               172.28.43.5
```

5.2. Network Regions

Network regions provide a means to logically group resources. Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that media gateway 1 is an Avaya G430 Media Gateway configured for network region 1.

```
display media-gateway 1
                              MEDIA GATEWAY
         Number: 1                           Registered?  y
           Type: g430              FW Version/HW Vintage: 29 .22 .3  /0
           Name: G430                     MGP IP Address: 172.28 .43 .6
      Serial No: 09IS05214297      Controller IP Address: 172.28 .43 .5
   Encrypt Link? y                           MAC Address: 00:07:3b:e4:68:91
 Network Region: 1    Location: 1              Enable CF? n
                                               Site Data:
  Recovery Rule: none

Slot   Module Type            Name                   DSP Type  FW/HW version
 V1:   S8300                  ICC MM                 MP20      16   0
 V2:   MM710                  DS1 MM
 V3:   MM712                  DCP MM

 V5:                                                 Expansion Type HW version
 V6:   MM711                  ANA MM                 EM200          0
 V7:
 V8:                                               Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```

IP telephones can be assigned a network region based on an IP address mapping. The following screen illustrates a subset of the IP network map configuration. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. Strictly speaking, this ip-network-map configuration is not necessary, since default region 1 is used for the Avaya IP Telephones.

```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING
                                               Subnet Network     Emergency
 IP Address                                    Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 172.28.43.100                           /      1      n
   TO: 172.28.43.110
```

The following screen shows IP Network Region 1 configuration. Connections within network region 1 use codec set 1 by virtue of the **Codec Set** configuration shown on Page 1 below. For the **Authoritative Domain** field, enter the SIP domain configured for this enterprise. Optionally, a descriptive **Name** can be configured. To enable direct media connections for calls between the Avaya devices in network region 1, ensure that the **Intra-region IP-IP Direct Audio** is set to "yes". To permit direct media connections to other regions (unless otherwise prohibited by the other region), set the **Inter-region IP-IP Direct Audio** field to "yes".

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name: Avaya devices
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 3, and that codec set 3 will be used for connections between region 1 and region 3. Later, when the SIP signaling group is defined, the "far-end region" will be set to network region 3. Having different network regions for the local Avaya devices and the far-end of a SIP trunk allows different codec parameters for intra-region connections (e.g., using codec set 1 for Avaya connections) and inter-region connections (e.g., using codec set 3 for Avaya-Cisco connections in the sample configuration). Once submitted, the configuration becomes symmetric, meaning that network region 3, Page 3 will also show codec set 3 for region 3 – region 1 connectivity.

```
change ip-network-region 1                                      Page   3 of  19

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1                                                                all
 2    2     y    NoLimit                                             n
 3    3     y    NoLimit                                             n
```

The following screen shows page 1 of the IP Network Region 3 configuration. Observe that the **Inter-region IP-IP Direct Audio** field has been set to “no”. As a result of interoperability issues summarized in Section 8.4, it is recommended to disable “shuffling” to direct media for connections between Cisco UCM devices in region 3 and Avaya devices in other regions (e.g., 1). Alternatively, direct media connections could be disabled on signaling group 26 (configured in Section 5.4).

```
change ip-network-region 3                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 3
Location:         Authoritative Domain:
    Name: Far-end-SIP
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

The following screen shows page 3 of the IP Network Region 3 configuration. The bolded row illustrates the symmetric configuration of the region 3-1 connectivity, using codec set 3.

```
change ip-network-region 3                                      Page   3 of  19

 Source Region: 3     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    3     y    NoLimit                                             n
 2
 3    3                                                                all
```

5.3. IP Codec Sets

The following screens show the configuration for codec sets 1 and 3. In general, an IP codec set is a list of allowable codecs in priority order. In the sample configuration, all connections among the Avaya devices use codec set 1, preferentially using G.711MU with SRTP encryption, as shown below.

```
change ip-codec-set 1                                          Page   1 of   2
                         IP Codec Set
   Codec Set: 1

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

    Media Encryption
1: 1-srtp-aescm128-hmac80
2: aes
3: none
```

In the sample configuration, all connections between the Avaya devices and the Cisco devices will use codec set 3, specified for inter-region connections between region 1 and region 3. During the testing, the codec parameters for codec set 3 were varied, with successful calls using G.711MU and variants of G.729, each with no encryption. For more information on G.729 variants, see Section 8.4.

```
change 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:
3:
4:
5:
6:
7:

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

5.4. SIP Signaling Group

This section illustrates the configuration of the SIP Signaling Group to Session Manager. The signaling group has a **Group Type** of "sip", and a **Near-end Node Name** of "procr", the S8300 Server. The **Far-end Node Name** is the node name "ASM" for Session Manager. The **Transport Method** is "tls", and the **Near-End Listen Port** and **Far-End Listen Port** use port 5061. The **Far-end Domain** has been configured to be "3", to allow different behaviors, such as codec selection, for intra-region and inter-region calls. Although not required, the **Enable Layer 3 Test** parameter is enabled to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Other fields can be left at default values, including "DTMF over IP" set to "rtp-payload" which corresponds to RFC 2833.

```
change signaling-group 26                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 26              Group Type: sip
                        Transport Method: tls
  IMS Enabled? n
     IP Video? n

   Near-end Node Name: procr                 Far-end Node Name: ASM
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 3
Far-end Domain:
                                             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): 6
```

5.5. SIP Trunk Group

This section illustrates the configuration of the SIP Trunk Group 26 to Session Manager. The trunk group has a **Group Type** of "sip". An appropriate Trunk Access Code (**TAC**) and **Group Name** are configured. Trunk group 26 is associated with **Signaling Group** 26, and the **Number of Members** field is 10, indicating that this trunk group can support ten simultaneous calls.

```
change trunk-group 26                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 26                   Group Type: sip           CDR Reports: y
  Group Name: ASM trunk                   COR: 1        TN: 1        TAC: 126
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                      Signaling Group: 26
                                                    Number of Members: 10
```

The following shows Page 2 for trunk group 26. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default value 600 to 900 to avoid unnecessary SIP messaging with Cisco UCM to negotiate to a higher refresh interval during call establishment.

```
change trunk-group 26                                           Page   2 of  21
      Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                             Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
```

The following shows Page 3 for trunk group 26. All parameters shown are at default values, with the exception of the bold fields, which optionally allow an Avaya-configured display string to appear on display-equipped telephones in the event that an anonymous or restricted incoming call is received from this trunk group. (The replacement display strings can be configured on page 9 of the “change system-features” form, not shown). In the sample configuration, the default “public” numbering is used, but private numbering may also be used.

```
change trunk-group 26                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
```

The following shows Page 4 for trunk group 26. All parameters shown are at default values, with the exception of the **Telephone Event Payload Type** associated with DTMF signaling, which has been set to the value “101”.

```
change trunk-group 26                                           Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 101
```

5.6. Public Numbering

The “change public-unknown-numbering” command may be used to define the format of numbers such as the “calling party number”. In the bolded row shown in the abridged output below, all calls originating from a 5-digit extension beginning with 143 (i.e., 143xx) will not have any number prefixed, but rather a 5 digit calling party number will be sent, when Trunk Group 26 is selected for the call. In the sample configuration, this allows the Avaya user’s five digit telephone extension to appear on the display of the Cisco telephones. In a production environment, other rows in this table may be used to ensure that an appropriate calling party number is sent for calls routed via trunks to the PSTN.

```
change public-unknown-numbering 0                              Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext              Trk       CPN          CPN
Len Code             Grp(s)    Prefix       Len
                                                     Total Administered: 4
 5  143              26                     5           Maximum Entries: 240
```

5.7. Uniform Dial Plan

The Uniform Dial Plan (UDP) is configured such that calls matching the 55xxx extension range of Cisco telephones are part of the overall UDP configuration. The following screen shows a sample UDP configuration. When a user dials a 5 digit extension beginning with 55 (i.e., 55xxx), the call will use Automated Alternate Routing (AAR) for further analysis.

```
change uniform-dialplan 5                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 0
  Matching                  Insert              Node
  Pattern       Len Del     Digits     Net Conv Num
 55              5   0                 aar  n
```

5.8. AAR Analysis

The AAR Analysis table is configured such that calls matching the 55xxx extension range of Cisco telephones are routed to **Route Pattern** 25, as shown below.

```
change aar analysis 55                                         Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all         Percent Full:    2

          Dialed           Total     Route    Call   Node  ANI
          String         Min  Max  Pattern    Type   Num   Reqd
    55                   5    5      25       aar          n
```

5.9. Route Pattern Configuration

Route pattern 25 is configured to include trunk group 26, the SIP trunk group to Avaya Aura™ Session Manager, as shown below.

```
change route-pattern 25                                         Page   1 of   3
                    Pattern Number: 25  Pattern Name: To-ASM
                             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: 26   0                                                            n   user
 2:                                                                   n   user
 3:                                                                   n   user
 4:                                                                   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                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 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
```

5.10. Saving Configuration Changes

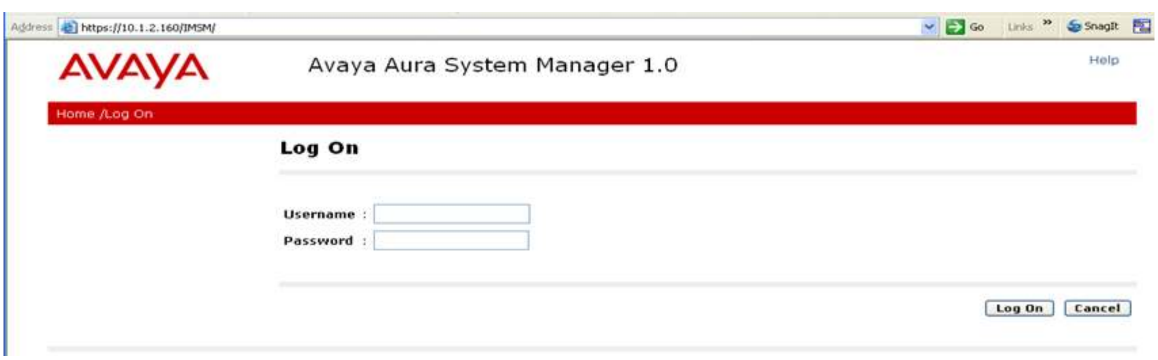
The command “save translation all” can be used to save the configuration.

6. Configuring Avaya Aura™ Session Manager

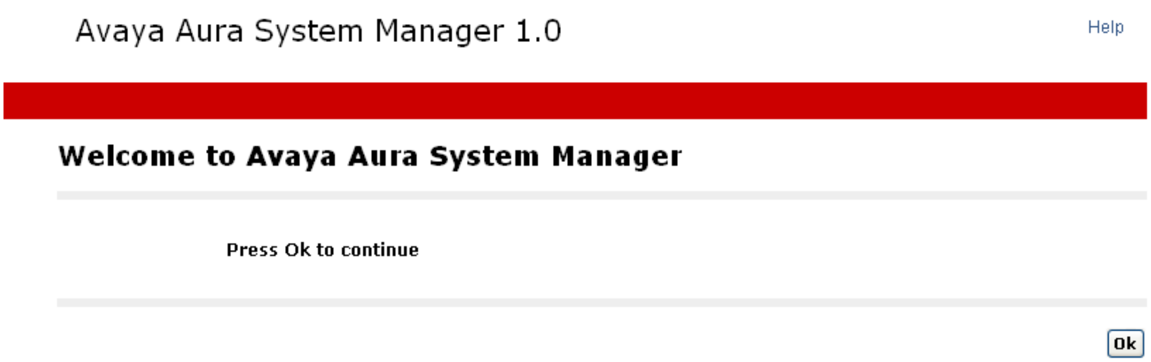
This section illustrates the procedures for configuring Avaya Aura™ Session Manager to interoperate with Cisco UCM. For further information on Avaya Aura™ Session Manager, please consult references [1], [2], and [3]. The configuration procedures include the following areas:

- SIP Domains – the domains for which Avaya Aura™ Session Manager is authoritative for routing SIP calls
- Locations – the logical or physical location of a SIP entity, which can be used for location-based routing or bandwidth management and call admission control
- Adaptations – SIP protocol adaptations (e.g., SIP header manipulations) can be used to improve and simplify interoperability with other SIP entities. Digit conversion adaptations can be used to modify digit strings on ingress/egress to Session Manager to normalize and simplify configuration of a common dial plan among systems that may have disparate dial plans
- SIP Entities – SIP entities correspond to the SIP telephony systems and Avaya Aura™ Session Manager instances.
- Entity Links - define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
- Time Ranges - allow time-based criteria for call routing
- Routing Policies - configurable call routing between the SIP Entities
- Dial Patterns – configurable criteria for call routing (e.g., called party number pattern matching) and routing policies to be used when criteria are met

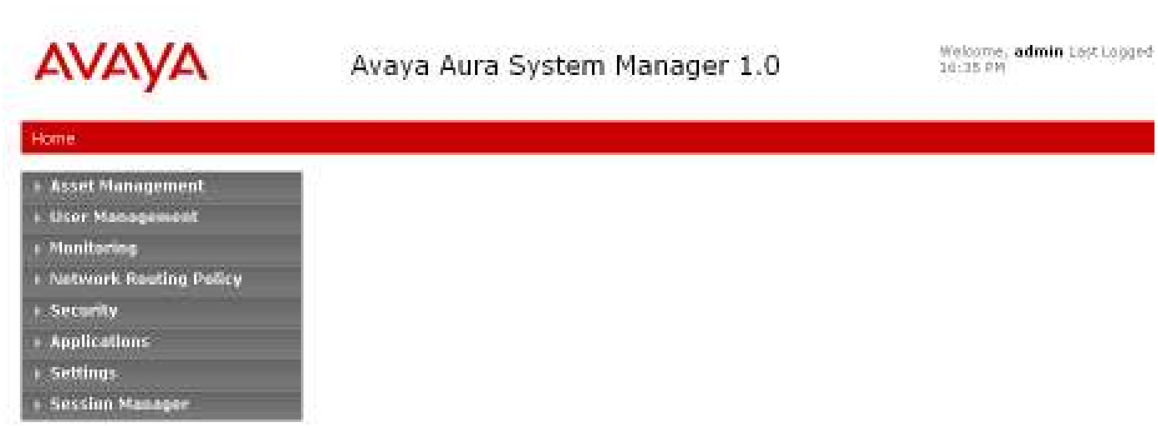
Access the System Manager using a Web Browser and enter http://<ip-address>/IMSM, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials.



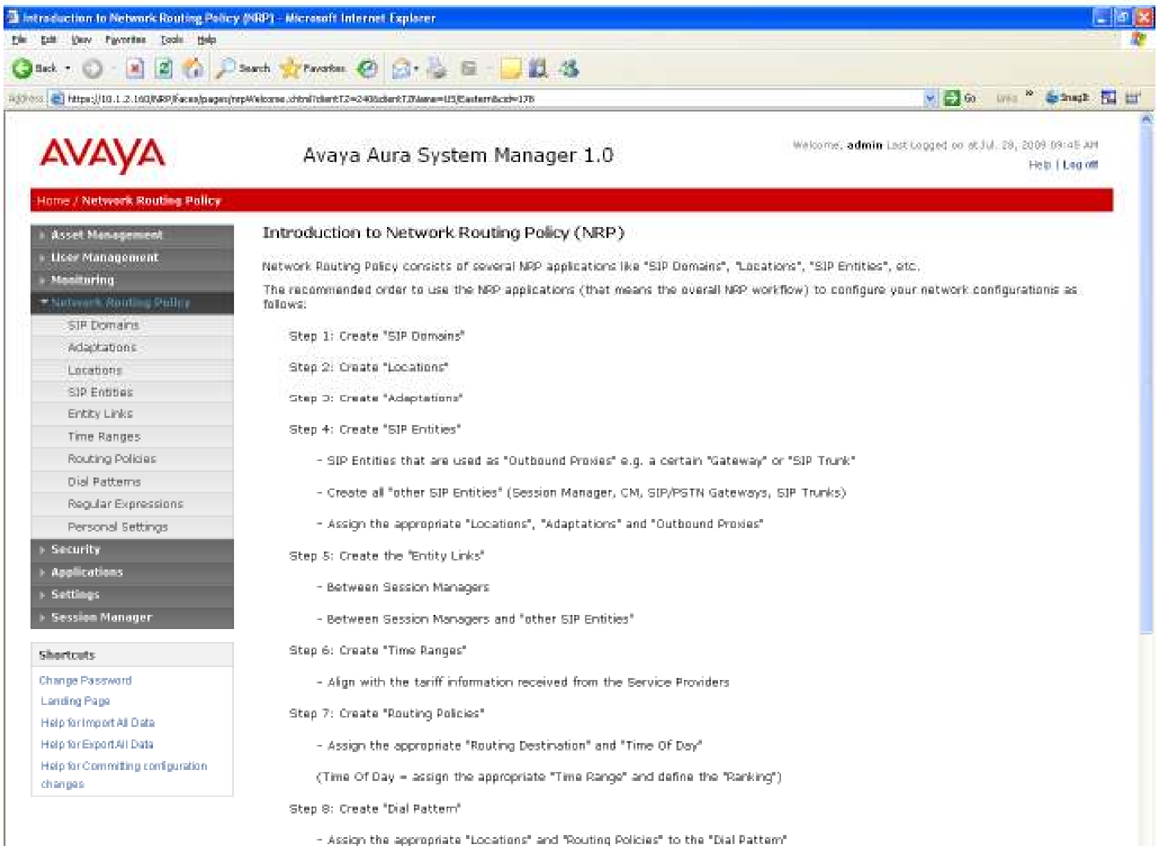
After successful log in, press **Ok** to continue.



After clicking **Ok**, the following screen is displayed.



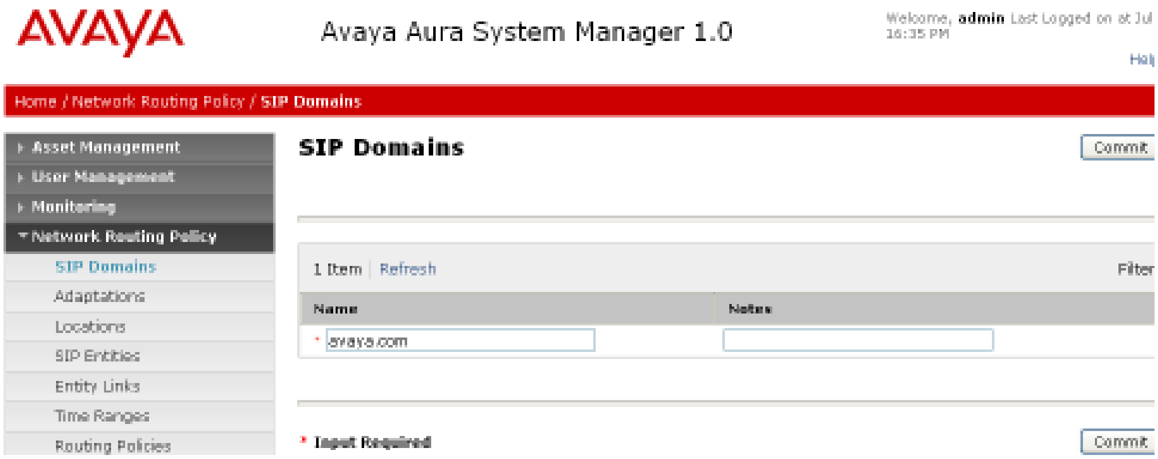
Select **Network Routing Policy** from the left panel menu. The following screen shows the options under the **Network Routing Policy** heading. The right hand side contains a step by step overview for configuring the Network Routing Policy. The steps referenced in the screen below correspond to the sub-heading numbers in this section.



6.1. Configure the SIP Domain

To add the SIP domain for which the communications infrastructure will be authoritative, select **Network Routing Policy → SIP Domains** on the left as shown below.

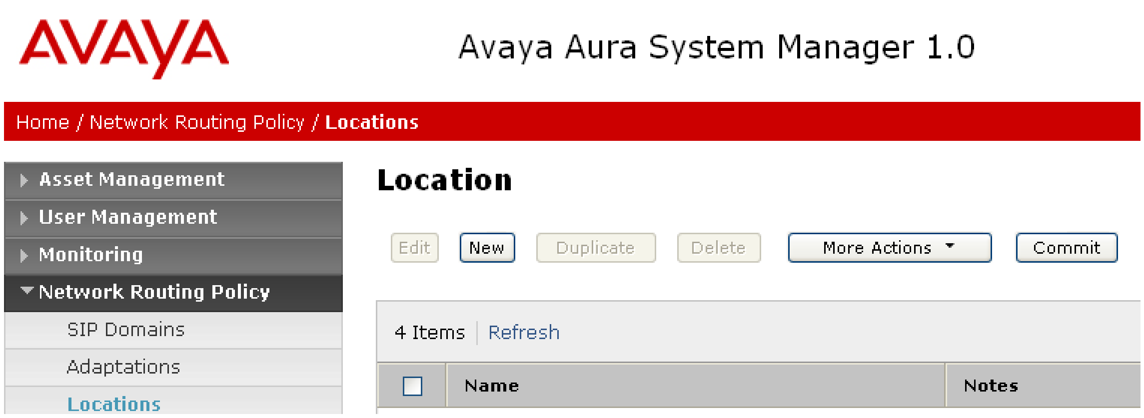
Click the **New** button. On the screen shown below, enter the authoritative domain name (e.g., "avaya.com") in the **Name** field. Optionally, enter descriptive text in the **Notes** field. Click the **Commit** button.



6.2. Configure Locations

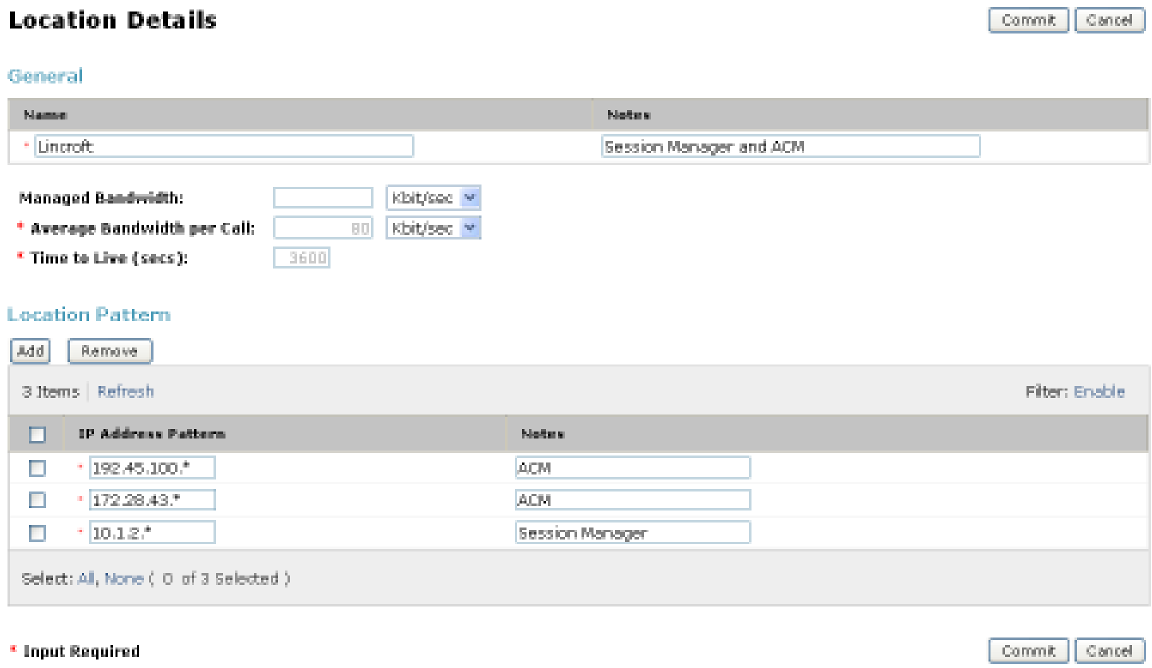
Locations can be used to identify logical or physical locations where SIP entities reside. If desired, the location of the originator of a call can be used as a routing criterion or for bandwidth management purposes. The screens associated with locations are illustrated below, although routing decisions in the sample configuration are not determined by the location, and bandwidth management techniques are not illustrated.

To configure locations, select **Network Routing Policy → Locations**, as shown below.

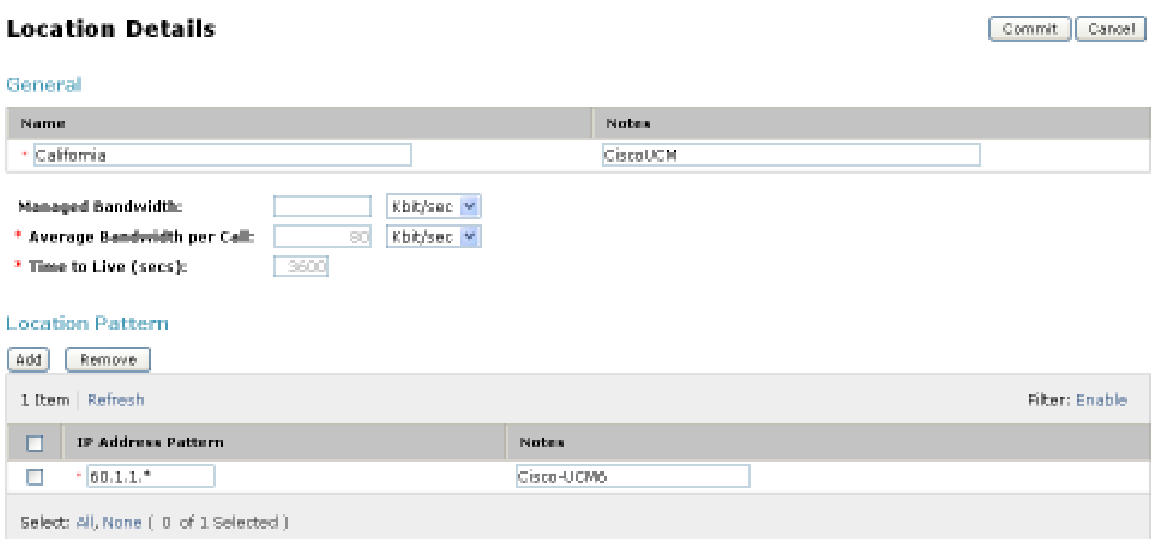


To add a new location, click **New**, or select a location from the list of existing locations.

The following screen shows the location whose **Name** is “Lincroft”. In the sample configuration, Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager are configured for the “Lincroft” location. The **IP Address Pattern** “10.1.2.*” corresponds to IP Addresses used for Session Manager, and “172.28.43.*” corresponds to IP Addresses used for Communication Manager.



The following screen shows the location whose **Name** is “California”. In the sample configuration, Cisco UCM is configured for the “California” location. As shown in **Figure 1**, the **IP Address Pattern** “60.1.1.*” corresponds to the IP Addresses used for Cisco UCM and the associated Cisco IP Telephones.

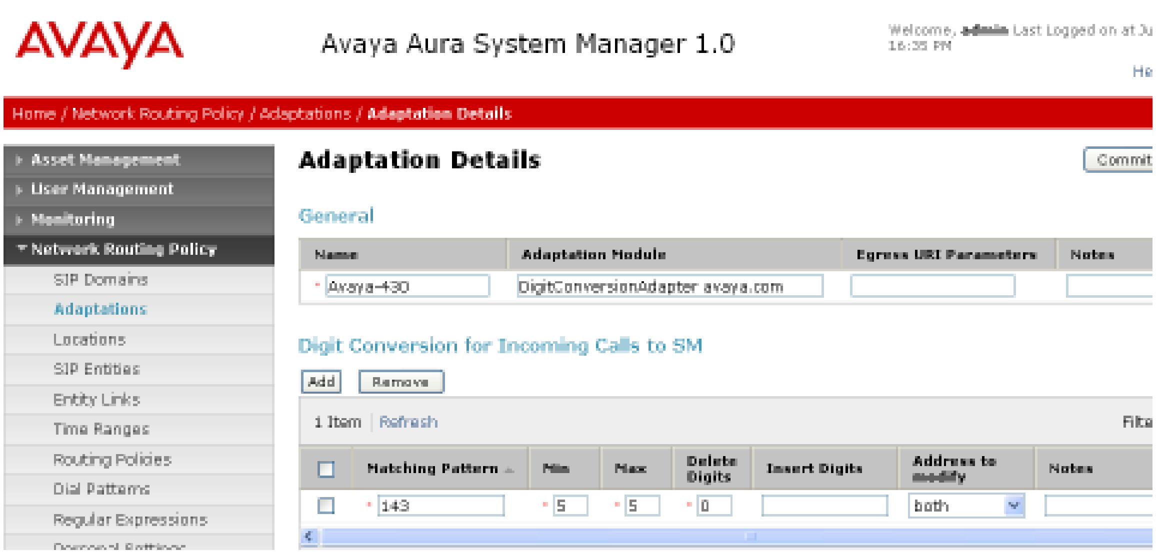


6.3. Configure Adaptations

To configure adaptations, select **Network Routing Policy → Adaptations**, as shown below.

Click the **New** button. In the sample configuration, both Avaya Aura™ Communication Manager and Cisco UCM used a uniform five-digit dial plan. As such, it is not necessary for System Manager to normalize the dial plan, but the following information was configured to illustrate the general mechanism:

Name A descriptive name for the adaptation (e.g., "Avaya-430")
Adaptation Module Enter "DigitConversionAdapter avaya.com"
Digit Conversion for Incoming Calls to SM
Matching Pattern 143 with a minimum and maximum length of 5 digits. This configuration corresponds to the range of local extensions on Avaya Aura™ Communication Manager.

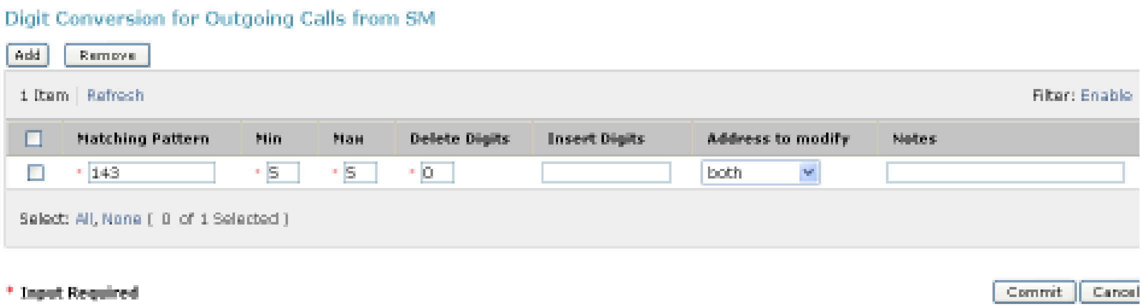


Return to **Network Routing Policy → Adaptations**. Click the **New** button to define an adaptation that will use the "CiscoAdapter". The CiscoAdapter converts SIP messaging traffic, such that Cisco UCM and Avaya Aura™ Communication Manager receive SIP message information (e.g., display information) where expected. See Section 8 for more specific information on the CiscoAdapter.

In the sample configuration, the following information was configured, and remaining fields were left at default values:

Name CiscoUCM-6, a descriptive name for the adaptation
Adaptation Module Enter "CiscoAdapter avaya.com"
Digit Conversion for Incoming Calls to SM
Matching Pattern 55 with a minimum and maximum length of 5 digits, corresponding to the extension range used by the telephones controlled by Cisco UCM.

In the sample configuration, it was not necessary to configure digit conversion for outgoing calls from Session Manager. However, to illustrate the screen, the following shows the **Digit Conversion for Outgoing Calls from SM** section of the **Adaptation Details** screen.



When finished, click the **Commit** button.

6.4. Configure SIP Entities

A SIP Entity must be added for the Avaya Aura™ Session Manager instance, and for each SIP-based system networked with Session Manager using SIP trunks. In the sample configuration, a SIP Entity is configured for Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Cisco UCM.

To configure SIP Entities, select **Network Routing Policy → SIP Entities**, as shown below. Any existing SIP Entities will be listed.

Click **New**. In the screen that is presented, enter the appropriate information for the SIP Entity. The following list provides guidance for the fields under the **General** heading:

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: IP Addresses are used in the sample configuration. Enter the IP Address of the Session Manager instance, or the SIP signaling interface for Communication Manager or Cisco UCM, as appropriate for the entity being configured.

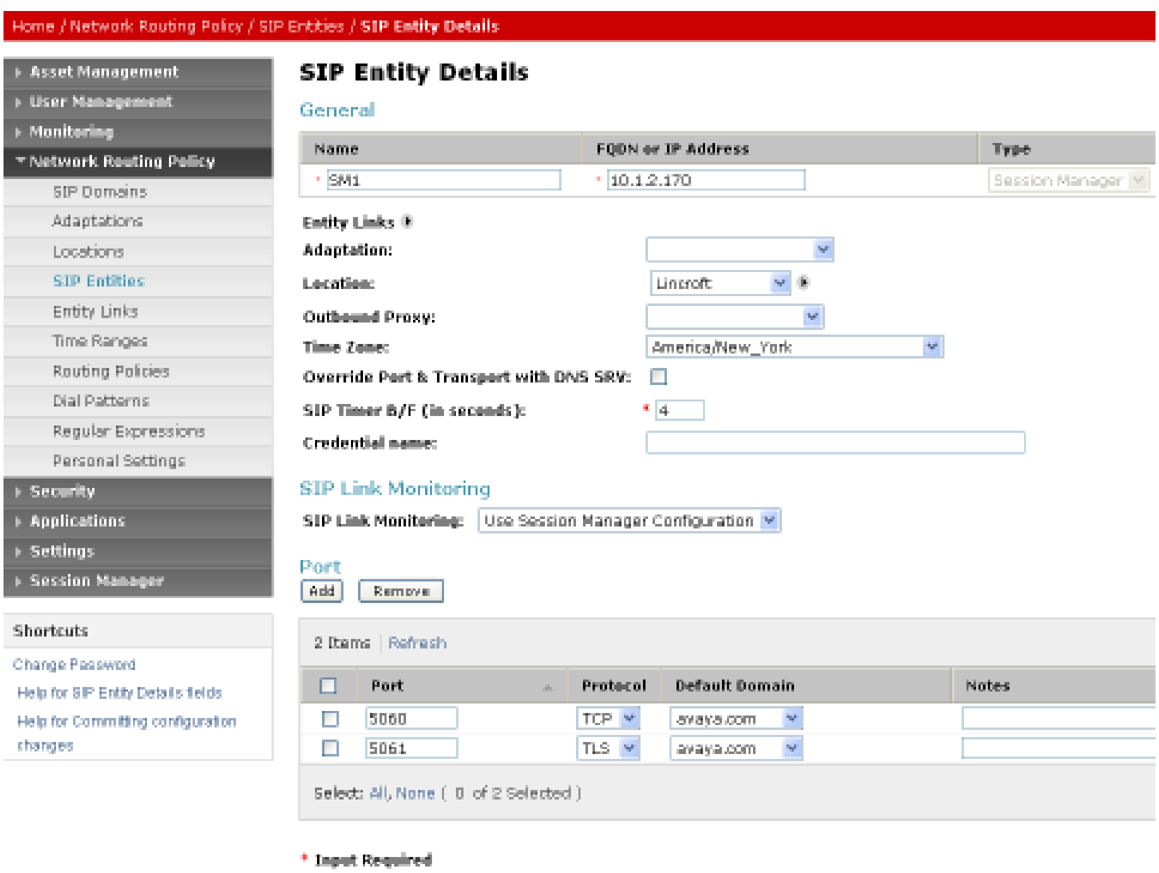
- **Type**: Choose "Session Manager" for the Session Manager SIP entity, "CM" for the Communication Manager SIP entity, and "Other" for Cisco UCM.
- **Adaptation**: For the Cisco UCM and Avaya Aura™ Communication Manager SIP entities, select the appropriate adaptation from the drop-down, as previously configured in Section 6.3.
- **Location:** Optionally, select a location previously configured in Section 6.2.
- **Time Zone:** Enter appropriate time zone for the SIP entity.

The following list provides guidance for the fields under the **Port** heading:

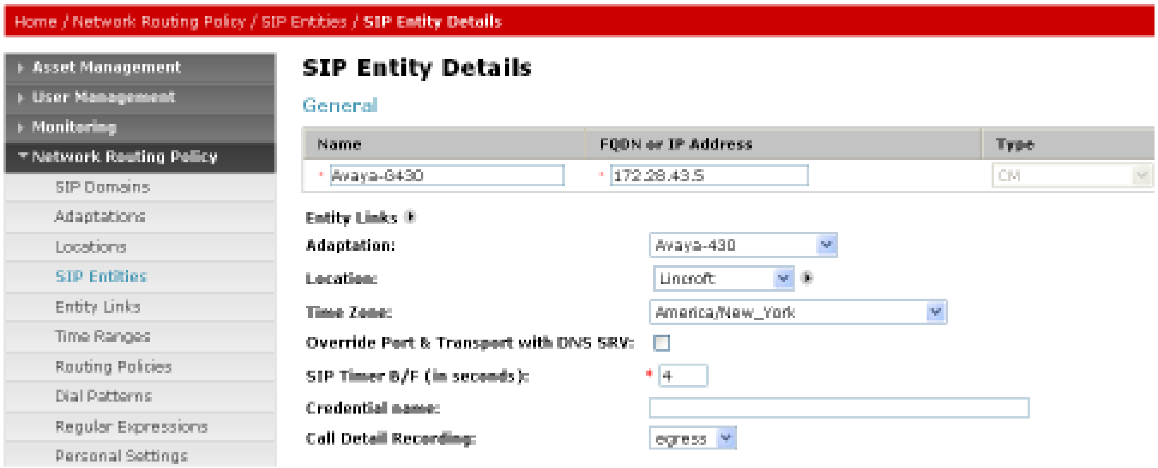
- **Port**: Port number on which the SIP entity listens for SIP requests
- **Protocol:** Transport protocol used for SIP requests
- **Default domain**: the appropriate SIP domain (e.g., "avaya.com" as defined in **Section 6.1**)

Default values can be used for the remaining fields. Click **Commit** to save each SIP entity definition.

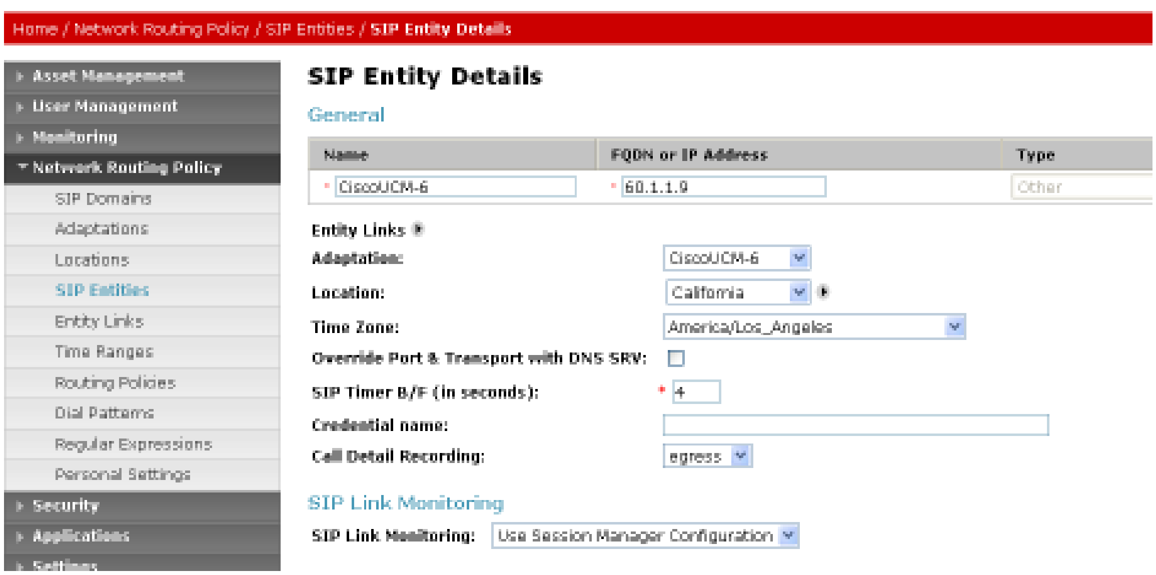
The configuration for the Session Manager SIP entity "SM1" is shown below. The configuration of the "SM1" SIP Entity is identical to the configuration previously illustrated and described in reference [6], which can be consulted if necessary.



Return to **Network Routing Policy → SIP Entities**, and click **New** to add the configuration for the Communication Manager SIP entity with **Name** “Avaya-G430”. The configuration of the Avaya-G430 SIP Entity is the same as the configuration previously described in reference [6].

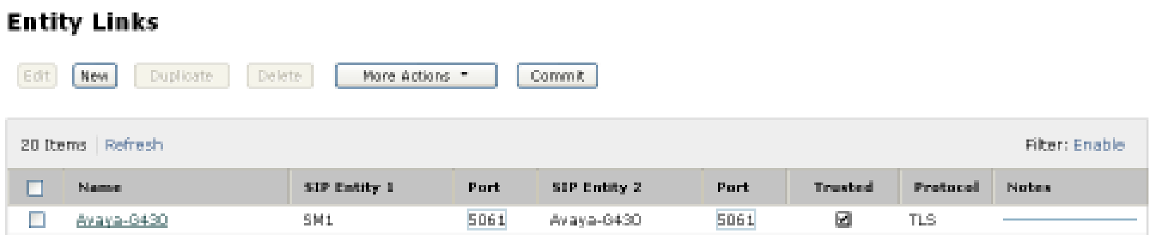


Return to **Network Routing Policy → SIP Entities**, and click **New** to add the configuration for the Cisco UCM SIP Entity. In the **Name** field, enter a descriptive name, such as “CiscoUCM-6”. The IP Address of Cisco UCM running Release 6 is 60.1.1.9 as can be seen in **Figure 1**. The **Type** is set to “Other”. “CiscoUCM-6” is selected as the **Adaptation**, and “California” is selected for the **Location** field. An appropriate **Time Zone** is selected for the location.



6.5. Configure Entity Links

A SIP trunk between Avaya Aura™ Session Manager and another SIP entity is described by an entity link. An entity link between Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager is required, and the configuration of this entity link is identical to the configuration of the link named "Avaya-G430" from reference [6]. In addition, an entity link between Avaya Aura™ Session Manager and Cisco UCM Release 6 is configured. To configure an entity link, select **Network Routing Policy → Entity Links**. Any existing entity links are listed, as shown below. The relevant parameters for the entity link "Avaya-G430" can be observed from this screen, and will not be repeated.

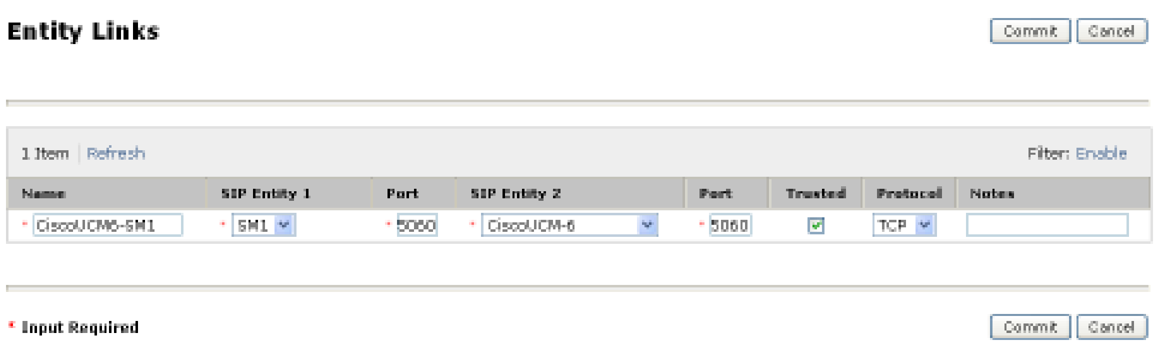


To add a new entity link, click **New**. The following list provides guidance for the fields:

- **Name**: Enter a descriptive name.
- **SIP Entity 1**: Select Avaya Aura™ Session Manager.
- **Port** field: Port number to which the other SIP entity will send SIP requests (i.e., a listen port for SIP Entity 1)
- **SIP Entity 2**: Select the SIP Entity corresponding to the other system (i.e., Avaya Aura™ Communication Manager or Cisco UCM Release 6).
- **Port** field: Port number where SIP Entity 2 listens for SIP requests
- **Trusted**: Check this box.
- **Protocol**: Transport protocol to be used to send SIP requests. In the sample configuration, TLS is used between Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. TCP is used between Avaya Aura™ Session Manager and Cisco UCM Release 6.
- **Notes**: Optional descriptive text

Click **Commit** to save each entity link definition.

The following portion of the new entity links screen shows the parameters used for the entity link between Session Manager and Cisco UCM Release 6.

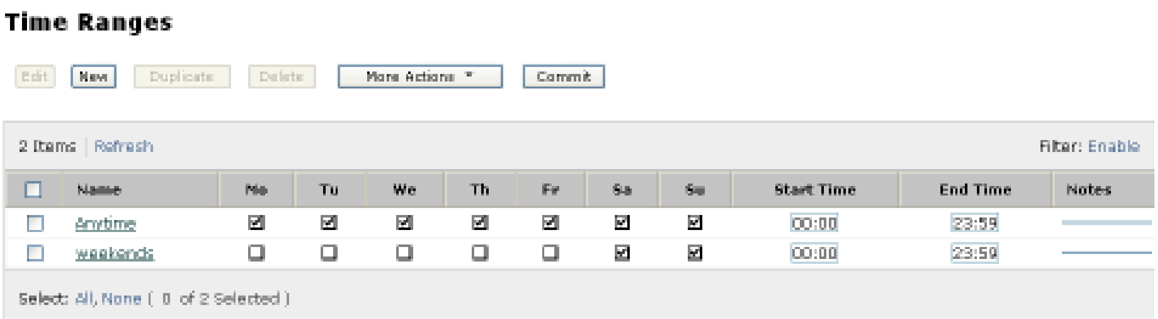


6.6. Configure Time Ranges

Time ranges are defined prior to defining routing policies in the next section. Avaya Aura™ Session Manager allows routing decisions to be a function of the time range. In the sample configuration, a policy was used that allowed routing to occur at anytime. To add a time range, select **Network Routing Policy → Time Ranges**. Click **New**. In the resultant screen, configure the following fields:

- **Name:** A descriptive name, such as "Anytime"
- **Mo** through **Su** checkboxes: check the box as appropriate for inclusion in the time range.
- **Start Time:** Enter the start time for the range (e.g., "00:00" for start of day).
- **End Time:** Enter the end time for the range (e.g., "23:59" for end of day).

Click **Commit** to save any changes. The following screen illustrates two self-explanatory time ranges, including the "Anytime" range.



Time Ranges

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

2 Items | Refresh | Filter: Enable

	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	Anytime	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	
☐	weekends	☐	☐	☐	☐	☐	☑	☑	00:00	23:59	

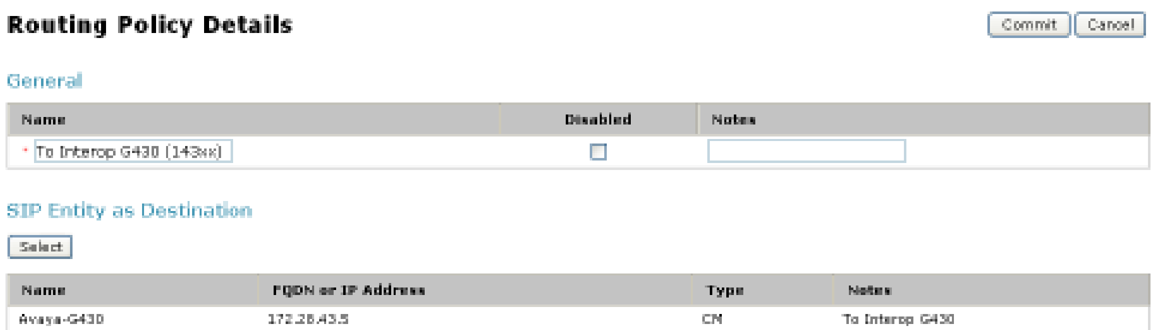
Select: All, None (0 of 2 Selected)

6.7. Configure Routing Policies

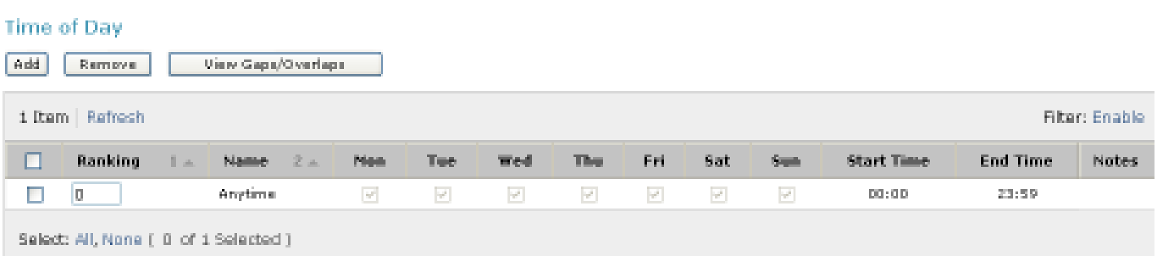
Routing policies describe the conditions under which calls will be routed among the configured SIP entities. In the sample configuration, one routing policy is configured for routing between Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager. This routing policy is identical to the routing policy named "To Interop G430 (143xx)" in reference [6]. Another routing policy is configured for routing between Avaya Aura™ Session Manager and Cisco UCM Release 6.

To add a routing policy, select **Network Routing Policy → Routing Policies**. As shown in the screen below, any existing policies are listed.

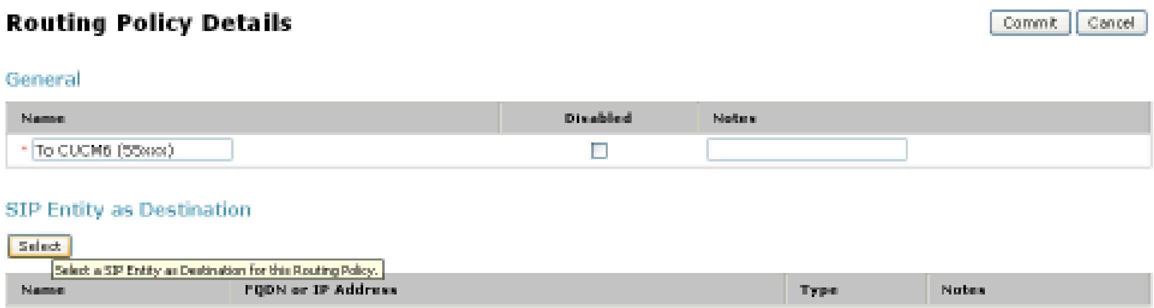
Click **New**. The resultant screen has several headings. Under the **General** heading, enter a descriptive name for this routing policy in the **Name** field. Under the **SIP Entity as Destination** heading, click the **Select** button, and select the appropriate destination SIP entity. The following portion of the "To Interop G430 (143xx)" policy screen is identical to the corresponding configuration from reference [6].



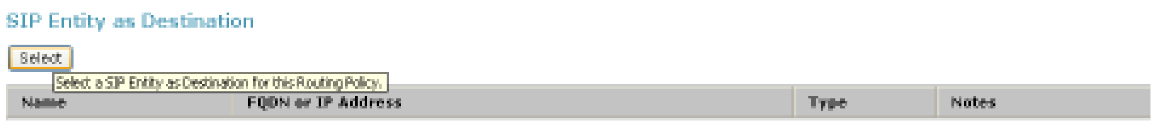
Under the **Time of Day** heading, click the **Add** button, and select the appropriate range configured in the prior section. In this case, the routing policy applies "Anytime".



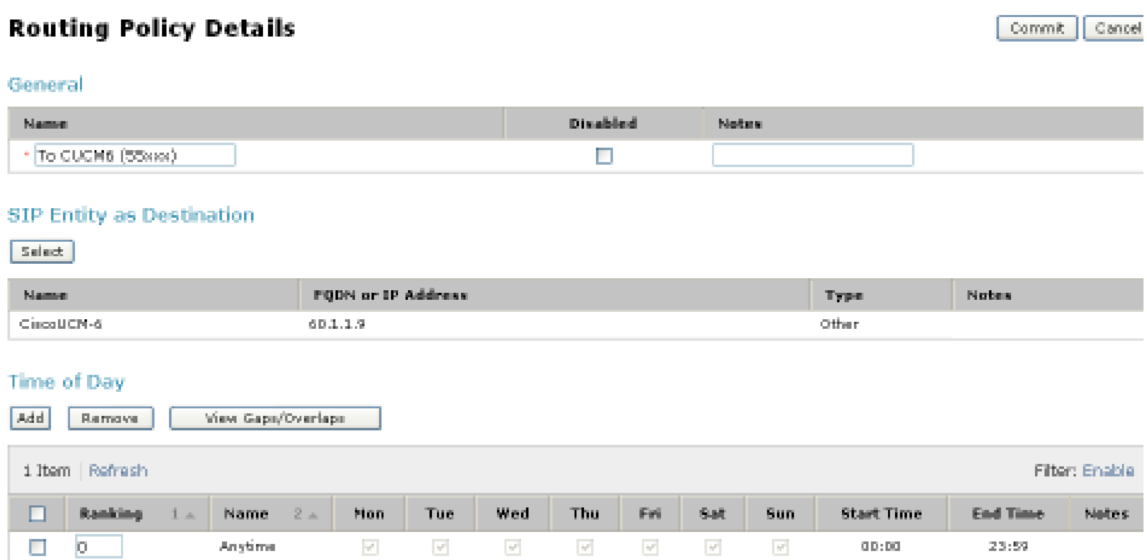
Return to **Network Routing Policy → Routing Policies**. Click **New** to add the routing policy that will be applicable to Cisco UCM Release 6. Under the **General** heading, enter a descriptive name for this routing policy, such as "To CUCM6 (55xxx)" in the **Name** field.



Under the **SIP Entity as Destination** heading, click the **Select** button. The following screen was captured while the mouse was positioned over the **Select** button to show an example of the "tool tips" available using System Manager.



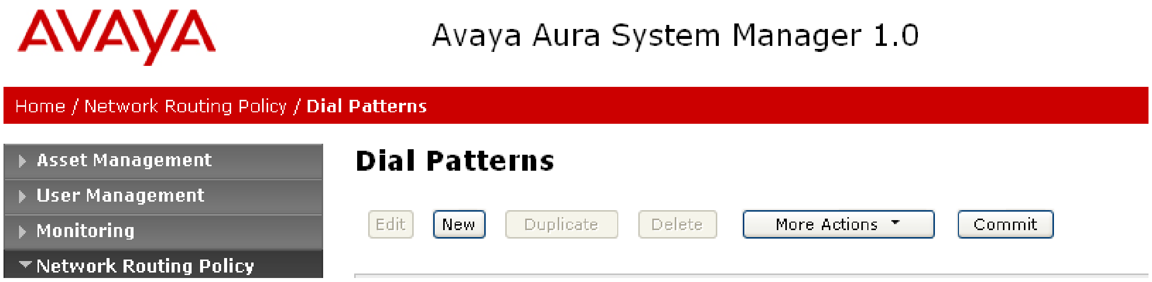
The following screen shows the "CiscoUCM-6" **SIP Entity as Destination** selection and "Anytime" **Time of Day** configuration for the policy named "To CUCM6 (55xxx)".



Dial patterns will be associated with the routing policy in the following section.

6.8. Configure Dial Patterns

Dial patterns are defined for directing calls to the appropriate SIP entity. In the sample configuration, five-digit numbers of the form 143xx are associated with extensions on Avaya Aura™ Communication Manager. Five-digit numbers of the form 55xxx are associated with telephones controlled by Cisco UCM Release 6. To add a dial pattern, select **Network Routing Policy → Dial Patterns**.

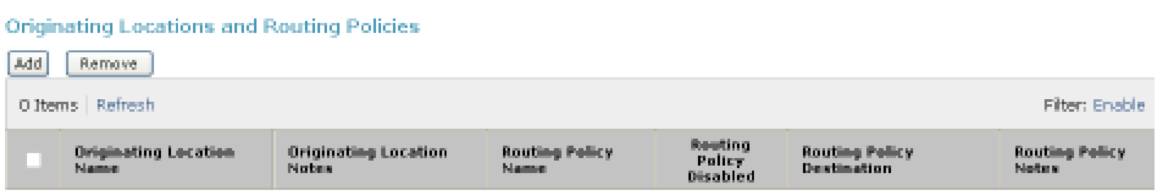


Click **New**. In the resultant screen, configure the following fields under the **General** heading:

- **Pattern:** The leading digits of the dialed number or prefix
- **Min**: the minimum length of a number to match
- **Max:** the maximum length of a number to match
- **SIP Domain:** select the appropriate SIP domain (e.g., "avaya.com").
- **Notes:** Descriptive text commenting on the purpose of this dial pattern

The following screen illustrates the portion of the screen for calls of the form 55xxx.

Under the **Originating Locations and Routing Policies** heading, click **Add.**



In the resultant screen, select the appropriate location and routing policy from the list. In the sample configuration, the “all” originating locations parameter is used. Since the dial pattern being added is for 55xxx, the “To CUCM6 (55xxx)” routing policy is selected.

Originating Location

5 Items | Refresh Filter: Enable

☐	Name	Notes
☑	-ALL-	Any Locations
☐	California	CiscoUCM
☐	Lincroft	Session Manager and ACM
☐	Lincroft-Mobile	DiVitas
☐	Toronto	Nortel CS1000 & Cisco UCME

Select: All, None (1 of 5 Selected)

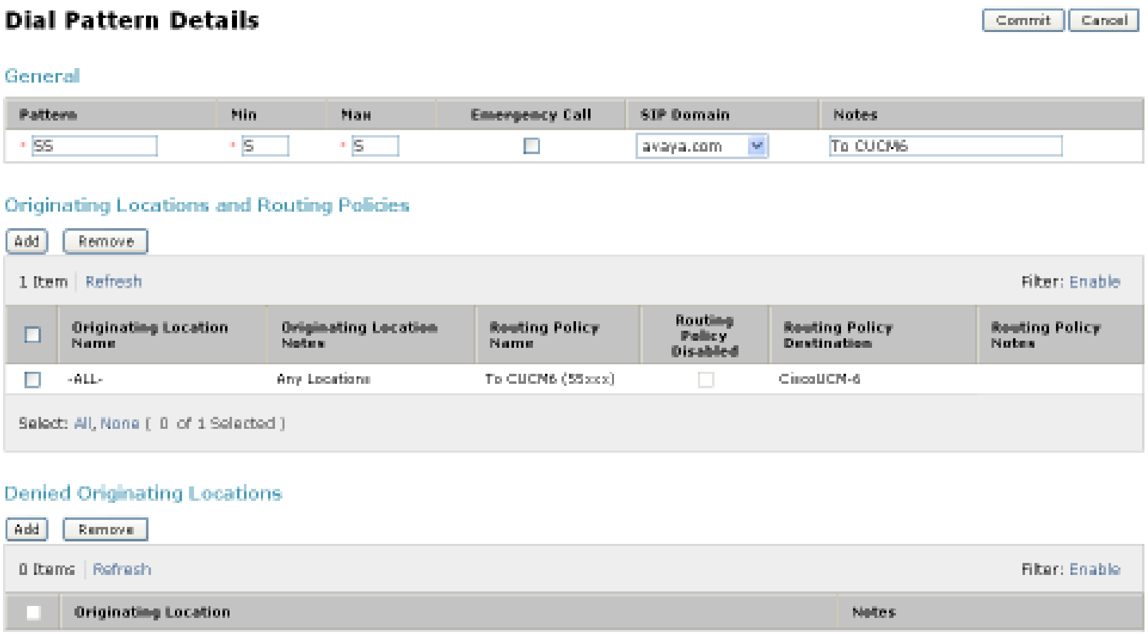
Routing Policies

12 Items | Refresh Filter: Enable

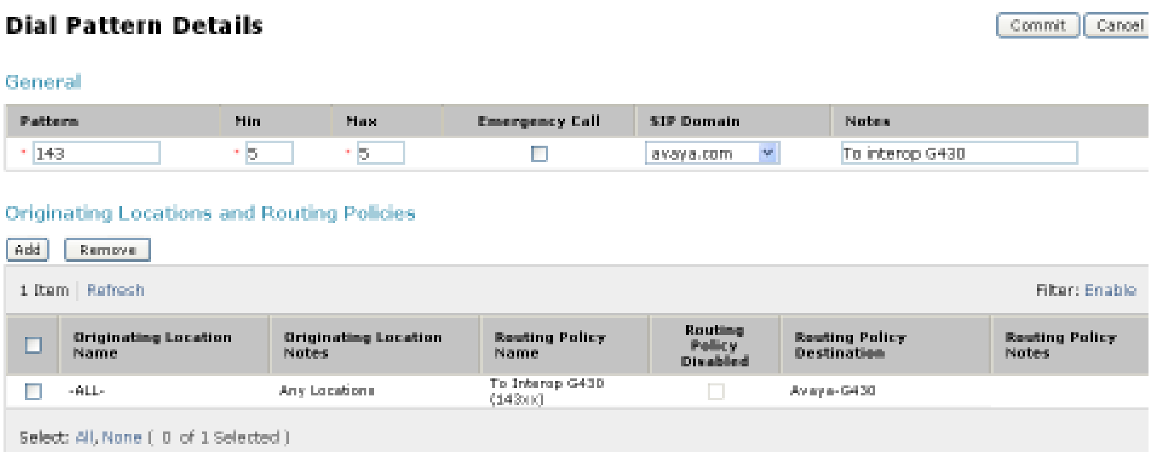
☐	Name	Disabled	Destination	Notes
☐	Call Center	☐	CallCenter	
☐	CS1000 via AC M1000	☐	AudioCodes M1000	
☐	Nortel CS1000	☐	Nortel CS1000	
☐	To Acme	☐	AcmePacket	
☐	To Avaya MM	☐	Avaya_MAS-Br2	
☑	To CUCM6 (55xxx)	☐	CiscoUCM-6	

Return to the **Dial Pattern Details** page, click **Commit** to save changes.

The following screen shows the “55xxx” dial pattern after committing the changes. Observe that **Denied Originating Locations** may also be configured, but are not used in the sample configuration.



The same process may be used to define the dial pattern for calls of the form 143xx. The following screen illustrates the completed configuration. Note that this dial pattern is identical to the corresponding dial pattern configured in reference [6].



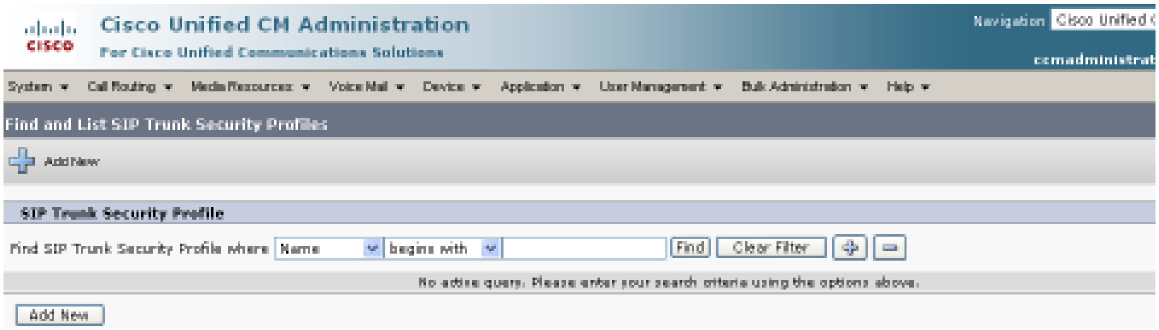
7. Configure Cisco UCM

This section provides the procedures for configuring Cisco UCM for a SIP trunk to Avaya Aura™ Session Manager. These Application Notes assume that the basic configuration needed to support Cisco IP telephones has previously been completed. For further information on Cisco UCM, please consult references [7] and [8].

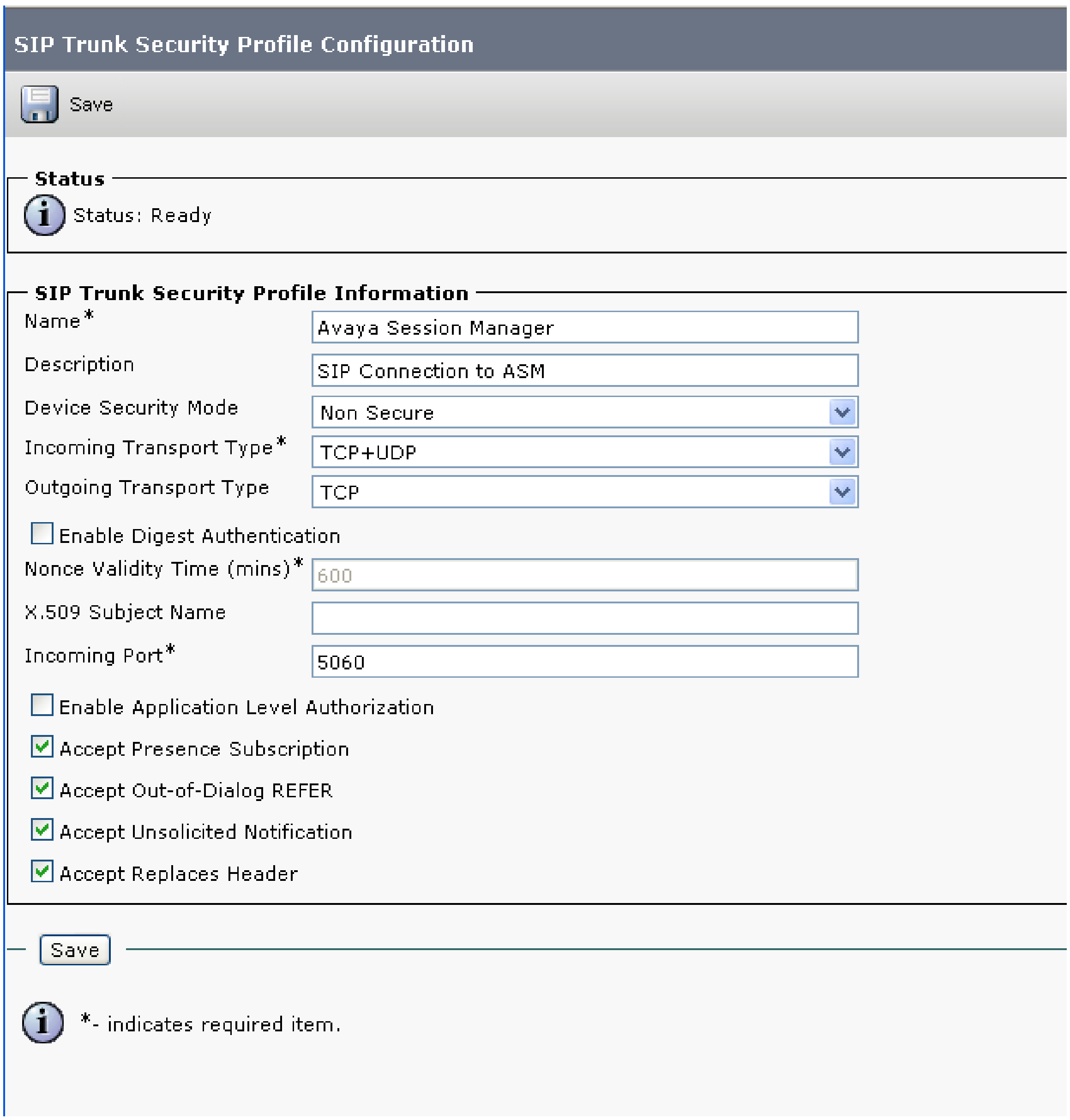
1. Enter the IP address of the CUCM into the Web Browser address field (e.g., 60.1.1.9 as shown in **Figure 1**). A screen such as the following is displayed. Click the link **Cisco Unified Communications Manager Administration**.

2. On the resultant screen (not shown), log in using appropriate Username and Password. After successful log in, a screen such as the following is displayed.

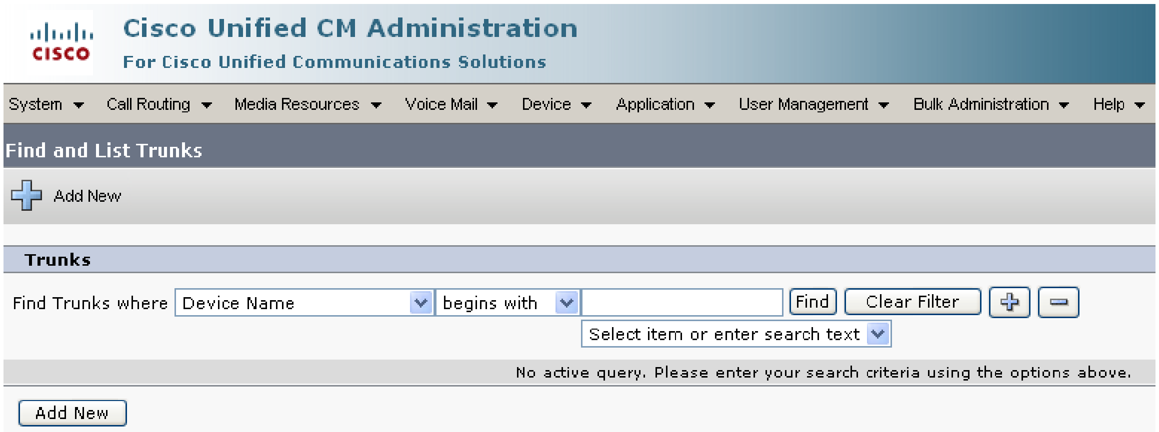
3. Select **System → Security Profile → SIP Trunk Security Profile** from the top menu. Click **Add New** to add a new SIP Trunk Security Profile.



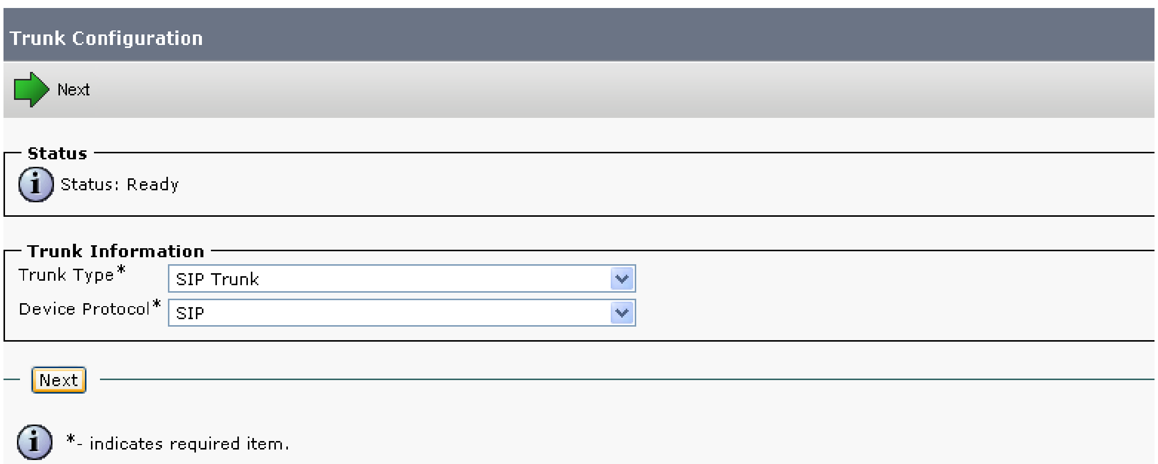
The following screen capture shows the SIP Trunk Security Profile used in the sample network. Configure the parameters as shown below and click **Save**.



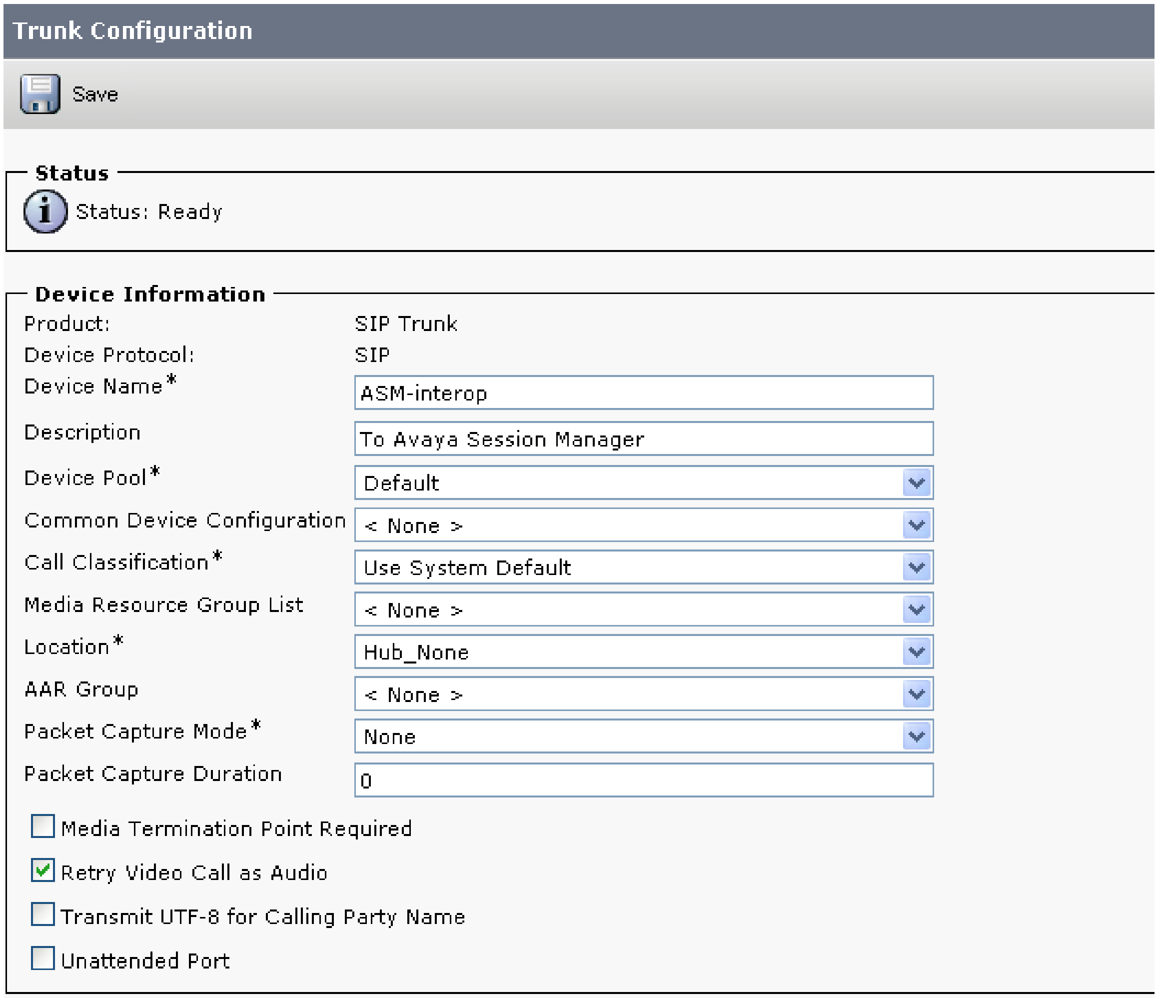
4. Add a new SIP trunk by selecting **Device → Trunk** from the top menu. Click **Add New** to add a new SIP trunk.



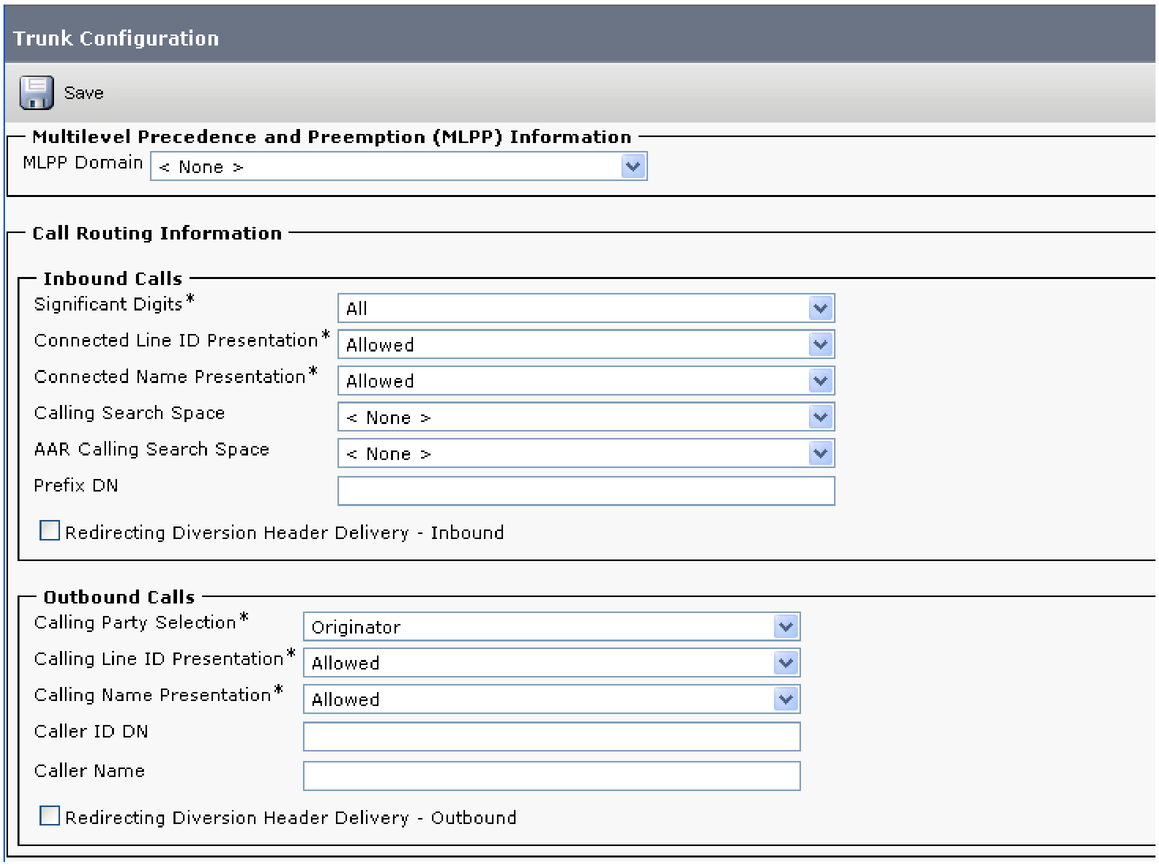
Select **SIP Trunk** as the **Trunk Type.** The **Device Protocol** field will automatically be changed to SIP. Click **Next** to continue.



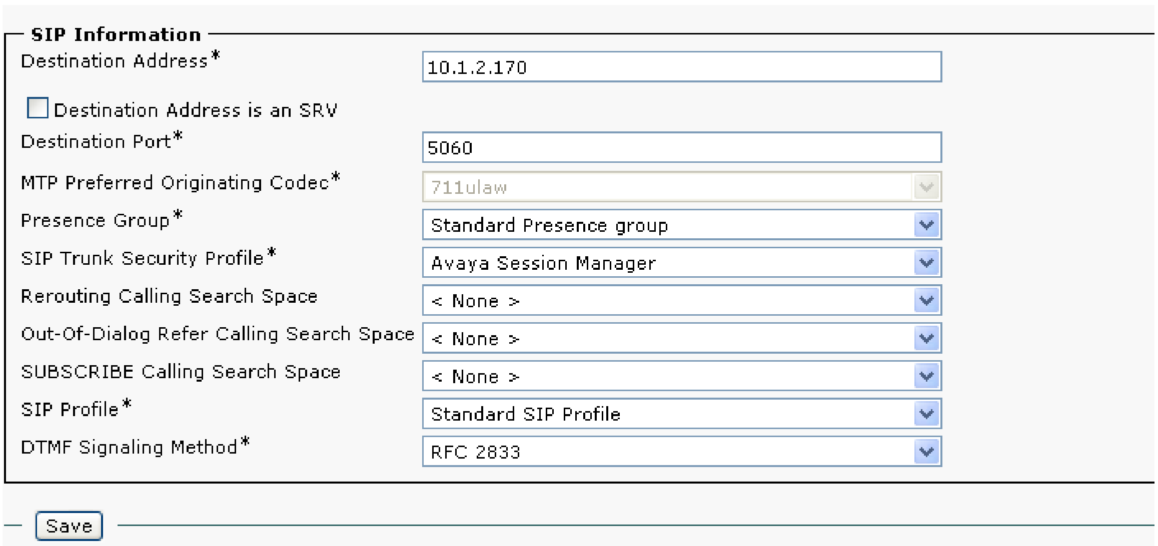
The following screen shows the parameters used in the sample configuration under the **Device Information** heading of the **Trunk Configuration** screen.



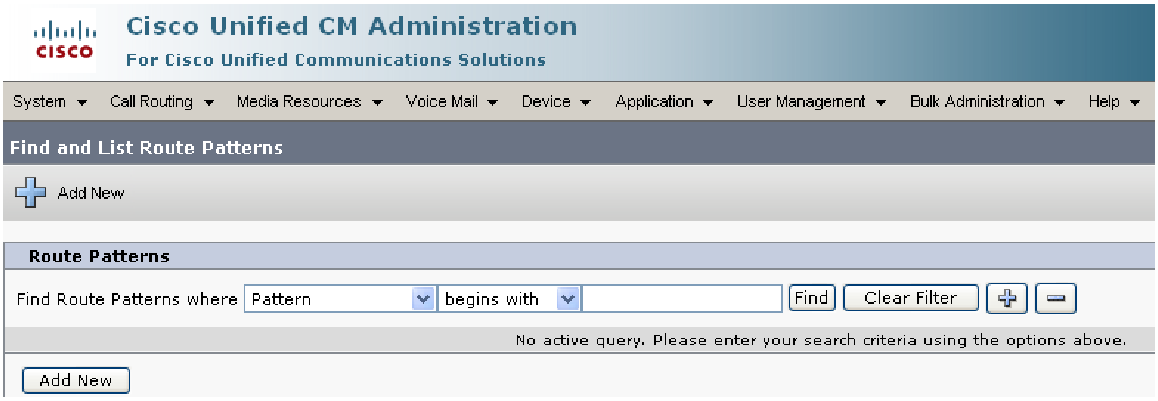
Scrolling down, the following screen shows the parameters used in the sample configuration under the **Call Routing Information** heading of the **Trunk Configuration** screen. The screen shows that calling and connected line presentation of name and number was allowed. Testing was also performed with these fields set to "Restricted". See Section 8.4 for further information on privacy considerations.



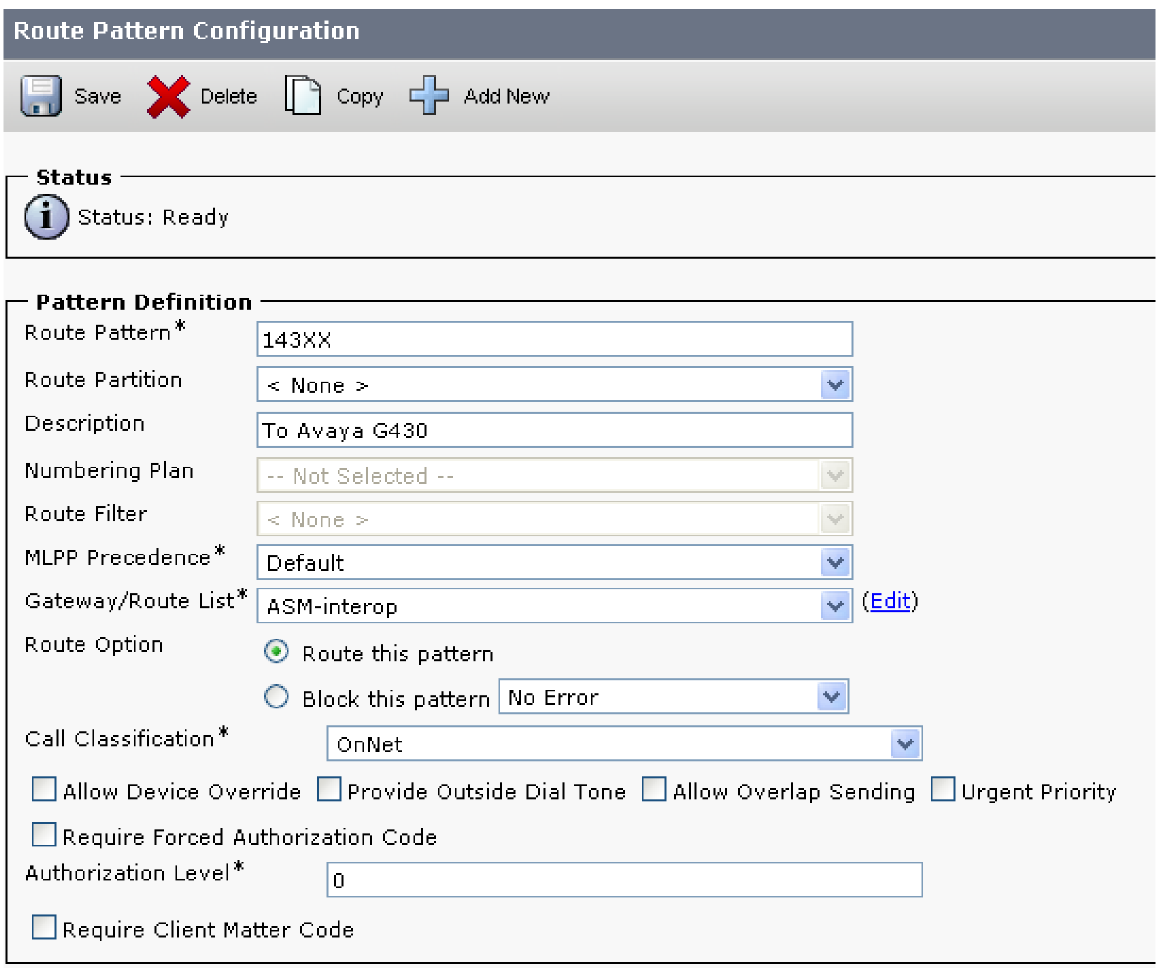
Scrolling down, the following screen shows the parameters used in the sample configuration under the **SIP Information** heading of the **Trunk Configuration** screen. Note that the **Destination Address** is set to the IP Address of Avaya Aura™ Session Manager (i.e., 10.1.2.170). The **Destination Port** is set to 5060, where Session Manager will be listening for SIP messages. The previously configured **SIP Trunk Security Profile** named "Avaya Session Manager" has been selected. The **DTMF Signaling Method** is set to "RFC 2833." Click **Save**.



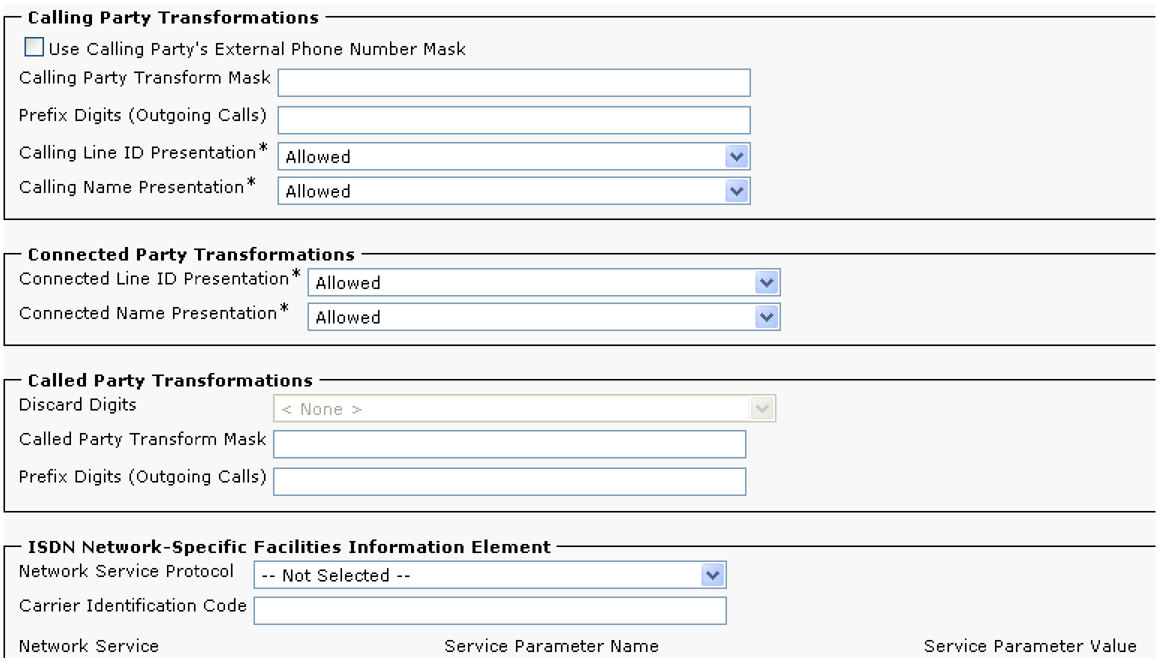
5. Select **Call Routing → Route/Hunt → Route Pattern.**



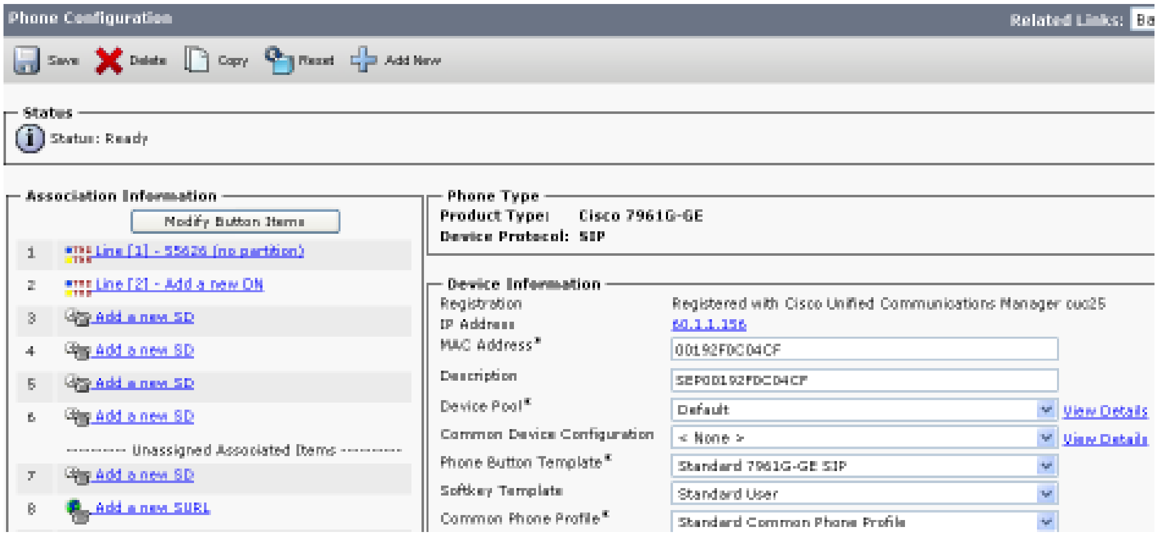
Click **Add New**. The new route pattern will enable dialed numbers of the form 143xx to be routed via the **Gateway/Route List** choice of "ASM-interop", which has been defined as the SIP trunk to Avaya Aura™ Session Manager. The following screen shows the parameters used in the sample configuration under the **Pattern Definition** heading of the **Route Pattern Configuration** screen.



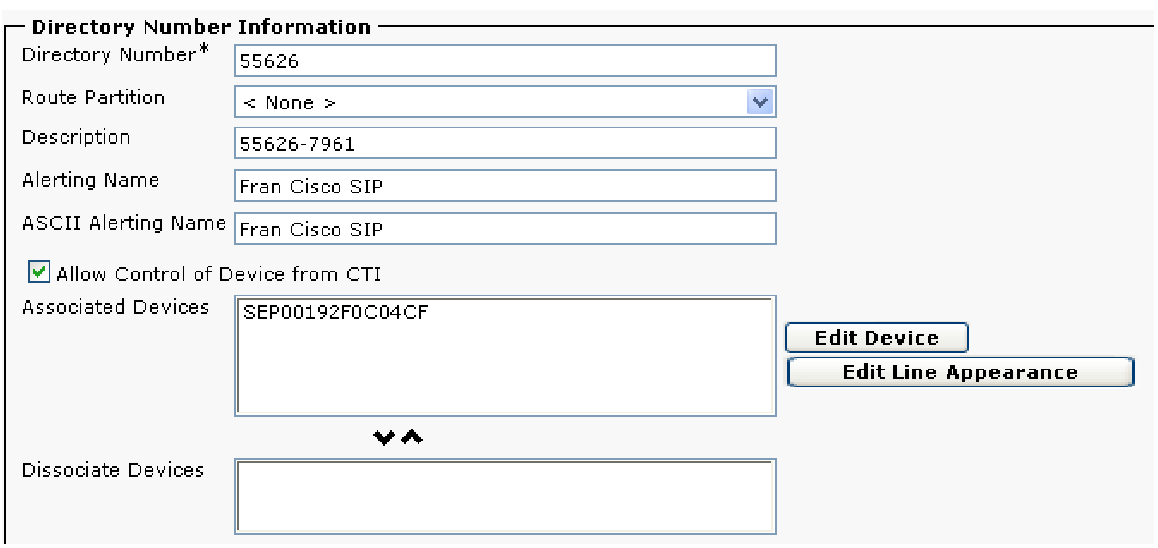
Scrolling down, the following screen shows the remaining parameters used in the sample configuration for the **Route Pattern Configuration** screen.   Note that calling and connected number and name presentation are allowed. Click **Save**.



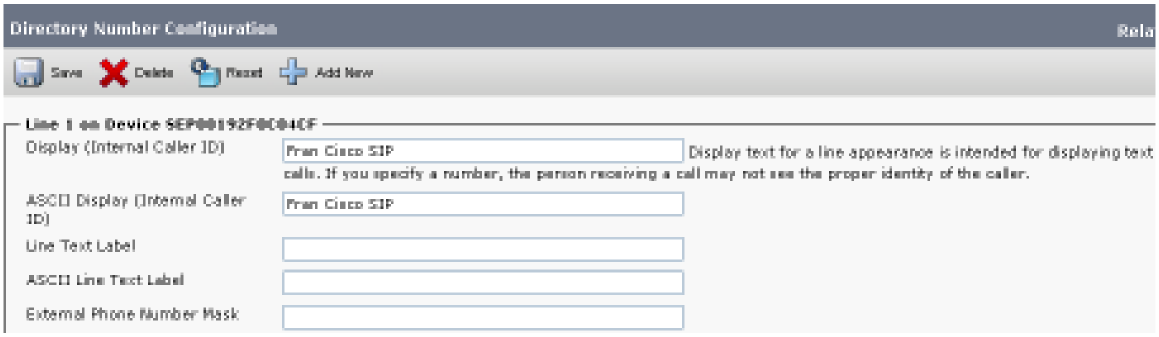
6. Select **Device → Phone.** Click on the device to be configured. The following screen shows the display after the phone shown as extension 55626 in **Figure 1** has been selected. On the left under the heading **Association Information**, click on line 1.



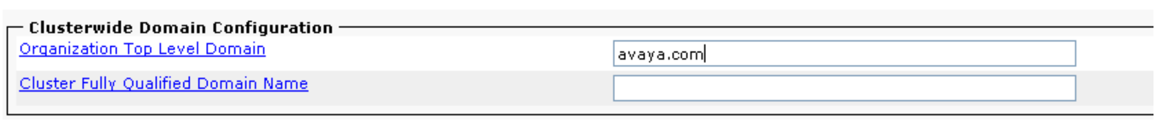
The following screen shows the parameters used in the sample configuration under the **Directory Number Information** heading for the selected line. Note that the **Alerting Name** and **ASCII Alerting Name** fields are populated with a name "Fran Cisco SIP" that will match the name configured for the line. Configuring these fields allows an Avaya caller to see the name of the alerting Cisco telephone during the ringing phase of the call.



Scrolling down, the following screen shows additional parameters used in the sample configuration for the **Directory Number Configuration** screen. Note that the **Display (Internal Caller ID)** and **ASCII Display (Internal Caller ID)** fields are configured with a name "Fran Cisco SIP" matching the **Alerting Name** illustrated previously. Click **Save**.



7. Select **System → Enterprise Parameters.** Scroll down to the heading **Clusterwide Domain Configuration**. Ensure that the **Organization Top Level Domain** matches the SIP domain configured in Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager. Recall that "avaya.com" has been used throughout the sample configuration.



8. Verifications

This section illustrates tests performed to verify the configuration.

8.1. Verify Avaya Aura™ Communication Manager

This section presents screens from Communication Manager that can be used to verify or troubleshoot the configuration.

8.1.1. SIP Signaling Group and Trunk Group Status

The SIP Signaling Group and SIP Trunk Group to Avaya Aura™ Session Manager should be in-service. The following screen shows the "status trunk 26" screen, showing all trunks are in-service and idle.

```
status trunk 26
                             TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy
0026/001 T00017   in-service/idle    no
0026/002 T00018   in-service/idle    no
0026/003 T00019   in-service/idle    no
0026/004 T00020   in-service/idle    no
0026/005 T00021   in-service/idle    no
0026/006 T00022   in-service/idle    no
0026/007 T00023   in-service/idle    no
0026/008 T00024   in-service/idle    no
0026/009 T00025   in-service/idle    no
0026/010 T00026   in-service/idle    no
```

If the trunk group is not in-service, check the SIP Signaling Group status. The following screen shows the "status signaling-group 26" screen, showing that the signaling group is in-service.

```
status signaling-group 26
                         STATUS SIGNALING GROUP

        Group ID: 26                                Active NCA-TSC Count: 0
      Group Type: sip                                Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

If the signaling group is in a "bypass" state, check the "Enable Layer 3 Test" parameter on the signaling group screen. If the "Enable Layer 3 Test" for the signaling group is set to "n", Communication Manager will use an "ICMP ping" test to verify that the far-end of the signaling group is reachable. Some networks may not pass ICMP ping, which is a possible cause for the signaling group to be marked for "bypass" and the corresponding trunk group to be marked "Out-of-Service/Far-end". In this state, Communication Manager would not use the trunk for outbound calls, but would allow an incoming call. In the sample configuration, the "Enable Layer 3 Test" has been set to "y", meaning that Communication Manager will use a SIP OPTIONS message to the far-end (Session Manager in this case) to verify connectivity. If the signaling group is marked for "bypass", and the SIP OPTIONS method is used, verify that the far-end node name (and corresponding IP Address) correctly refers to Session Manager. Verify that Session Manager is on-line and configured properly for a SIP Entity to Communication Manager. The Session Manager SIP Entity representing Communication Manager should specify the IP Address corresponding to the node name at the "near-end" of the Communication Manager signaling group (i.e., in this case, the S8300 "procr" IP Address).

8.1.2. Avaya Telephone Calls Cisco Telephone

This section has example calls where an Avaya H.323 telephone calls Cisco SIP and SCCP telephones. Greater detail is included in the initial illustrations, since the results including displays and connection topology are independent of the called telephone type in the sample configuration.

8.1.2.1 Avaya H.323 Telephone Calls Cisco SIP Telephone

The following "list trace station" output illustrates a call from the Avaya IP Telephone with extension 14302 to Cisco SIP Telephone extension 55626. The Avaya telephone, with IP Address 172.28.43.102 in network region 1, dials 55626. The call is routed using UDP and AAR to route pattern 25 containing trunk group 26. When the Cisco telephone is ringing, the Cisco telephone's display will show "From Fred-Avaya (14302)" which correspond to the name and extension of the Avaya calling telephone. Similarly, the Avaya telephone will display "Fran Cisco SIP 55626", which correspond to the Alerting Name and number configured for the called Cisco telephone. (See Section 7, Step 6 for the screen showing Alerting Name for this user). Upon answer by the called Cisco user, the displays are unchanged. The "far-end" region is region 3, and therefore the media connection is between region 1 and region 3. Codec set 3 governs this connectivity, and the final connection uses G.711MU, which was specified in ip-codec-set 3 at the time of this call. Recall that "shuffling" to ip-direct media has been disabled for inter-region connections involving region 3. The final media path connects the Cisco SIP Telephone with IP Address 60.1.1.156 in network region 3 to the Avaya G430 VoIP resources, at 172.28.43.6.

```
list trace station 14302                                                Page   1
                                LIST TRACE
time            data
10:39:15     active station    14302 cid 0xc8
10:39:15     G711MU ss:off ps:20
             rgn:1 [172.28.43.102]:2122
             rgn:1 [172.28.43.6]:2050
10:39:17     dial 55626 route:UDP|AAR
10:39:17     term trunk-group 26    cid 0xc8
10:39:17     dial 55626 route:UDP|AAR
10:39:17     route-pattern  25 preference 1  cid 0xc8
10:39:17     seize trunk-group 26 member 1  cid 0xc8
10:39:17     Calling Number & Name NO-CPNumber NO-CPName
10:39:17     Setup digits 55626
10:39:17     Calling Number & Name 14302 Fred-Avaya
10:39:17     Proceed trunk-group 26 member 1  cid 0xc8
10:39:17     Alert trunk-group 26 member 1  cid 0xc8
10:39:24     G711MU ss:off ps:20
             rgn:3 [60.1.1.156]:23334
             rgn:1 [172.28.43.6]:2054
10:39:24     active trunk-group 26 member 1  cid 0xc8
```

The "status trunk" command can also be used, as shown below for this same call, while active. Page 2 is shown below. The near-end and far-end signaling IP Addresses and Ports can be observed for the TLS connection between Communication Manager and

Session Manager. The media connection information shows that the call is "ip-direct" between the two telephones, using G.711MU.

```
status trunk 26/1                                               Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: 01A0017
  Signaling   IP Address                             Port
   Near-end:  172.28.43.5                          : 5061
    Far-end:  10.1.2.170                           : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-tdm        Authentication Type: None
    Near-end Audio Loc: MG1                    Codec Type: G.711MU
   Audio      IP Address                             Port
   Near-end:  172.28.43.6                          : 2054
    Far-end:  60.1.1.156                           : 23334
```

On page 3, further details can be observed. Since codec set 1 used for intra-region connections in region 1 is configured to prefer SRTP encryption, the connection between the Avaya IP Telephone (172.28.32.102) and the G430 VoIP Resource uses "1-srt-aescm128-hmac80".   The connection from the G430 VoIP Resource to the Cisco SIP telephone (60.1.1.156) is not encrypted.

```
status trunk 26/1                                               Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00017
T00017:TX:60.1.1.156:23334/g711u/20ms
001V085:RX:172.28.43.6:2054/g711u/20ms:TX:ctxID:71
001V087:RX:ctxID:71:TX:172.28.43.6:2050/g711u/20ms/1-srtp-aescm128-hmac80
S00001:RX:172.28.43.102:2122/g711u/20ms/1-srtp-aescm128-hmac80
```

If the Avaya telephone holds the call, music on hold from the Avaya G430 announcement capability is heard by the Cisco telephone via the existing connection to the G430 VoIP.

If the Cisco telephone holds the call, the media path must move from the Cisco SIP telephone to the Cisco UCM resource playing the music. The following is an example status screen taken when the Cisco phone had held the call, and the Avaya telephone user was listening to music from Cisco UCM.

```
status trunk 26/1                                              Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: 01A0017
  Signaling   IP Address                               Port
   Near-end:  172.28.43.5                            : 5061
    Far-end:  10.1.2.170                             : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-tdm        Authentication Type: None
    Near-end Audio Loc: MG1                    Codec Type: G.711MU
   Audio      IP Address                               Port
   Near-end:  172.28.43.6                            : 2054
    Far-end:  60.1.1.9                               : 4000
```

If the Cisco SIP telephone resumes the held call, the media path moves off Cisco UCM back to the Cisco SIP telephone. That is, the connection topology returns to the status before the call was held.

If the Cisco SIP telephone transfers the call to the Cisco SCCP telephone, the transfer is successful, and the final connection topology has the Avaya G430 VoIP resource communicating directly with the transferred-to Cisco SCCP telephone. Post transfer, the display on the transferred-to telephone is "From Fred-Avaya (14302)", the name and number of the Avaya telephone. The display on the Avaya telephone updates to "Cisco SCCP 55612", the name and number of the transferred-to Cisco SCCP telephone.

8.1.2.2 Avaya H.323 Telephone Calls Cisco SCCP Telephone

The following "list trace station" output illustrates a call from the Avaya IP Telephone with extension 14302 to Cisco SCCP Telephone extension 55612. The Avaya telephone, with IP Address 172.28.43.102 in network region 1, dials 55612. The call is routed using UDP and AAR to route pattern 25 containing trunk group 26. When the Cisco telephone is ringing, the Cisco telephone's display will show "From Fred-Avaya (14302)" which correspond to the name and extension of the Avaya calling telephone. Similarly, the Avaya telephone will display "Fran Cisco SCCP 55612", which correspond to the Alerting Name and number configured for the called Cisco telephone. (See Section 7, Step 6 for more information). Upon answer by the called Cisco user, the displays are unchanged. The "far-end" region is region 3, and therefore the media connection is between region 1 and region 3. Codec set 3 governs this connectivity, and the final connection uses G.711MU, which was specified in ip-codec-set 3 at the time of this call. Recall that "shuffling" to ip-direct media has been disabled for inter-region connections involving region 3. The final media path connects the Cisco SCCP Telephone with IP Address 60.1.1.158 in network region 3 to the Avaya G430 VoIP resources, at 172.28.43.6.

```
list trace station 14302                                            Page   1

                                LIST TRACE
time            data
10:20:52     active station    14302 cid 0xc6
10:20:52     G711MU ss:off ps:20
             rgn:1 [172.28.43.102]:2122
             rgn:1 [172.28.43.6]:2056
10:20:55     dial 55612 route:UDP|AAR
10:20:55     term trunk-group 26    cid 0xc6
10:20:55     dial 55612 route:UDP|AAR
10:20:55     route-pattern  25 preference 1  cid 0xc6
10:20:55     seize trunk-group 26 member 10  cid 0xc6
10:20:55     Calling Number & Name NO-CPNumber NO-CPName
10:20:55     Setup digits 55612
10:20:55     Calling Number & Name 14302 Fred-Avaya
10:20:55     Proceed trunk-group 26 member 10  cid 0xc6
10:20:55     Alert trunk-group 26 member 10  cid 0xc6
10:20:57     active trunk-group 26 member 10  cid 0xc6
10:20:57     G711MU ss:off ps:20
             rgn:3 [60.1.1.158]:22272
             rgn:1 [172.28.43.6]:2052
```

The “status trunk” command can also be used, with similar output to that already presented in the prior section. Rather than repeat, more detailed information is provided for an Avaya held call. If the Avaya telephone holds the call, music on hold from the Avaya G430 announcement capability is heard by the Cisco telephone via the connection to the G430 VoIP. The following screen illustrates the connection while on hold at the Avaya side. Port “1V902” is a G430 Media Gateway announcement resource.

```
status trunk 26/10                                           Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00026
T00026:TX:60.1.1.158:22272/g711u/20ms
001V086:RX:172.28.43.6:2052/g711u/20ms:TX:ctxID:58
001V902:RX:tdm:NIL
dst port: 001V902
```

Once the call is resumed, two-way audio is restored properly.

If the Cisco telephone holds the call, the media path must move from the Cisco SCCP telephone to the Cisco UCM resource playing the music. Details are the same as those provided in the previous section, substituting the Cisco SCCP phone IP Address for the Cisco SIP phone IP Address. If the Cisco SCCP telephone resumes the held call, the media path moves off Cisco UCM back to the Cisco SCCP telephone. That is, the connection topology returns to the status before the call was held.

If the Cisco SCCP telephone transfers the call to the Cisco SIP telephone, the transfer is successful, and the final connection topology has the Avaya G430 VoIP resource communicating directly with the transferred-to Cisco SIP telephone. Post transfer, the display on the transferred-to telephone is “From Fred-Avaya (14302)”, the name and number of the Avaya telephone. The display on the Avaya telephone updates to “Fran Cisco SIP 55626”, the name and number of the transferred-to Cisco SIP telephone.

If the Avaya IP telephone transfers the call to the Avaya digital telephone, the transfer is successful, and the final connection topology remains the same, since the Avaya G430 VoIP resource is already employed. Post transfer, the display on the transferred-to Avaya telephone is "Fran Cisco SIP 55626", the name and number of the connected Cisco telephone. The display on the connected Cisco telephone updates to "From Digital Sam (14303)", the name and number of the transferred-to Avaya telephone.

8.1.3. Cisco Telephone Calls Avaya Telephone

This section has example calls where Cisco SIP and SCCP telephones call the Avaya IP telephone.

8.1.3.1 Cisco SIP Telephone calls Avaya H.323 Telephone

The following "list trace tac" output illustrates an incoming call from the SIP trunk to Session Manager for a call from Cisco SIP Telephone extension 55626 to Avaya IP Telephone extension 14302. When the Avaya telephone is ringing, the Cisco telephone's display will show "To Fred-Avaya (14302)" which correspond to the name and number of the called Avaya telephone. Similarly, the Avaya telephone will display "Fran Cisco SIP 55626", which correspond to the name and number configured for the calling Cisco telephone. Upon answer by the called Avaya user, the displays are unchanged. (Do not be deceived by the trace output below showing no calling number and name. The number and name of the Cisco caller do appear on the Avaya telephone's display).

Similar to the calls from Avaya to Cisco, the final media path is between the Cisco telephone (60.1.1.156) and the Avaya G430 VoIP Resource (172.28.43.6).

```
list trace tac 126                                                    Page   1
                                LIST TRACE
time            data

11:21:21     Calling party trunk-group 26 member 1  cid 0xd2
11:21:21     Calling Number & Name NO-CPNumber NO-CPName
11:21:21     active trunk-group 26 member 1  cid 0xd2
11:21:21     dial 14302
11:21:21     ring station    14302 cid 0xd2
11:21:21     G711MU ss:off ps:20
             rgn:1 [172.28.43.102]:2122
             rgn:1 [172.28.43.6]:2052
11:21:23     active station    14302 cid 0xd2
11:21:23     G711MU ss:off ps:20
             rgn:3 [60.1.1.156]:29908
             rgn:1 [172.28.43.6]:2058
```

Hold/resume and transfer scenarios from both the Avaya telephone and Cisco telephone were verified and work properly as described previously. Screen details would be redundant and reveal no new information.

Note: failure to re-establish a two-way talk path after hold and resume from the Cisco SIP Telephone for a call from the Cisco SIP Telephone to the Avaya H.323 telephone is the primary case leading to the recommendation in these Application Notes to disable shuffling to ip-direct media. If "ip-direct" were enabled, the final media path for the calls that are the subject of this section would indeed be "ip-direct" between the Avaya and Cisco SIP Telephone. However, resuming a held call from the Cisco SIP telephone in this specific scenario results in one-way audio, for the same reasons described in Section 9 of reference [6]. As a result of this problem, it was deemed impractical to allow "ip-direct" media paths. A workaround is to disable "ip-direct" media (e.g., using the signaling group or network region forms).

8.1.3.2 Cisco SCCP Telephone calls Avaya H.323 Telephone

The following "list trace tac" output illustrates an incoming call from the SIP trunk to Session Manager for a call from Cisco SCCP Telephone extension 55612 to Avaya IP Telephone extension 14302. When the Avaya telephone is ringing, the Cisco telephone's display will show "To Fred-Avaya (14302)" which correspond to the name and number of the called Avaya telephone. Similarly, the Avaya telephone will display "Cisco SCCP 55612", which correspond to the Name and number configured for the calling Cisco telephone. Upon answer by the called Avaya user, the displays are unchanged..

Similar to the corresponding calls from Avaya to Cisco, the final media path is between the Cisco telephone (60.1.1.158) and the Avaya G430 VoIP Resource (172.28.43.6).

```
list trace tac 126                                                        Page   1
                                LIST TRACE
time            data
11:31:33     Calling party trunk-group 26 member 1  cid 0xd4
11:31:33     Calling Number & Name NO-CPNumber NO-CPName
11:31:33     active trunk-group 26 member 1  cid 0xd4
11:31:33     dial 14302
11:31:33     ring station    14302 cid 0xd4
11:31:33     G711MU ss:off ps:20
             rgn:1 [172.28.43.102]:2122
             rgn:1 [172.28.43.6]:2054
11:31:37     active station    14302 cid 0xd4
11:31:37     G711MU ss:off ps:20
             rgn:3 [60.1.1.158]:20298
             rgn:1 [172.28.43.6]:2050
```

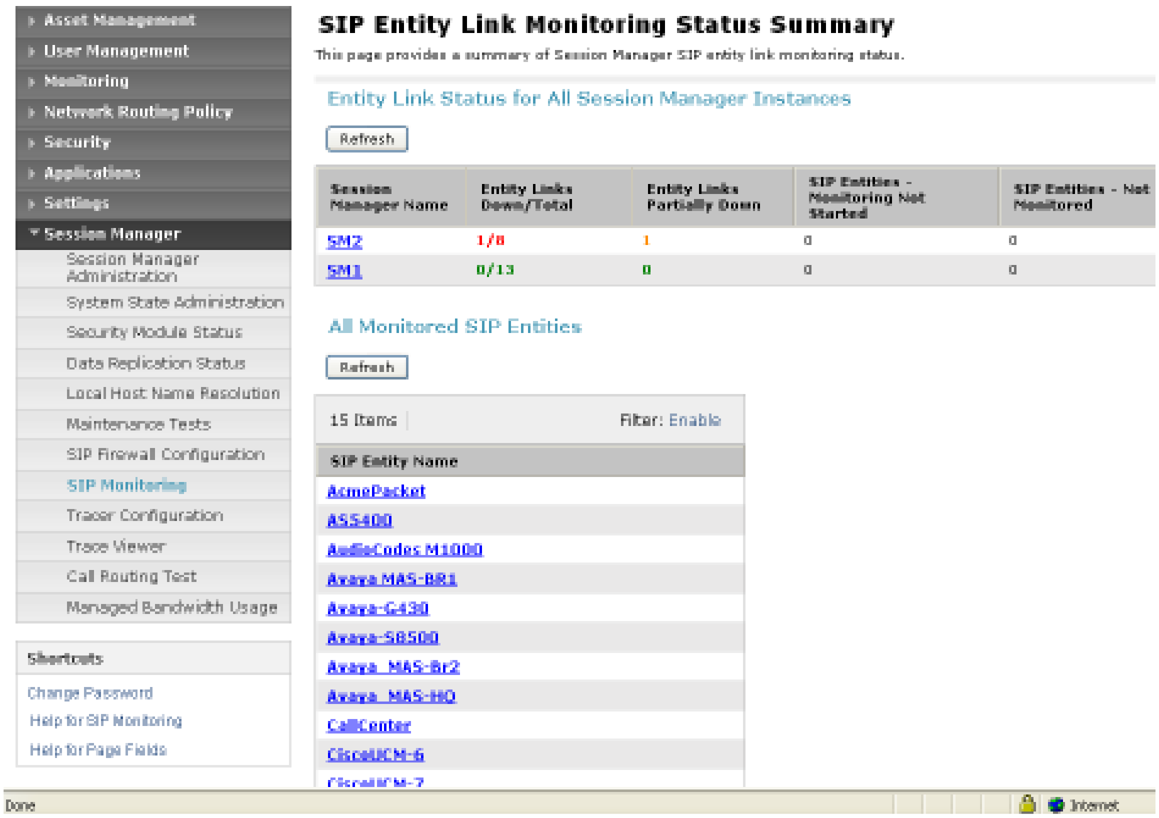
Hold/resume and transfer scenarios from both the Avaya telephone and Cisco telephone were verified and work properly as described previously. Screen details would be redundant and reveal no new information.

8.2. Verify Avaya Aura™ Session Manager

Avaya Aura™ Session Manager includes SIP monitoring and routing test capabilities that can aid in verifying proper configuration and operation.

8.2.1. SIP Monitoring

Select **Session Manager → SIP Monitoring** as shown below.



Select the name of the relevant SIP entity from the list of monitored SIP entities. The following screen shows a sample result when the “CiscoUCM-6” SIP Entity was selected. Observe that the connection is up. Cisco UCM is responding to the SIP OPTIONS message from Session Manager with a “200 OK”.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CiscoUCM-6

Refresh | Summary View

1 Item | Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▸ Show	SM1	60.1.1.9	5060	TCP	Up	200 OK	Up

Under the **Details** column, **Show** can be clicked to obtain further information, which may be particularly relevant if there is a problem. In this case, **Show** reveals the following:

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CiscoUCM-6

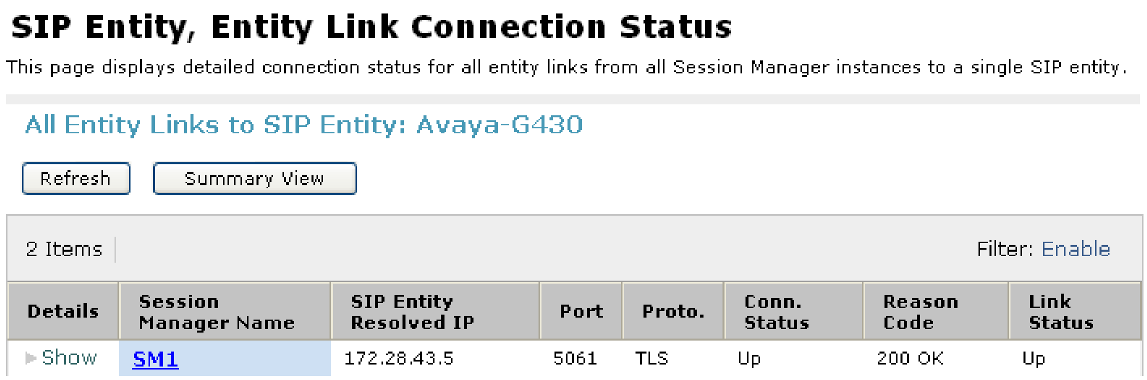
Refresh | Summary View

1 Item | Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▾Hide	SM1	60.1.1.9	5060	TCP	Up	200 OK	Up

Time Last Down	Time Last Up	Last Message Sent	Last Response Latency (ms)
Never	Jul 24, 2009 3:32:16 PM EDT	Jul 28, 2009 9:43:06 AM EDT	19

Similarly, information about the status of the link between Session Manager and Communication Manager can be obtained by selecting **Session Manager → SIP Monitoring** and clicking on the link named "Avaya-G430". As can be seen in the screen below, the connection is "Up". Communication Manager is also responding with a "200 OK" to SIP OPTIONS sourced by Session Manager.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Avaya-G430

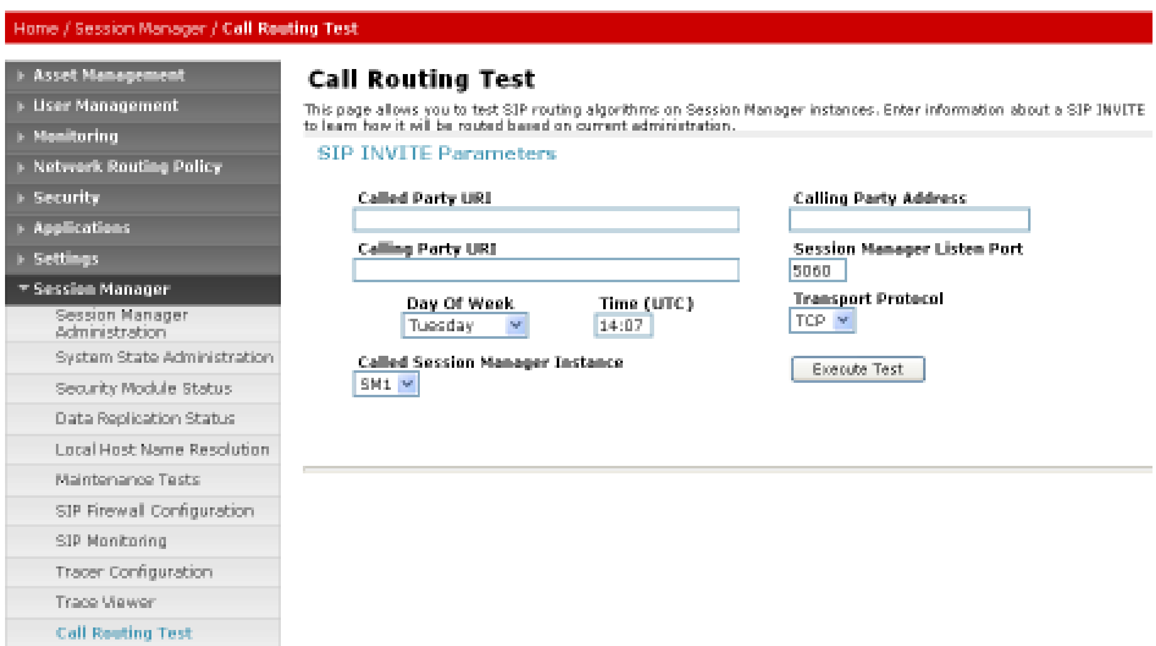
Refresh | Summary View

2 Items | Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▸ Show	SM1	172.28.43.5	5061	TLS	Up	200 OK	Up

8.2.2. Call Routing Test

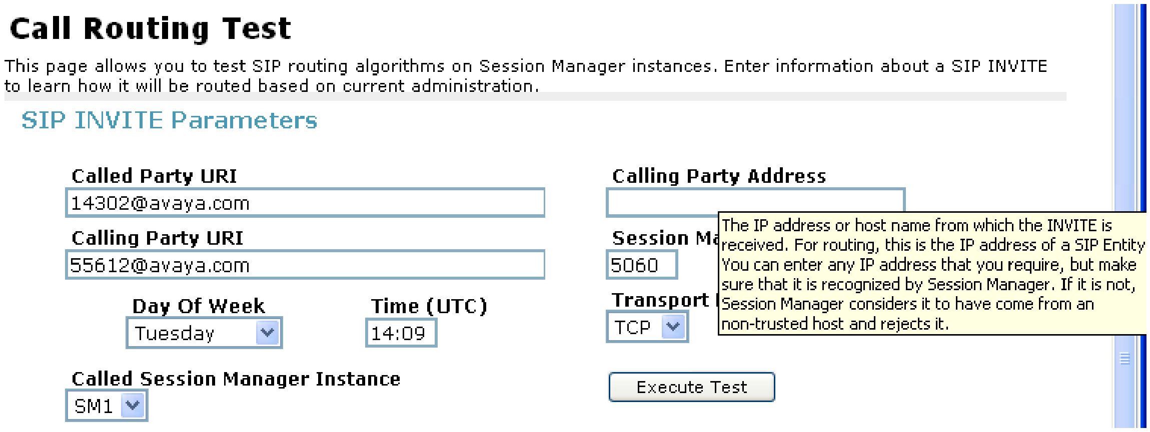
To check that the configured Network Routing Policy will result in the expected routing between systems, select **Session Manager → Call Routing Test.** The following screen is presented.



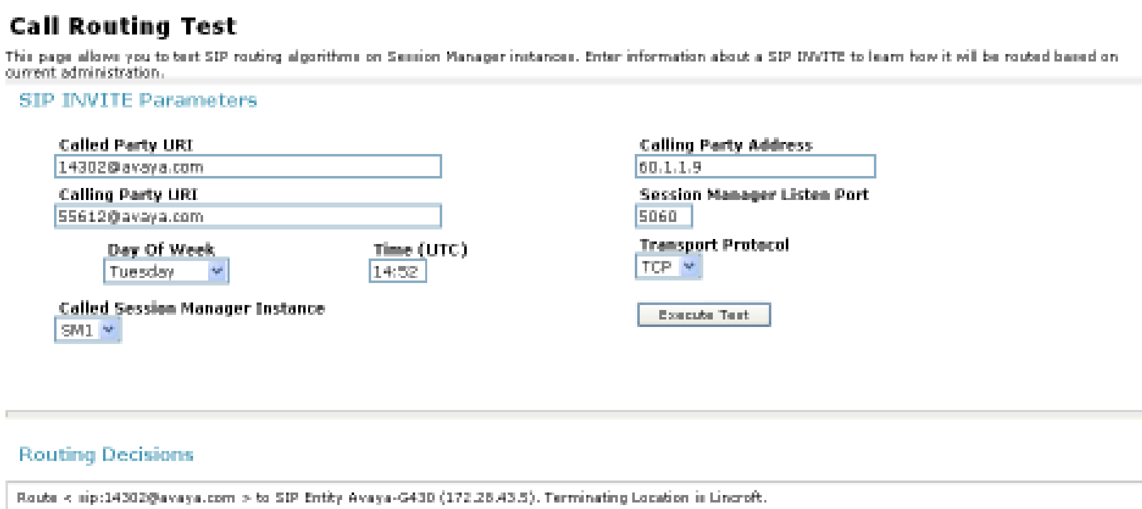
8.2.2.1 Cisco Telephone Calls Avaya Telephone

The following screen shows an example of a routing test for a Cisco telephone (55612) calling an Avaya telephone (14302). The self-explanatory **Called Party URI** and **Calling Party URI** fields are populated for a routing query. The mouse was placed over the

Calling Party Address field, showing an example of a "tool tip" associated with the fields.



After typing in the **Calling Party Address** with the IP Address of Cisco UCM, the **Execute Test** button is pressed. The following screen illustrates the summary result, under the heading **Routing Decisions**. If the caller is extension 55612, and the call comes from Cisco UCM using TCP port 5060, and arrives Tuesday at 14:52 (or "Anytime" in the sample configuration), and the called party is 14302, the call will be routed to SIP Entity "Avaya-G430" at terminating location "Lincroft". This is the expected result from the configuration presented in **Section 6**.



Scrolling down below the **Routing Decisions** heading, additional information is available that may reinforce understanding of the configuration and decision process. For example, from the following series of screen captures, it can be observed that the originating SIP entity is recognized as "CiscoUCM-6" in location "California". The CiscoAdapter is invoked to set, and the P-Asserted-Identity (PAI)is populated with the calling party number. (For an actual call that contained the caller's name in the Remote-Party-ID field, Session Manager would also copy the calling party name). No location-specific routing entry has been configured, but an "ALL" locations entry matches.

Routing Decision Process

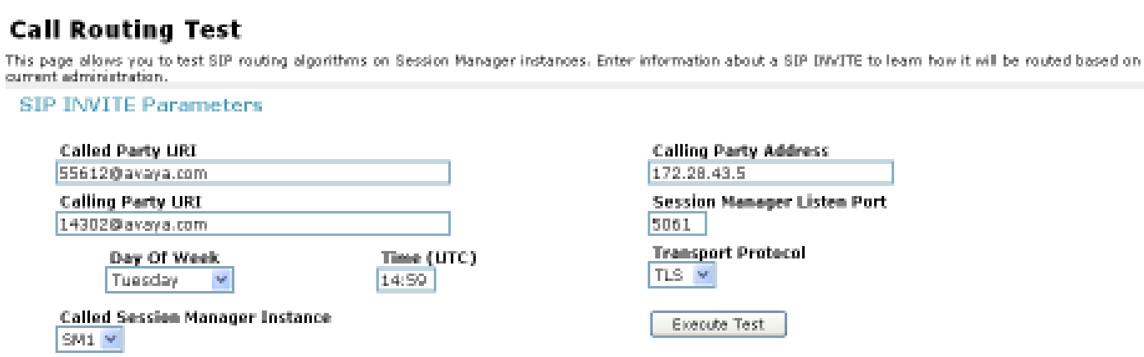
NRP Sip Entities: Originating SIP Entity is CiscoUCM-6.
NRP Adaptations: CiscoAdapter avaya.com applied.
NRP Adaptations: P-Asserted-Identity set to sip:55612@avaya.com
Originating Location is California. Using digits < 14302 > and host < avaya.com > for routing.
NRP Dial Patterns: No matches for digits < 14302 > and domain < avaya.com >.
NRP Dial Patterns: No matches for digits < 14302 > and domain < null >.
NRP Dial Patterns: No matches found for California. Trying again using NRP Dial Patterns that specify -ALL- NRP Locations.
NRP Dial Patterns: Found a Dial Pattern match for pattern < 143 > Min/Max length 5/5 and domain < avaya.com >.

Continuing to scroll down, the call will be routed to SIP Entity "Avaya-G430" using TLS and port 5061. Additional information follows, which is not presented here.

NRP Routing Policies: Ranked destination NRP Sip Entities: Avaya-G430.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP Sip Entities: Avaya-G430.
Adapting and proxying for SIP Entity Avaya-G430.
NRP Entity Links: Found direct link to destination. Link uses TLS to port 5061.

8.2.2.2 Avaya Telephone Calls Cisco Telephone

The following screen shows an example of a routing test for an Avaya telephone (14302) calling a Cisco telephone (55612). The Calling Party Address is the IP Address of the Avaya S8300 running Communication Manager. In this case, TLS and port 5061 is selected.



The following screen shows the summary result. The call will be routed to Cisco UCM at IP Address 60.1.1.9, in terminating location "California".

Routing Decisions

Route < sip:55612@avaya.com > to SIP Entity CiscoUCM-6 (60.1.1.9). Terminating Location is California.

Scrolling down below the **Routing Decisions** heading, the originating SIP entity is recognized as "Avaya-G430" in location "Lincroft". No location-specific routing entry is configured for Lincroft, but the "ALL" locations configuration matches. The screen below is truncated, but continuing further would illustrate the populating of the "Remote-Party-ID".

Routing Decision Process

NRP Sip Entities: Originating SIP Entity is Avaya-G430.
NRP Adaptations: DigitConversionAdapter avaya.com applied.
NRP Adaptations: P-Asserted-Identity set to sip:14302@avaya.com
Originating Location is Lincroft. Using digits < 55612 > and host < avaya.com > for routing.
NRP Dial Patterns: No matches for digits < 55612 > and domain < avaya.com >.
NRP Dial Patterns: No matches for digits < 55612 > and domain < null >.
NRP Dial Patterns: No matches found for Lincroft. Trying again using NRP Dial Patterns that specify -ALL- NRP Locations.
NRP Dial Patterns: Found a Dial Pattern match for pattern < 55 > Min/Max length 5/5 and domain < avaya.com >.
NRP Routing Policies: Ranked destination NRP Sip Entities: CiscoUCM-6.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP Sip Entities: CiscoUCM-6.
Adapting and proxying for SIP Entity CiscoUCM-6.

8.2.3. CiscoAdapter Summary for Improved Display Interoperability

Section 8.1.2 and Section 8.1.3 provide a summary of expected displays for basic calls and transferred calls. The CiscoAdapter of Session Manager plays an important role in providing display interoperability. For example, Cisco UCM sends and processes display information that appears in the "Remote-Party-ID". The Session Manager CiscoAdapter can extract information from standard SIP elements and populate the "Remote-Party-ID" for Cisco UCM consumption. Similarly, the Session Manager CiscoAdapter can extract information from the "Remote-Party-ID" and populate standard SIP elements for proper processing by Communication Manager.

8.2.3.1 Avaya Telephone Calls Cisco Telephone

When an Avaya telephone calls a Cisco telephone, the SIP INVITE message sent from Communication Manager to Session Manager will include standard SIP information about the caller (e.g., in the From header and P-Asserted-Identity or PAI). As the call passes through Session Manager, Session Manager inserts the Remote-Party-ID containing the name and number of the Avaya caller. The Cisco telephone displays the caller's information. When the Cisco telephone alerts, Cisco UCM sends a "180 RINGING" SIP message to Session Manager with the Remote-Party-ID containing the "Alerting Name" (if configured, see Section 7, Step 6) and number of the ringing telephone. Session Manager extracts the information from the Remote-Party-ID and populates the PAI in the 180 RINGING sent to Communication Manager.

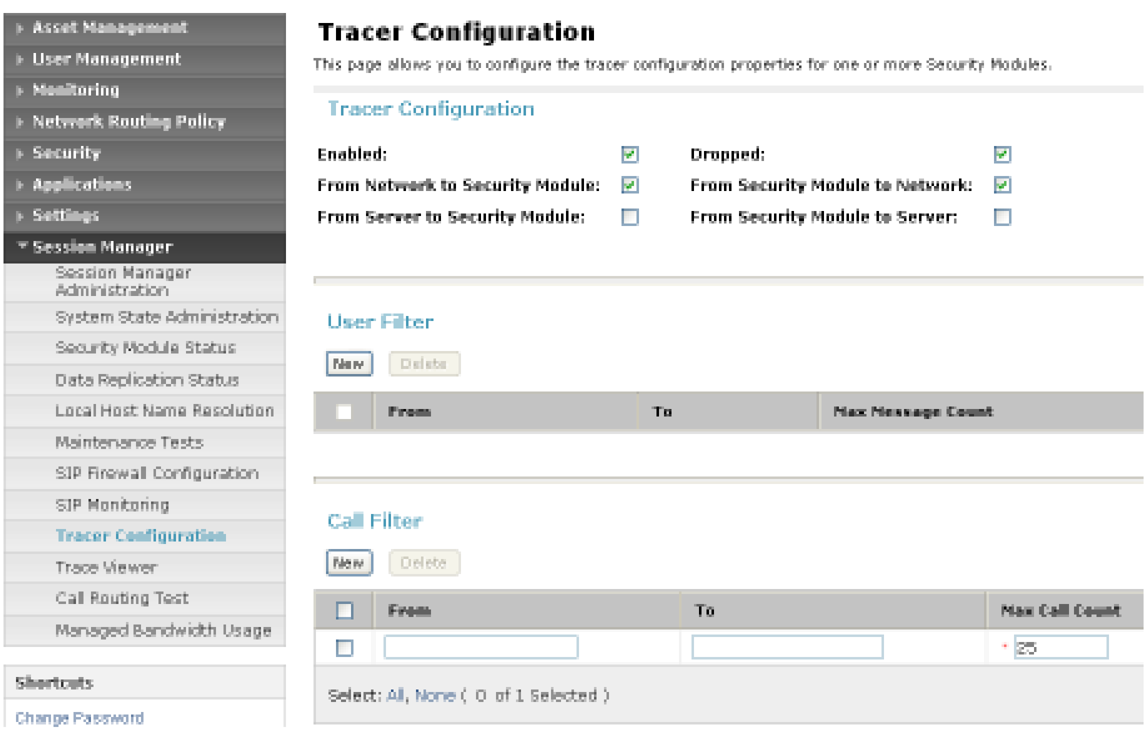
Communication Manager displays the name and number of the alerting Cisco user on the calling party's display. A similar adaptation is performed on the 200 OK message when the Cisco telephone answers the call.

8.2.3.2 Cisco Telephone Calls Avaya Telephone

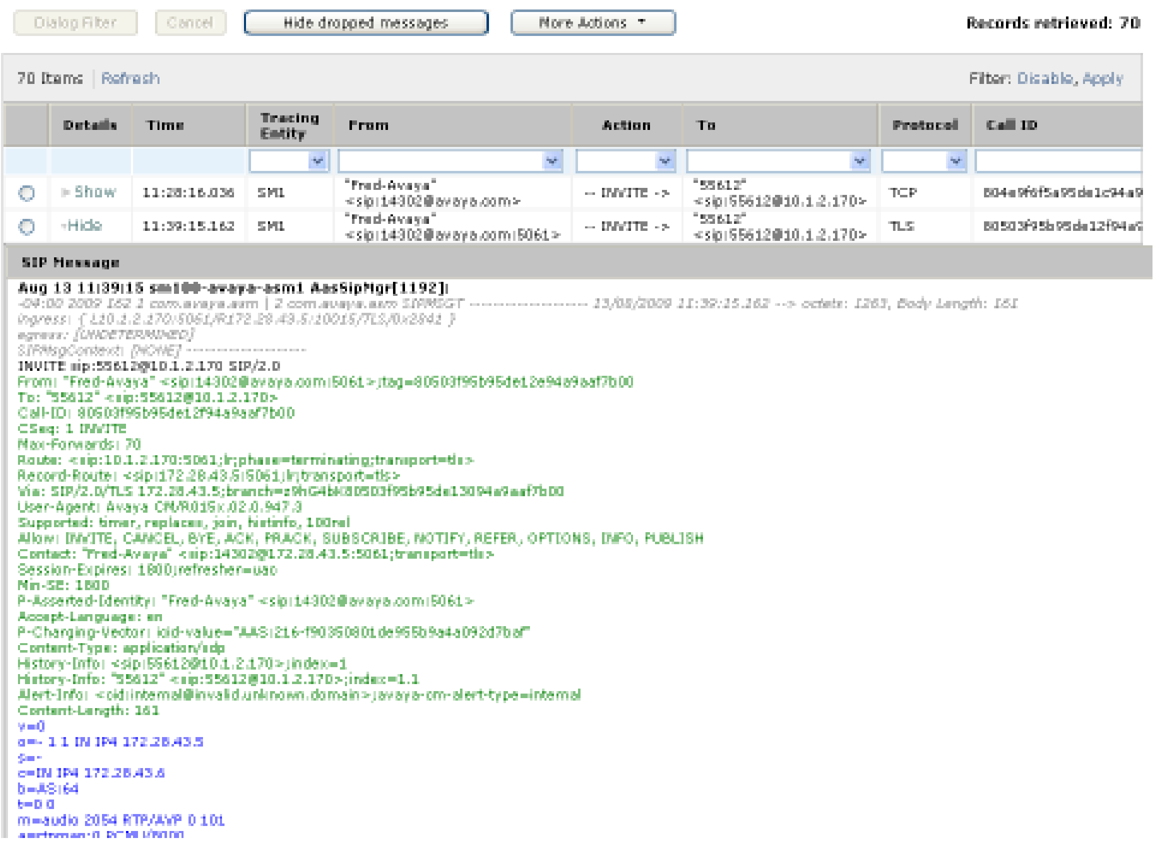
When a Cisco telephone calls an Avaya telephone, the SIP INVITE message sent from Cisco UCM to Session Manager can include the caller's name and number in the Remote-Party-ID. As the call passes through Session Manager, Session Manager extracts the caller's information from the Remote-Party-ID and populates standard SIP elements (e.g., PAI) in the SIP INVITE toward Communication Manager, which displays the caller's information on the alerting Avaya phone. When the Avaya telephone rings, Communication Manager sends a "180 RINGING" SIP message to Session Manager with the name and number of the ringing user in standard SIP elements (e.g., Contact, PAI). Session Manager extracts the alerting party information and populates the Remote-Party-ID for the 180 RINGING back to Cisco UCM. Cisco UCM displays the name and number of the alerting Avaya user on the calling party's display. A similar adaptation is performed on the 200 OK message when the Avaya telephone answers the call.

8.2.4. SIP Message Tracing

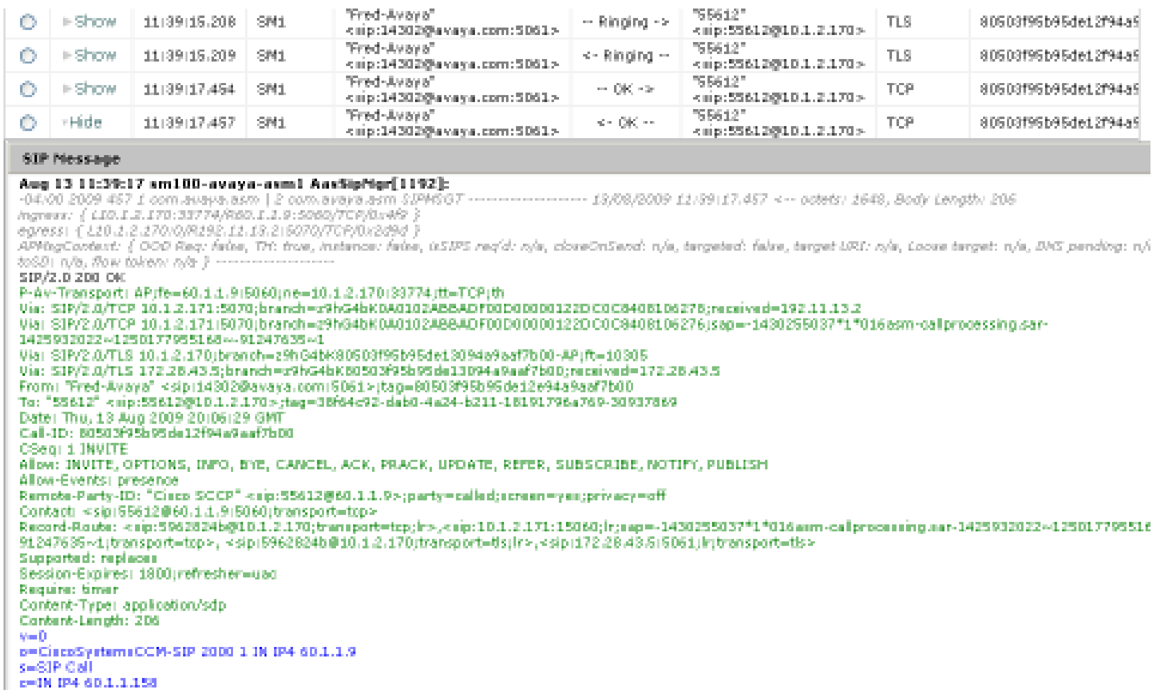
This section provides examples of Session Manager SIP message traces using the sample configuration. To configure tracing, select **Session Manager → Tracer Configuration** as shown below. Chapter 8 of reference [2] provides details on the available SIP tracing and filtering options available via this screen.



Once the tracer configuration has been established, SIP message traces can be viewed by selecting **Session Manager → Tracer Viewer**. The following screen shows an example of an expanded SIP INVITE message sent by Communication Manager to Session Manager. Note that SIP message tracing visibility via Session Manager is still possible when TLS is used between Communication Manager and Session Manager. That is, it is not necessary to change the transport to TCP in order to have visibility into the SIP messages as is typically the case using a line monitoring tool.



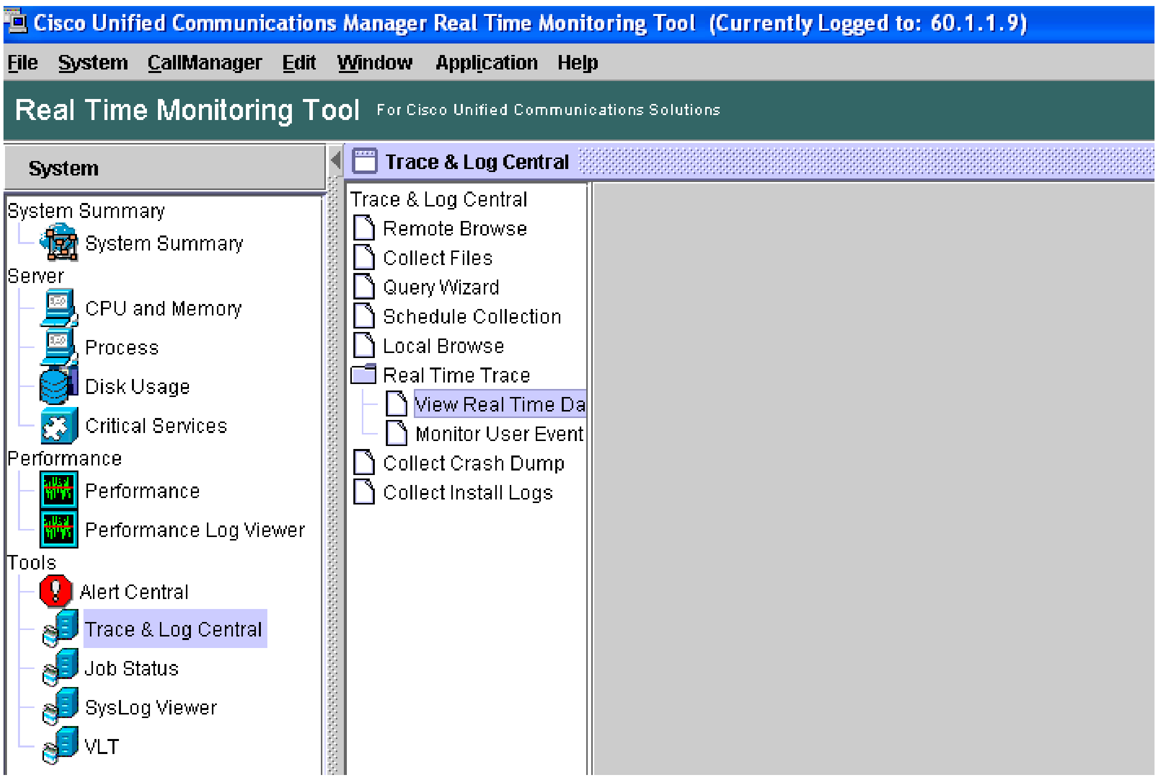
The following screen shows an expanded 200 OK from Cisco UCM for this same call. Observe the contents of the Remote-Party-Id containing the name and number of the answering Cisco telephone.



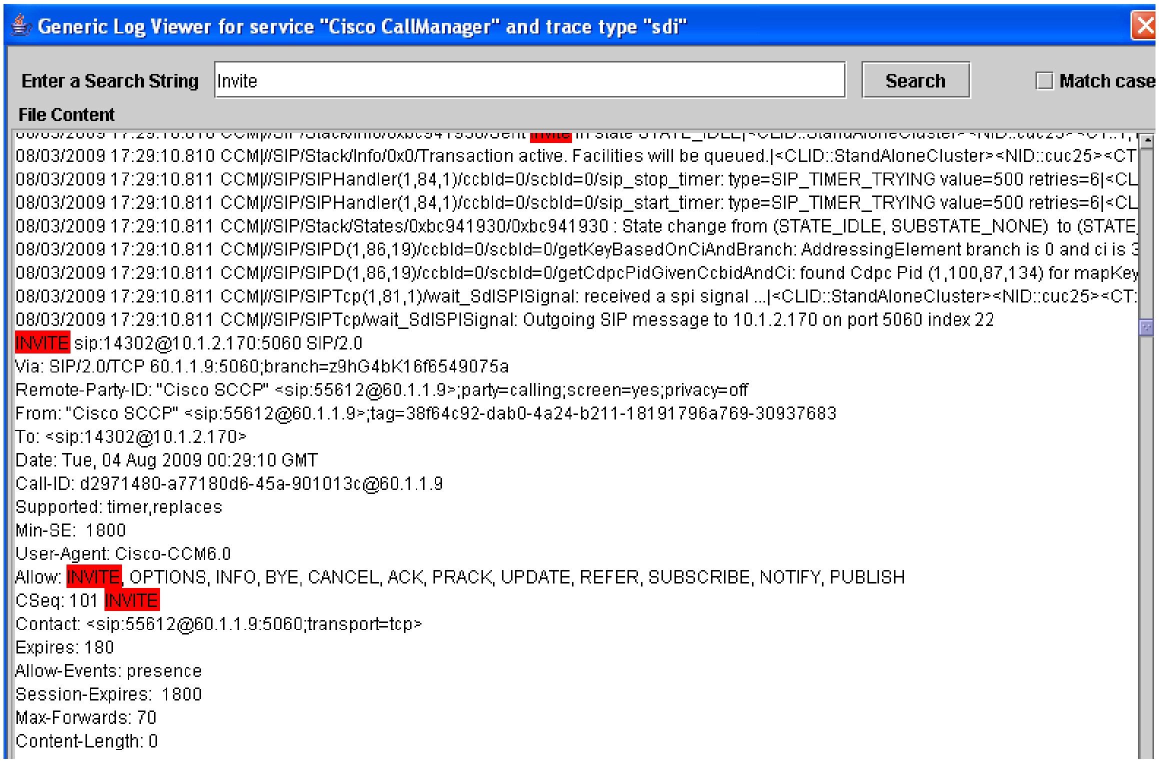
The following screen shows an expanded 200 OK from Session Manager to Communication Manager for this same call. Observe the contents of the P-Asserted-Identity inserted by the Session Manager "CiscoAdapter".

8.3. Verify Cisco Unified Communications Manager

The Real Time Monitoring Tool (RTMT) can be used to monitor events on Cisco UCM. This tool can be downloaded by selecting **Application → Plugins** from the top menu of the Cisco UCM Administration Web interface. For further information on this tool, please consult with reference [9]. Once the Real Time Monitoring Tool plug-in is installed, real-time data can be captured by selecting **Tools → Trace & Log Central** in the left panel, and **Real Time Trace → View Real Time Data** on the right.



The following screen shows an example of a small portion of detailed trace information available with the tool. In this case, a call was made from Cisco telephone extension 55612 to Avaya telephone extension 14302. The string "Invite" was entered in the top search bar.



8.4. Verification Summary

Verification of the configuration described in these Application Notes included the following items:

- Basic calls between telephones on Avaya Aura™ Communication Manager and Cisco Unified Communications Manager. A sampling of detailed trace output for calls can be found in Sections 8.1.2 and 8.1.3. Calls can be made in both directions using G.711MU and variants of G.729. For G.729 interoperability with Cisco SIP phones, the Avaya Aura™ Communication Manager IP codec set (i.e., codec set 3 in the sample configuration) must include "G.729" or "G.729A". If G.729B is desired for other types of connections for which the communicating devices indicate support, the Communication Manager codec set can list both "G.729B" and "G.729" to avoid a codec set mismatch for calls involving a Cisco SIP phone.

- Proper display of the calling and called party name and number information was verified for all telephones with the basic call scenario. Display examples are provided in Section 8.1.2 and 8.1.3. Presentation of the calling party information can also be restricted from presentation. For example, an Avaya user may use the "Calling Party Number Block" feature to prevent calling party information from appearing on the display of a called Cisco telephone, which will display "From Private". Similarly, if "Calling Line ID Presentation for Outbound Calls" is set to restricted for the Cisco SIP Trunk, the Avaya caller will see "CALL FROM <configurable string>" where the <configurable string> text is configured via the "CPN/ANI/ICLID Replacement for Restricted Calls" parameter on page 9 of the Communication Manager "change system-features" form.

- Verification of common telephony operations included:
  - Hold, music-on-hold, and resume from hold
  - Unattended (blind) transfer
  - Attended (consult) transfer
  - Conference via conference key on telephones
  - Conference via join of Avaya meet-me conference, which also verified proper collection of post-answer DTMF via RFC2833 to collect the conference password
  - Call forwarding all calls

The following interoperability issues were observed:

- Display related:
  - For proper display of calling and called party information, ensure that Cisco UCM users are configured as described in Section 7, Step 6. If the Cisco Alerting Name is not configured, or configured with a different name than the name associated with the line, displays will differ from the intuitive displays described in Section 8.1.2 and 8.1.3.
  - Restricted presentation of display information is either off, (i.e., both name and number appear on the display), or privacy is full, where neither name nor number are presented on the display. That is, it is not possible to restrict only the number but display the name, or restrict only the name, and display the number.
  - If a call is established between an Avaya telephone and a Cisco telephone, and the call is transferred from the Cisco telephone back to another Avaya telephone, the transferred-to Avaya telephone will continue to display the name and number of the Cisco telephone, even after completion of the transfer.
- Shuffling to ip-direct related:
  - See Section 8.1.3.1 for a specific scenario that forces the recommendation to disable ip-direct media connections between Avaya telephones and Cisco telephones. This problem has also been observed with Cisco UCM Release 7, and further elaboration can be found in Section 9 of reference [6].
  - Even if shuffling to ip-direct media is administratively enabled, calls between Avaya H.323 telephones and Cisco SCCP telephones will result in the same connection topology as illustrated in these Application Notes in Sections 8.1.2 and 8.1.3. That is, the final media path across the SIP trunk will be from the

Avaya G430 VoIP resource to the Cisco SCCP telephone, whether ip-direct media is disabled or enabled.

9. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager can interoperate with Cisco Unified Communications Manager Release 6 using SIP trunks via Avaya Aura™ Session Manager.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Avaya Aura™ Session Manager Overview*, Doc # 03-603323
[2] *Installing and Administering Avaya Aura™ Session Manager*, Doc # 03-603324
[3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc # 03-603325
[4] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, May 2009
[5] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509 May 2009
[6] *Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Cisco Unified Communications Manager (Release 7), Issue 1.0*
https://devconnect.avaya.com/public/flink.do?f=/public/download/interop/ASM-ACM-CUCM.pdf

Product documentation for Cisco Systems products may be found at http://www.cisco.com

[7] *Cisco Unified Communications Manager Administration Guide,* Release 6.0(1), Part Number: OL-12525-01
[8] *Cisco Unified Serviceability Configuration Guide for Cisco Unified Communications Manager*, Release 6.0(1), Part Number: OL-12425-01
[9] *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide,* Release 6.0(1), Part Number: OL-12414-01

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