Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Cisco Unified Communications Manager – 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 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 Avaya G430 Media Gateway, and Cisco Unified Communications Manager runs on 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) using SIP trunks.

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. The Cisco UCM supports the Cisco 7965 IP Telephone (SIP) and the Cisco 7912 IP Telephone (SCCP). SIP trunks are used to connect these two systems to Avaya Aura™ Session Manager. All inter-system calls are carried over these SIP trunks. Avaya Aura™ Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow for multi-vendor systems to interoperate. The Avaya Aura™ Session Manager is managed by a separate Avaya Aura™ System Manager, which can manage multiple Avaya Aura™ Session Managers.

3. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All telephones in the 172.28.10.0/24 IP network are either registered with Avaya Aura™ Communication Manager and uses extension 143xx. All IP telephones in the 172.29.5.0/24 IP network are registered with Cisco UCM and uses extension 60xxx. 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.

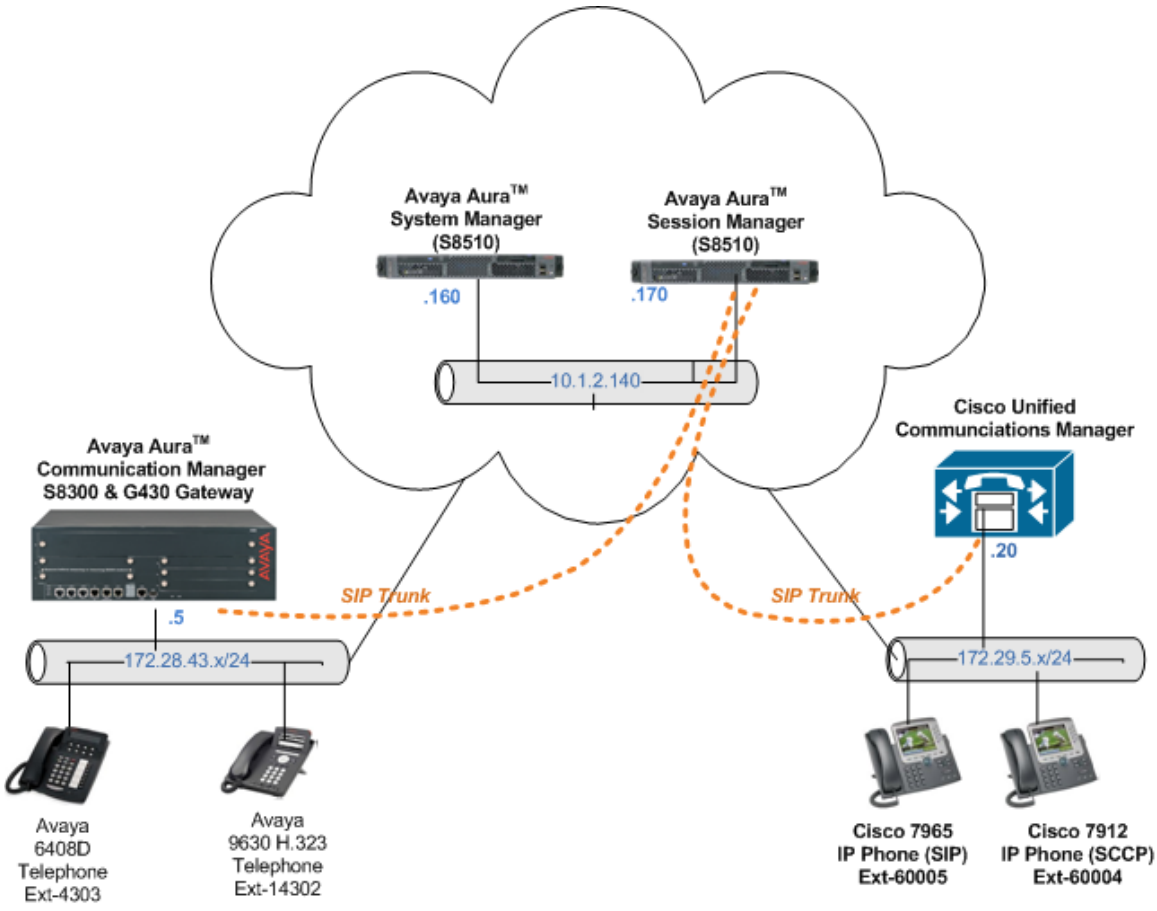


Figure 1: Sample Network Configuration

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) SP0 (02.0.947.3-17250)
Avaya Aura™ System Manager - Running on an Avaya S8510 Server	1.0
Avaya Aura™ Session Manager - Running on an Avaya S8510 Server	1.1
Avaya 9630 IP Telephone (H.323)	3.0
Avaya 6402D Digital Telephone	-
Cisco Unified Communications Manager	7.0.1.1.11000-2 or 7.0.2.2000-5
Cisco 7965 Unified IP Phone (SIP)	SIP45.8-4-1S
Cisco 7912 Unified IP Phone (SCCP)	App Load ID CP7912080003SCCP070409A Boot Load ID LD0100BOOT021112A

5. Configure Avaya Aura™ Communication Manager

This section shows the configuration of Avaya Aura™ Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Avaya Aura™ Communication Manager, please consult with references [4] and [5]. The procedures include the following areas:

- Verify Avaya Aura™ Communication Manager license
- Administer system parameters features
- Administer IP nodes names
- Administer IP interface
- Administer IP codec set and network region
- Administer SIP trunk group and signaling group
- Administer SIP trunk group members and router patterns
- Administer location and public unknown numbering
- Administer uniform dial plan and AAR analysis

1. Use the "display system-parameter customer options" command to verify whether the **Maximum Administered SIP Trunks** field value with the corresponding value in the USED column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

   Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                    Page   2 of  10
                              OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 50    6
          Maximum Concurrently Registered IP Stations: 450   1
            Maximum Administered Remote Office Trunks: 450   0
Maximum Concurrently Registered Remote Office Stations: 450   0
             Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                       Maximum Video Capable Stations: 100   0
                   Maximum Video Capable IP Softphones: 100   0
                       Maximum Administered SIP Trunks: 100   20
```

2. Use the "change system-parameters features" command to allow for trunk-to-trunk transfers.

   This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to "all" to enable all trunk-to-trunk transfers on a system wide basis.

   Note: This feature poses significant security risk, and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels.

```
change system-parameters features                             Page   1 of  18
                           FEATURE-RELATED SYSTEM PARAMETERS
                              Self Station Display Enabled? n
                                   Trunk-to-Trunk Transfer: all
              Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: music Type: ext   14383
             Music (or Silence) on Transferred Trunk Calls? no
                      DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
```

3. Use the “change node-names ip” command to add entries for the “procr” and Avaya Aura™ Communication Manager that will be used for connectivity. In the sample network, “procr” and “172.28.43.5” are entered as Name and IP Address for the Avaya Aura™ Communication Manager running on the Avaya S8300 Server. In addition, “ASM” and “10.1.2.170” are entered for Avaya Aura™ Session Manager.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM                  10.1.2.170
default              0.0.0.0
msgserver            172.28.43.9
procr                172.28.43.5
```

4. Use the “change ip-network-region n” command, where “n” is the network region number to configure the network region being used. In the sample network ip-network-region 1 is used. For the Authoritative Domain field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec-Set** to 1 to use ip-codec-set 1.

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name: ASM-to-Cisco
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
```

5. Use the “change ip-codec-set n” command, where “n” is the existing codec set number to configure the desired audio codec.

Note: In addition to the “G.711MU” codec shown below, “G.729” and “G.729AB” have also been verified to be interoperable with Cisco UCM via SIP trunks.

```
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:
```

6. In the test configuration, signal group 25 along with trunk group 25 were used to reach Avaya Aura™ Session Manager. Use the “add signaling-group n” command, where “n” is the signaling-group number being added to the system. The “Far-end Domain” is left blank so that the signaling group accepts any authoritative domain.

```
                               SIGNALING GROUP

 Group Number: 25             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: 1
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? n                 Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

7. Use the “add trunk-group n” command, where “n” is the new trunk group number being added to the system.

   The following screens show the settings used for trunk group 25.

```
Add trunk-group 25                                          Page   1 of  21
                               TRUNK GROUP

Group Number: 25                   Group Type: sip           CDR Reports: y
  Group Name: To-ASM                        COR: 1        TN: 1        TAC: 125
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                 Auth Code? n

                                                    Signaling Group: 25
                                                  Number of Members: 10
```

```
add trunk-group 25                                          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

 Show ANSWERED BY on Display? Y
```

```
add trunk-group 25                                          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
```

8. Use the "change public-unknown-numbering" command to define the calling party number to be sent out to through the SIP trunk. Add an entry for the trunk group defined in **Step 7**. In the sample network configuration below, all calls originating from a 5-digit extension beginning with 143 and routed to trunk group 25 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
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: 3
 5  143          25                       5          Maximum Entries: 240
```

9. Configure the dial plan for dialing 5-digit extensions beginning with "60" to stations registered with Cisco UCM. Use the "change dialplan analysis" command to define dialed string 60 as an aar call type.

```
change dialplan analysis                                    Page   1 of  12
                          DIAL PLAN ANALYSIS TABLE
                               Location:  all          Percent Full:    2

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
    1           3    dac
    143         5    ext
    60          5    aar
    8           1    fac
    9           1    fac
    *           3    fac
    #           3    fac
```

10. Use the “change aar analysis n” command where “n” is the dial string pattern to configure an aar entry for Dialed String 60 to use Route Pattern 25.

```
change aar analysis 60                                          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
   60                    5    5    25        aar          n
   7                     7    7    254       aar          n
   8                     7    7    254       aar          n
   9                     7    7    254       aar          n
```

11. Configure a route pattern to correspond to the newly added SIP trunk group. Use the “change route-pattern n” command, where “n” is the route pattern number specified in **Step 10**. Configure this route pattern to route calls to trunk group number 25 configured in **Step 7.**

```
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: 25   0                                                        n   user
 2:                                                               n   user
 3:                                                               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
```

12. Use the “save translation” command to save all changes.

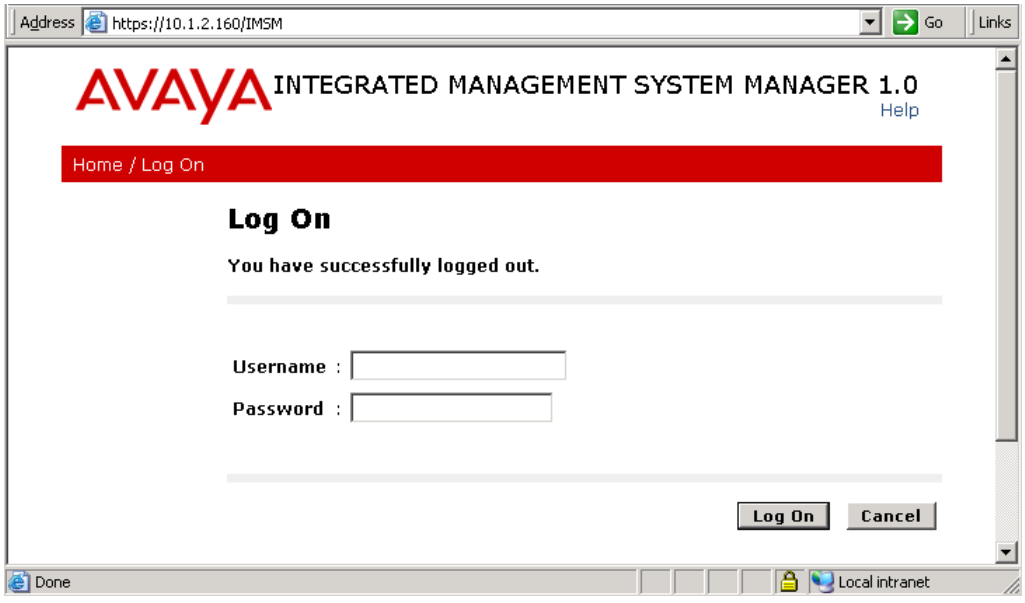
```
save translation

                               SAVE TRANSLATION

          Command Completion Status                              Error Code

          Success                                                0
```

6. Configuring Avaya Aura™ Session Manager

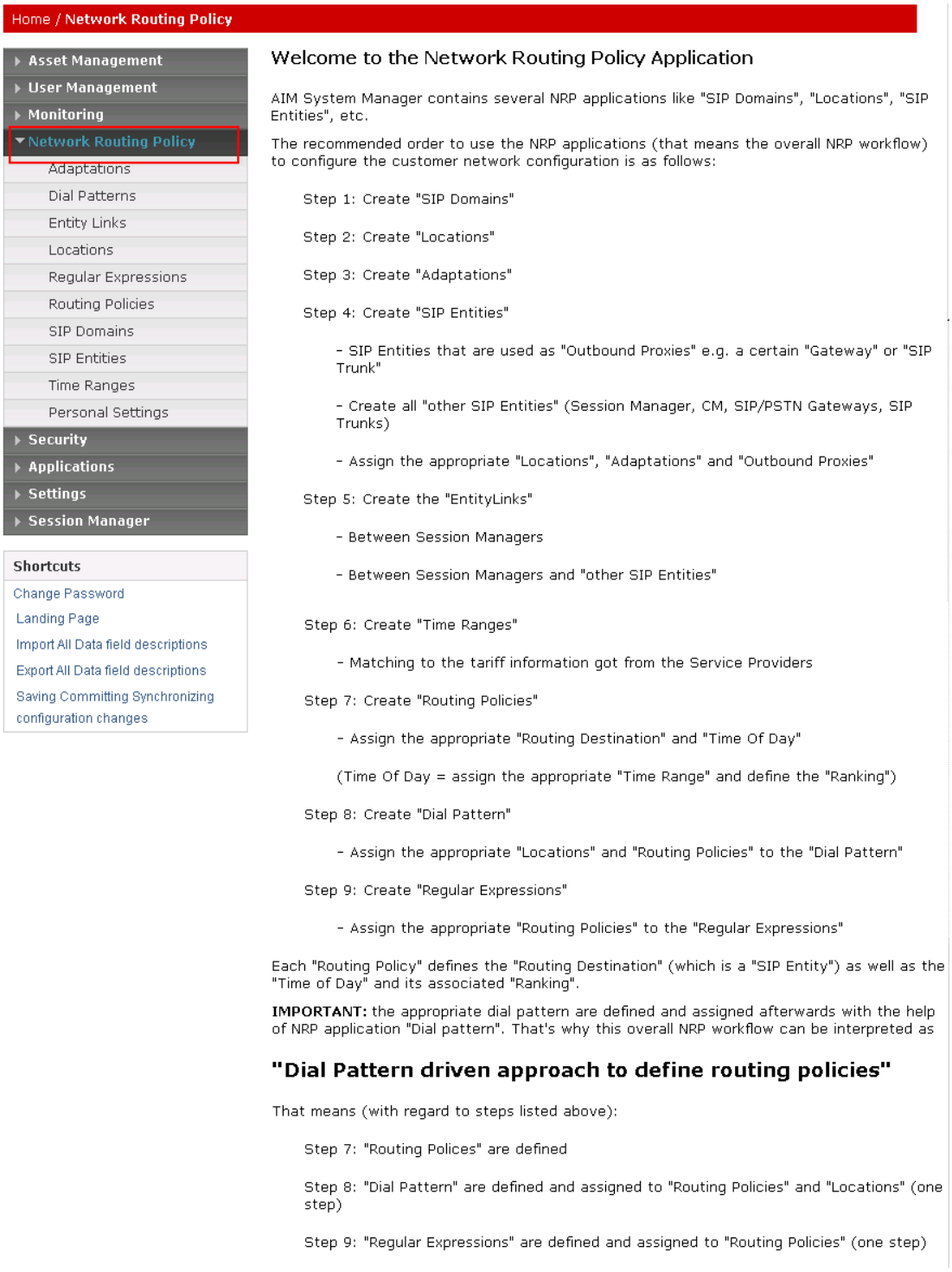
This section provides the procedures for configuring Avaya Aura™ Session Manager. For further information on Avaya Aura™ Communication Manager, please consult with references [1], [2], and [3]. The procedures include the following areas:

- SIP domain
- Adaptations
- SIP Entities corresponding to the SIP telephony systems and Avaya Aura™ Session Manager
- Entity Links, which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
- Time Ranges during which routing policies are active
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern how a call is routed
- Avaya Aura™ Session Manager, corresponding to the Avaya Aura™ Session Manager Server to be managed by Avaya Aura™ System Manager

1. Access the Avaya Aura™ System Manager using a Web Browser and entering http://<ip-address>/IMSM, where <ip-address> is the IP address of Avaya Aura™ System Manager. Log in using appropriate credentials and accept the subsequence Copyright Legal Notice.



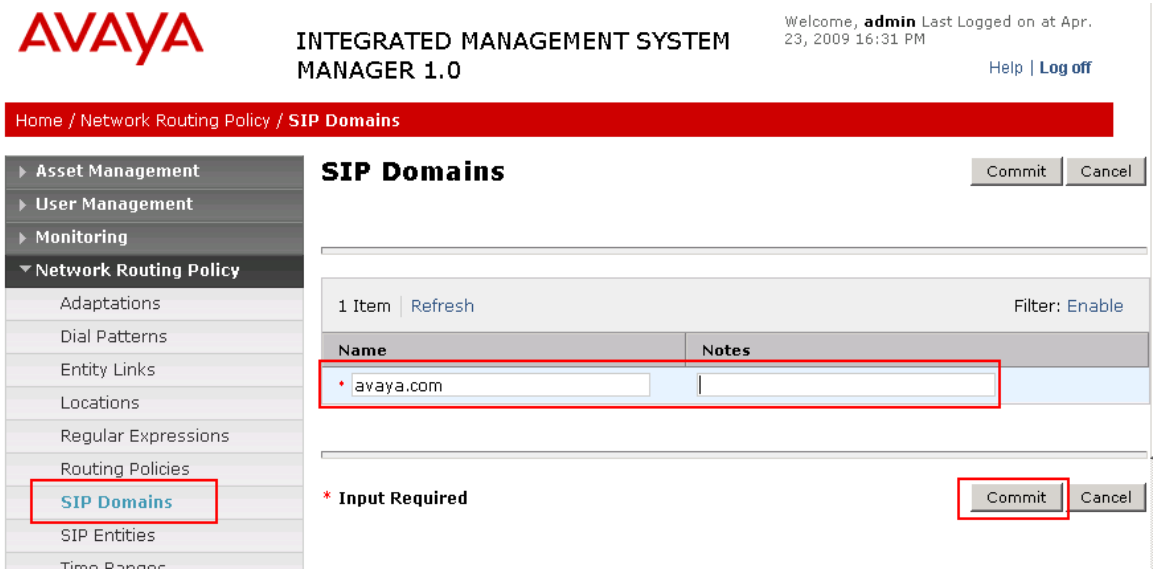
2. Begin configuration by selecting **Network Routing Policy** from the left panel menu. A short procedure for configuring Network Routing Policy is shown on the right panel.



3. Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting SIP Domains on the left panel menu and clicking the **New** button (not shown) to create a new SIP domain entry. The following screen will be shown after clicking **New**. Click **Commit** to save changes.

    Name The authoritative domain name (e.g., "avaya.com")
    Notes Description for the domain (optional)

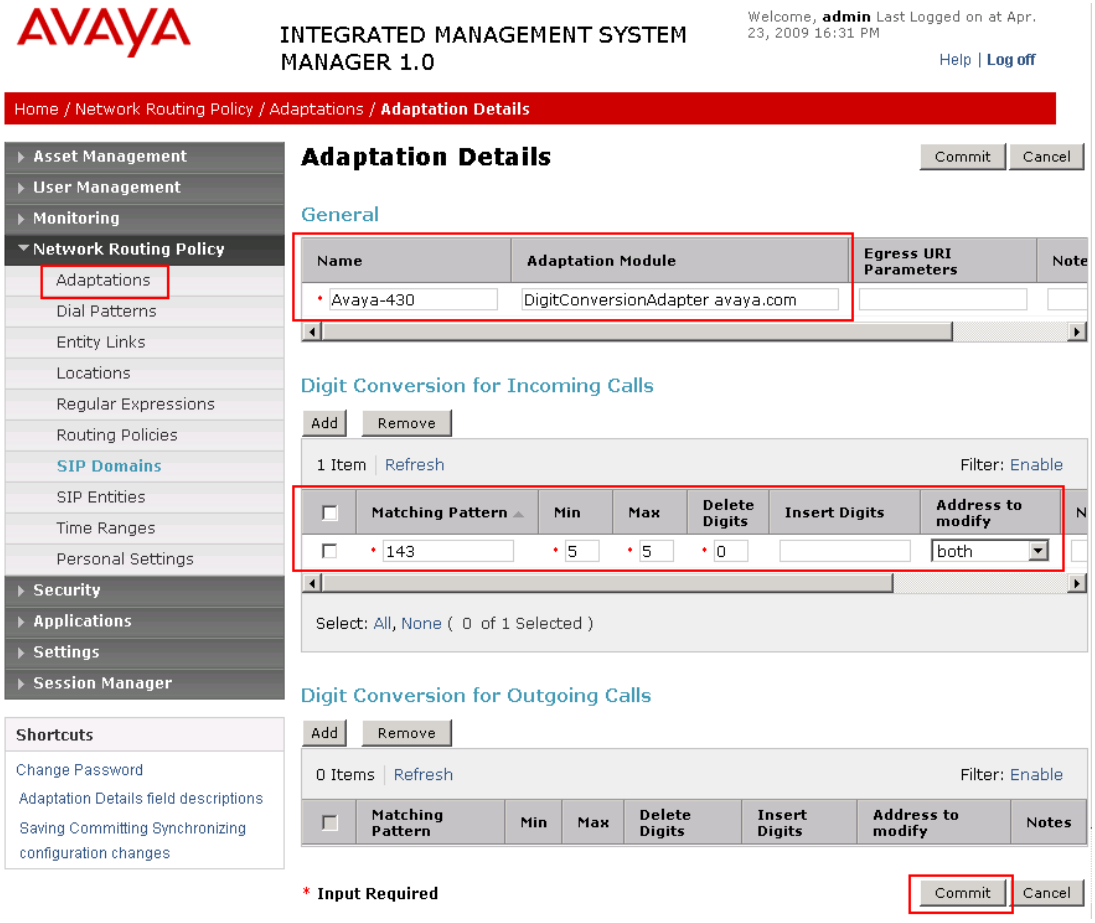
    Note: Since the sample network does not deal with any foreign domains, no additional SIP Domains entry is needed.



4. Create 2 Adaptations entry. One for incoming call from Avaya Aura™ Communication Manager, and the other for incoming call from Cisco UCM.

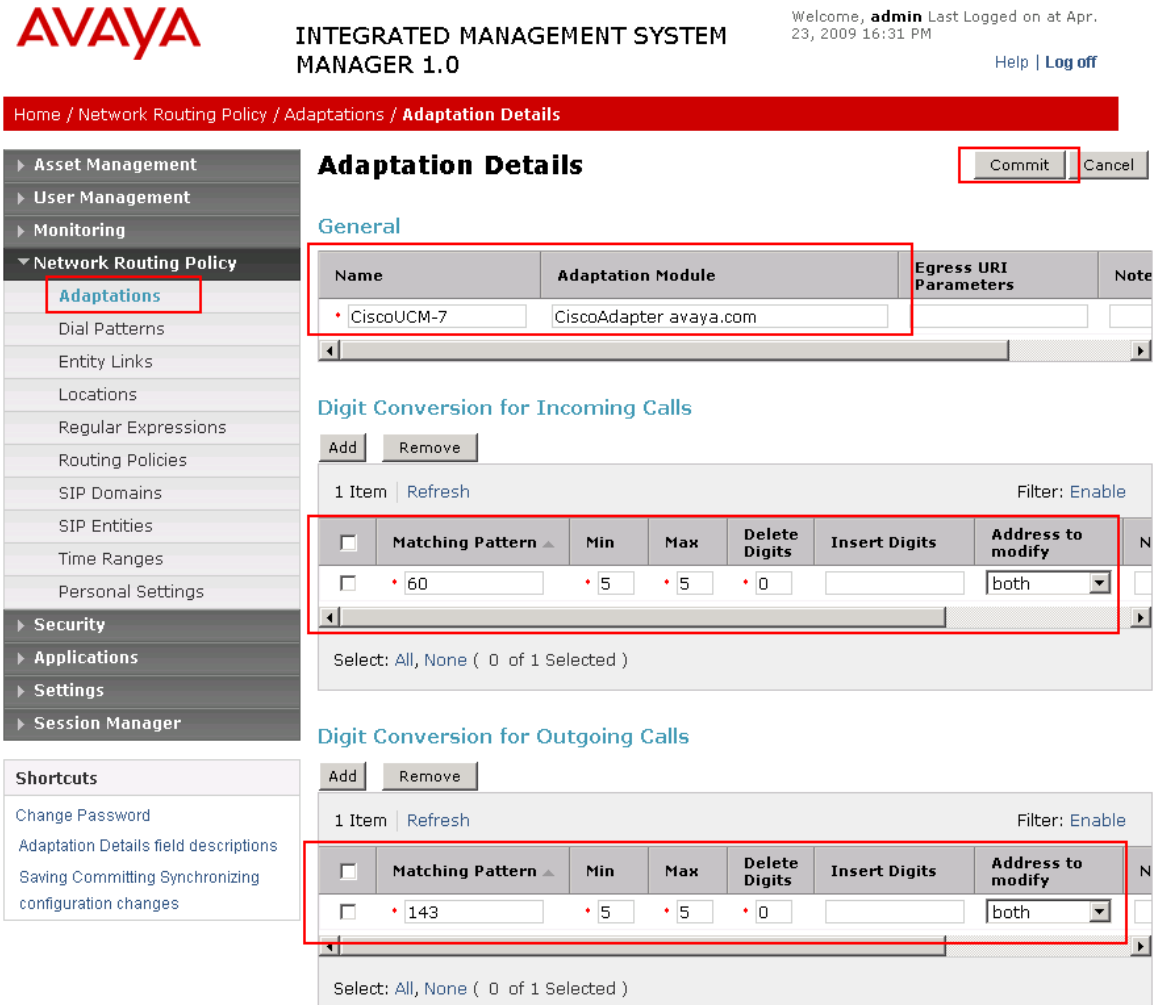
   For the Avaya Aura™ Communication Manager adaptation, enter the following information.

   Name An informative name for the adaptation (e.g., Avaya-G430)
   Adaptation Module Enter "DigitConversionAdapter avaya.com"
   Digit Conversion for incoming Calls
   Matching Pattern 143 with a minimum and maximum of 5 digits long, which is the dial pattern for station registered with Avaya Aura™ Communication Manager.



For the Cisco UCM adaptation, enter the following information.

Name CiscoUCM-7, an informative name for the adaptation
Adaptation Module Enter "CiscoAdapter avaya.com"
Digit Conversion for incoming Calls
Matching Patterns 60 with a minimum and maximum of 5 digits long, which is the dial pattern for station registered with Cisco UCM.



5. A SIP Entity must be added for Avaya Aura™ Session Manager for each SIP-based telephony system supported by a SIP Trunk. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown) on the right. Enter the following for each SIP Entity.

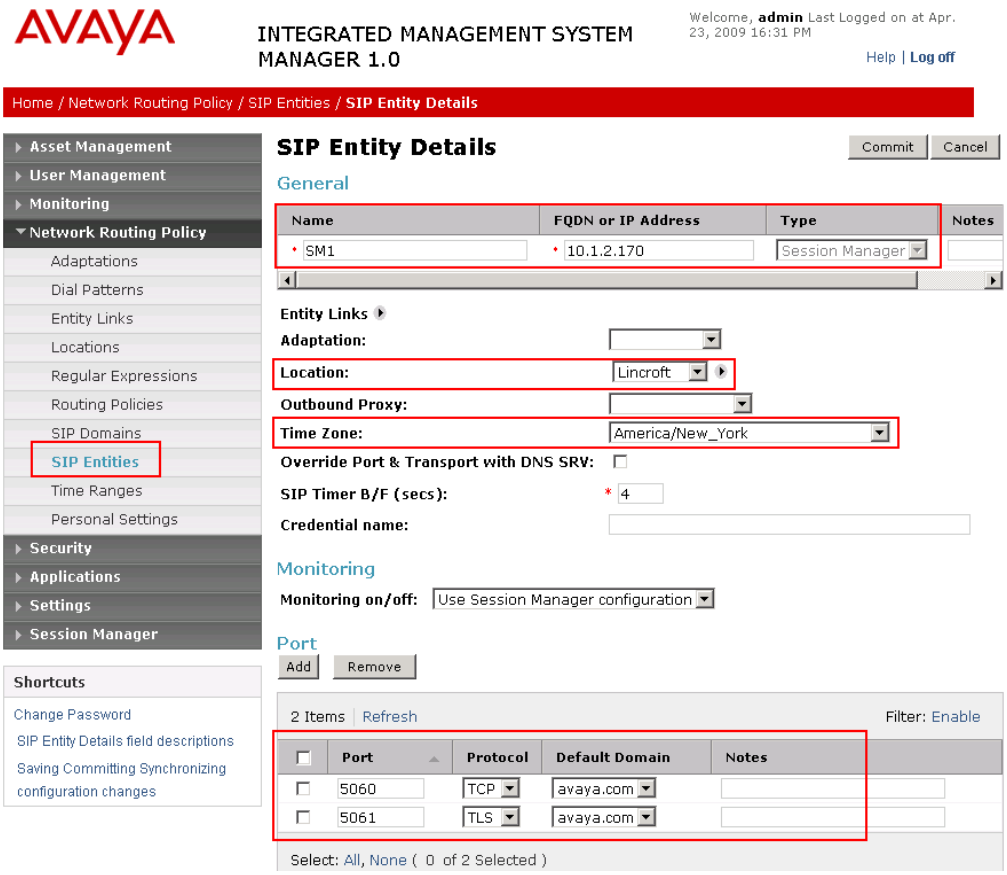
   Under General:

Name	An informative name (e.g., SM1)
FQDN or IP Address	IP address of the ASM or the signaling interface on the telephony system
Type	” Session Manager” for Avaya Aura™ Session Manager, “CM” for Avaya Aura™ Communication Manager, or “Other” for Cisco UCM
Time Zone	Time zone for this location

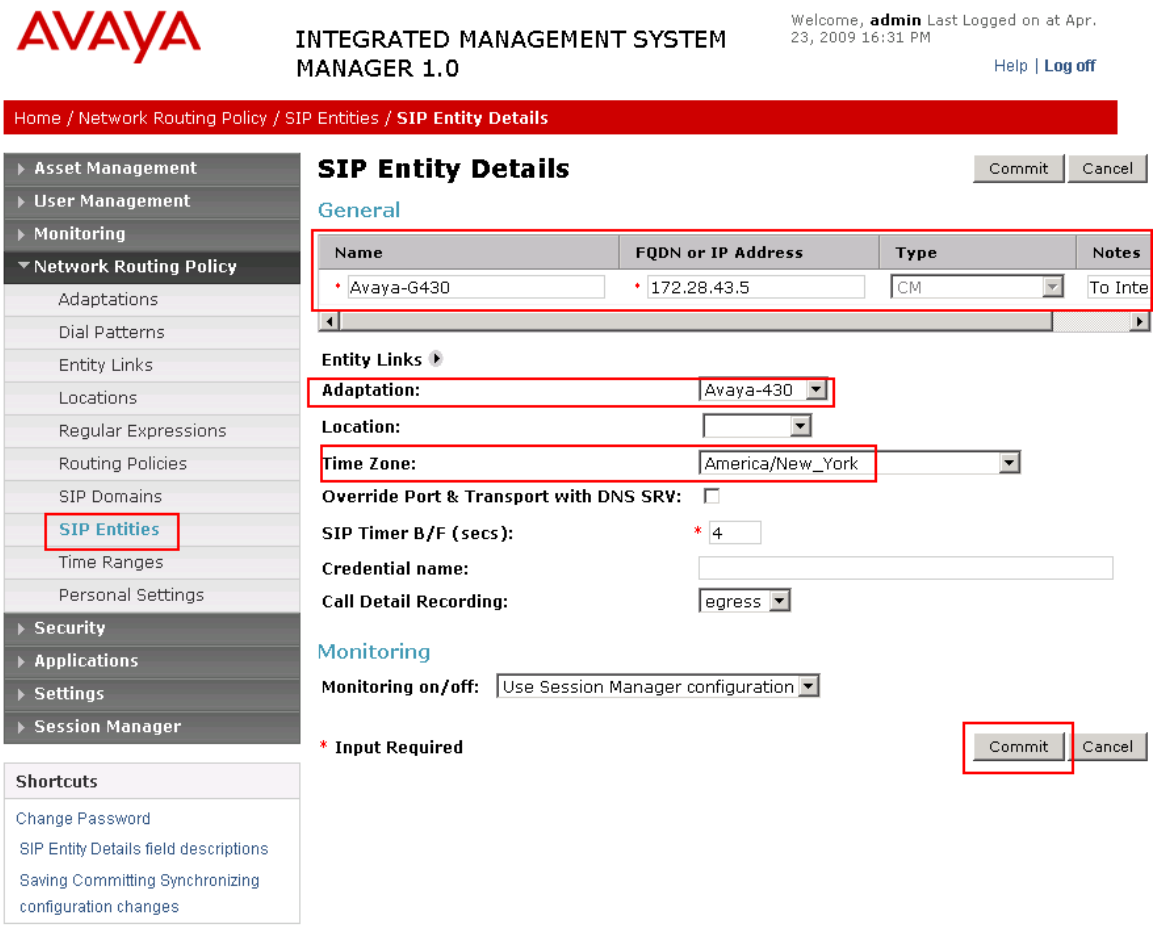
   Under Port, click **Add,** and then edit the fields in the resulting new row

Port	Port number on which the system listens for SIP requests
Protocol	Transport protocol to be used to send SIP requests

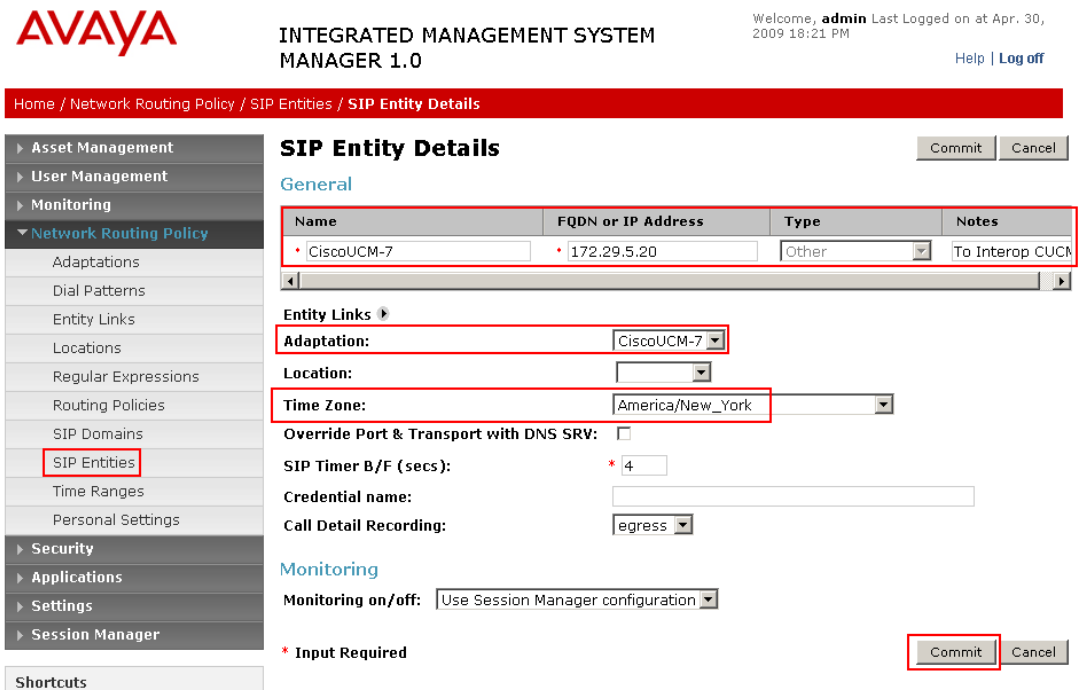
   The following screen shows the SIP Entity for Avaya Aura™ Session Manager after clicking New.



The following screen shows the SIP Entity for Avaya Aura™ Communication Manager.



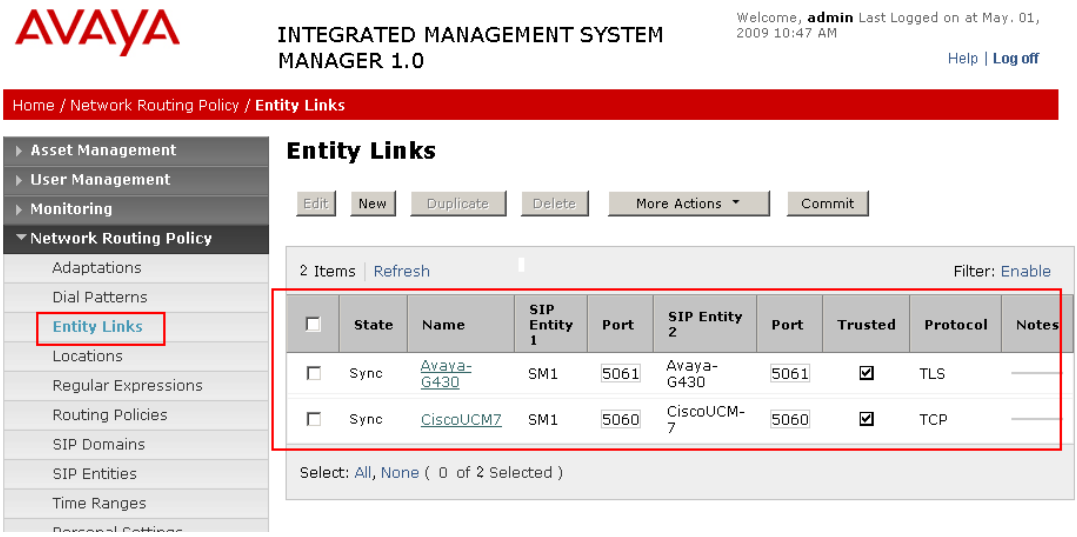
The following screen shows the SIP Entity for Cisco UCM.



6. A SIP trunk between Avaya Aura™ Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed.

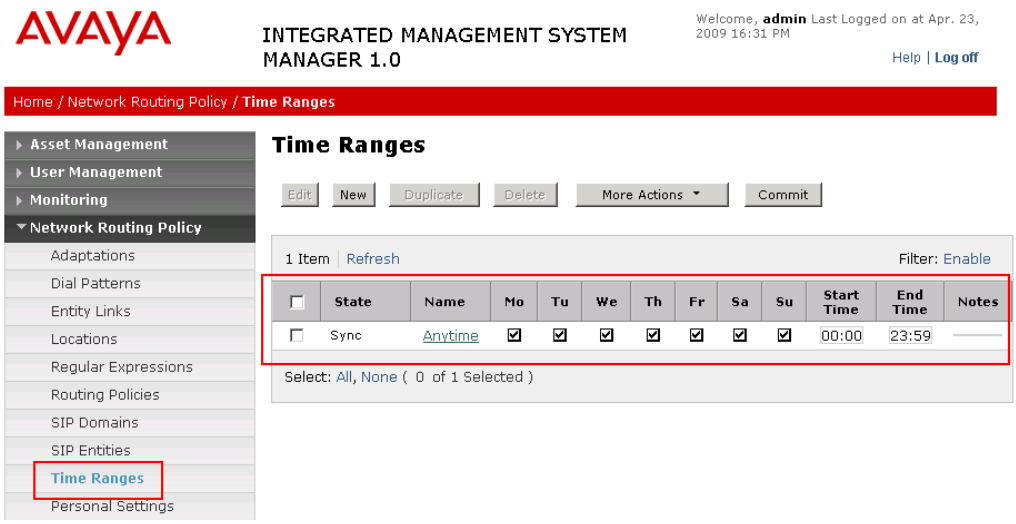
Name	An informative name
SIP Entity 1	Select SM1
Port	Port number to which the other system sends its SIP requests
SIP Entity 2	The other SIP Entity for this link, created in **Step 5**
Port	Port number to which the other system expects to receive SIP requests
Trusted	Whether to trust the other system
Protocol	Transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in the sample network.



7. Before adding routing policies (see next step), time ranges must be defined during which the policies will be active. In the sample network, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges** from the left panel menu and then click New on the right. Fill in the following fields.

Name	An informative name (e.g. "Anytime")
Mo through Su	Check the box under each day of the week for inclusion
Start Time	Enter start time (e.g. "00:00" for start of day)
End Time	Enter end time (e.g. "23:59" for end of day)



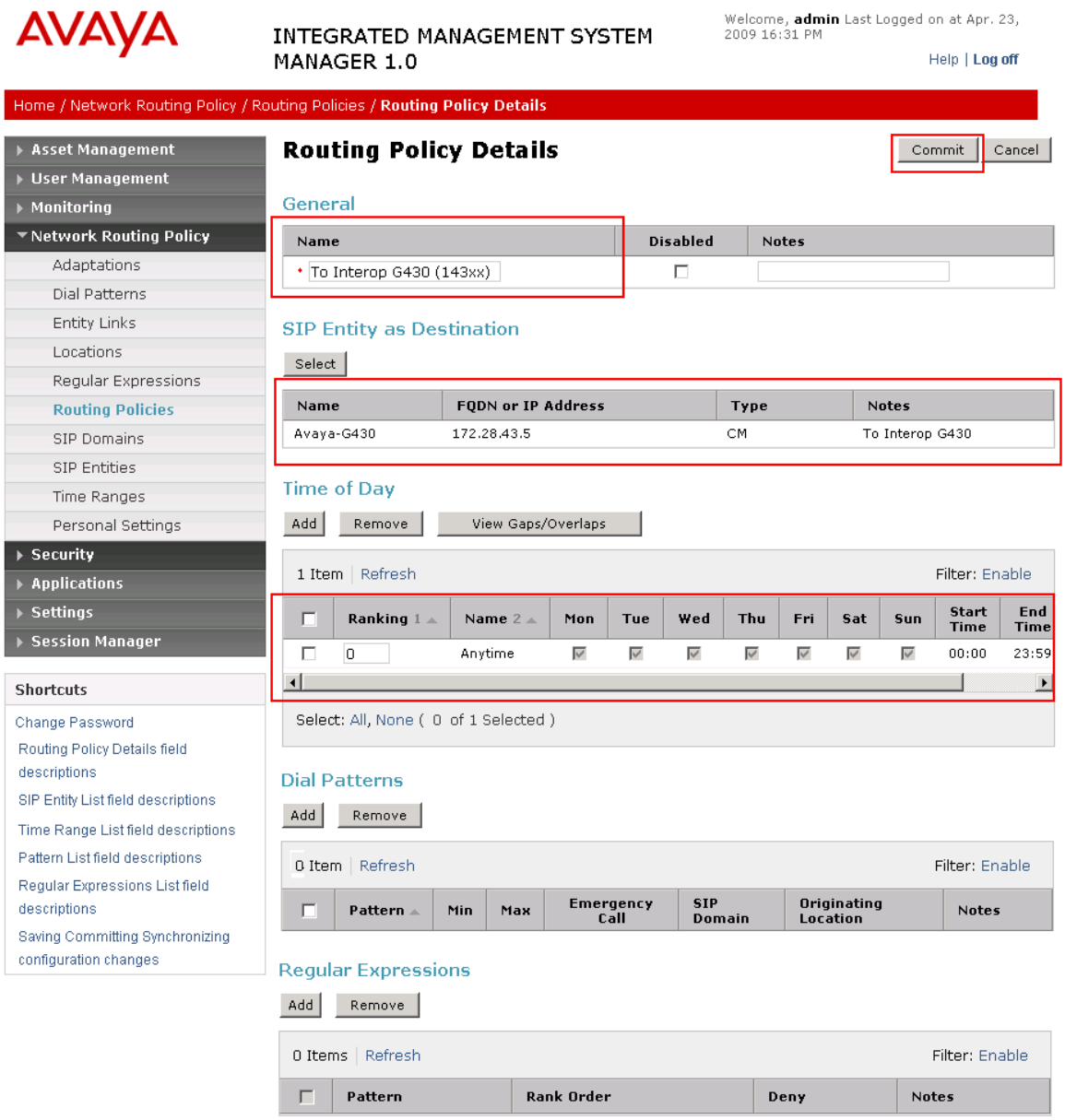
8. Create routing policies to direct how calls will be routed to a system. Two routing policies must be added; one for Avaya Aura™ Communication Manager and one for Cisco UCM. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown) on the right.

   Under General
   Enter an informative name

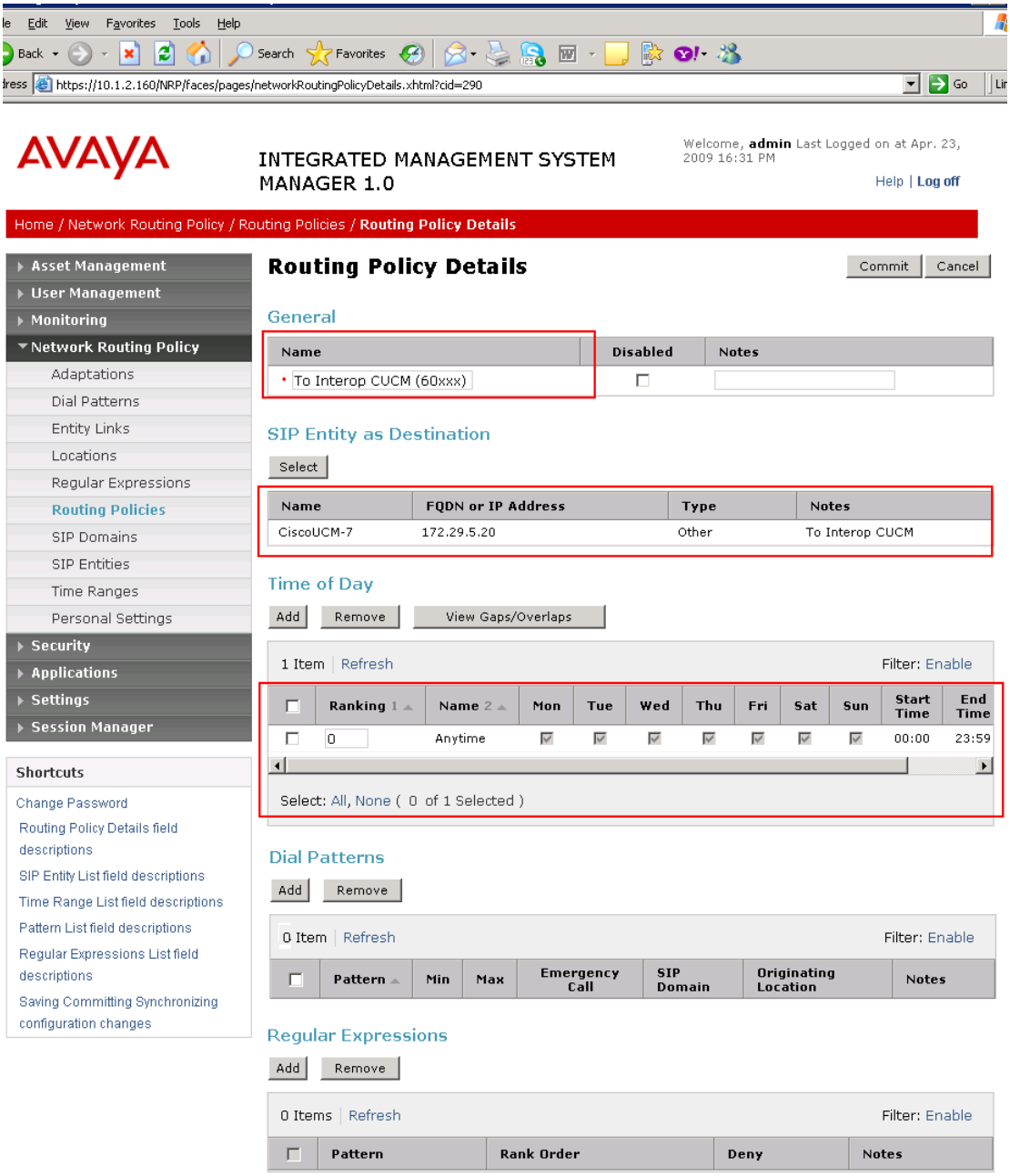
   Under SIP Entity as Destination
   Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

   Under Time of Day
   Click **Add**, and then select the time range configured in the previous step.

The following is screen shows the Routing Policy for Avaya Aura™ Communication Manager.



The following is screen shows the Routing Policy for Cisco UCM.

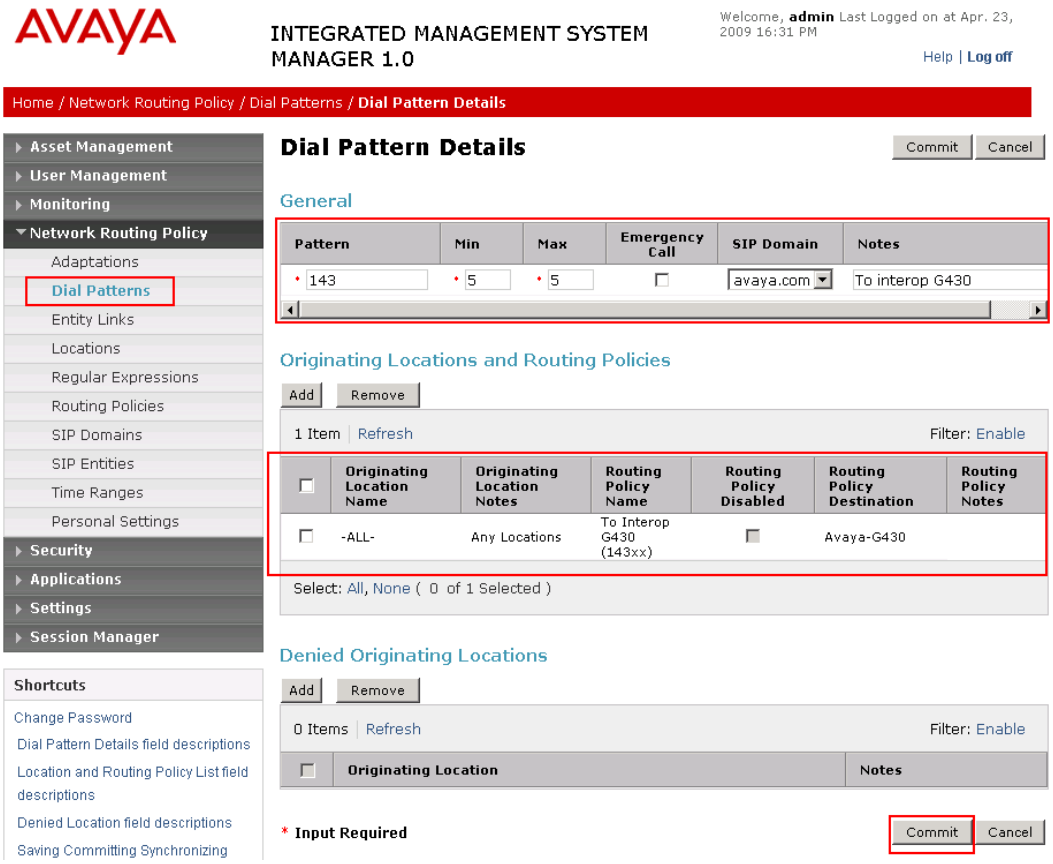


9. A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, 5-digit extension beginning with “143” reside on Avaya Aura™ Communication Manager, and 5-digit extension beginning with “60” reside on Cisco UCM. To add a dial pattern, select Dial Patterns on the left panel menu, and then click on the **New** button on the right (not shown).

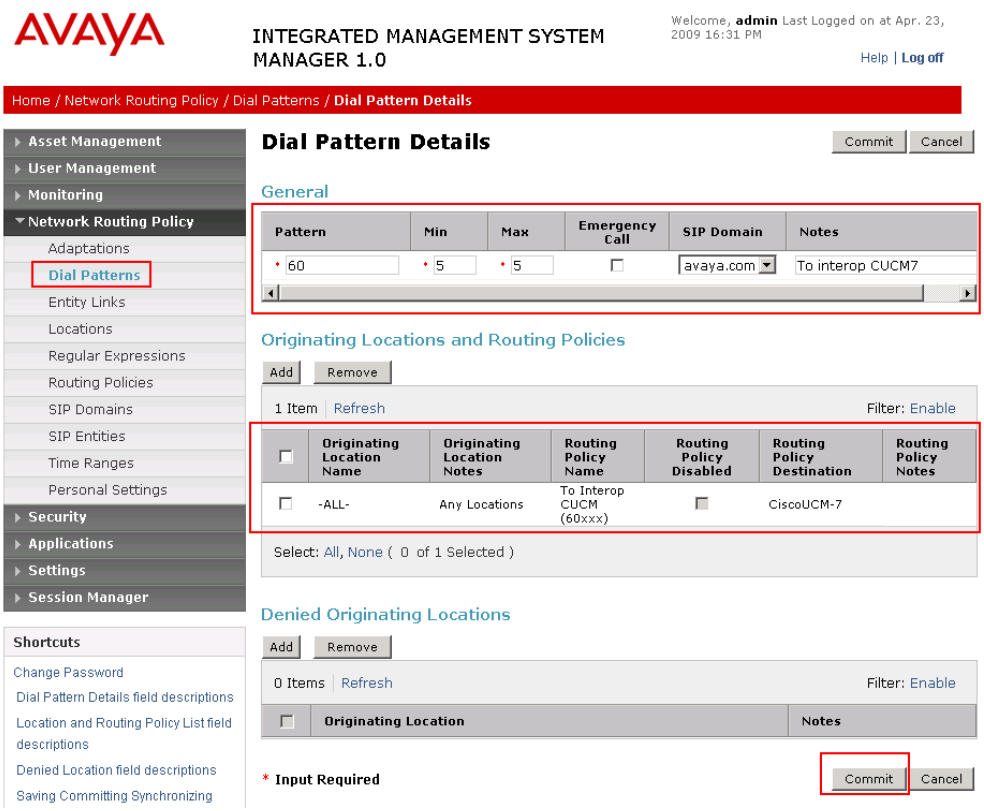
   Under General

Pattern	Dialed number or prefix
Min	Minimum length of dialed number
Max	Maximum length of dialed number
Notes	Comment on purpose of dial pattern

   The following screen shows the dial pattern to Avaya Aura™ Communication Manager.



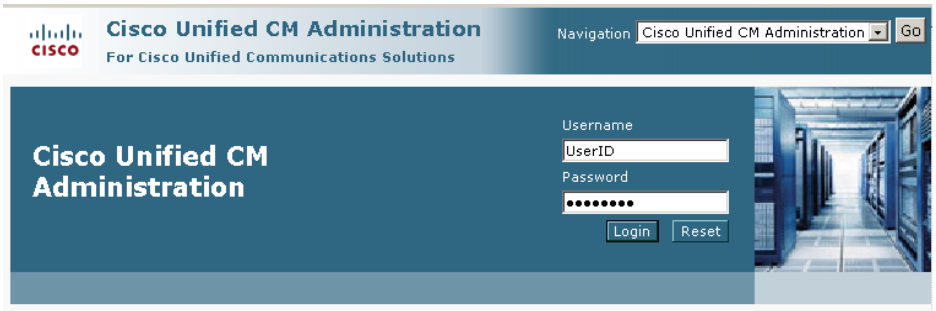
The following screen shows the dial pattern to Cisco UCM.



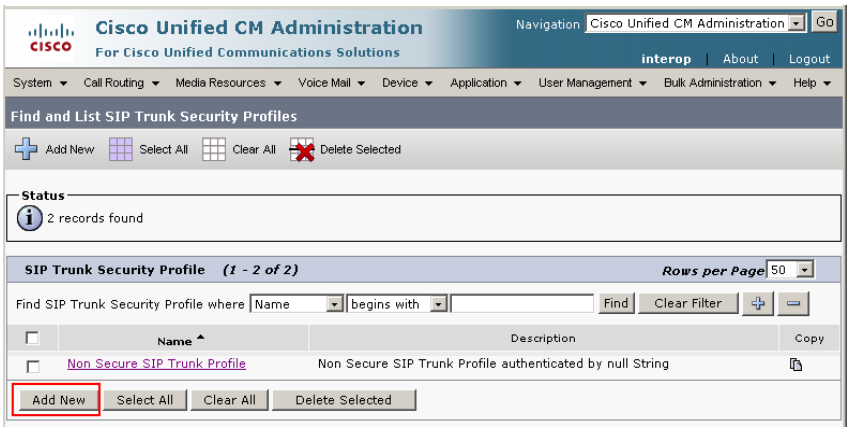
7. Configure Cisco UCM

This section provides the procedures for configuring Cisco UCM. The procedures include configuration of the following items. These Application Notes assumed that the basic configuration needed to support Cisco IP telephones has been completed. For further information on Cisco UCM, please consult references [6] and [7].

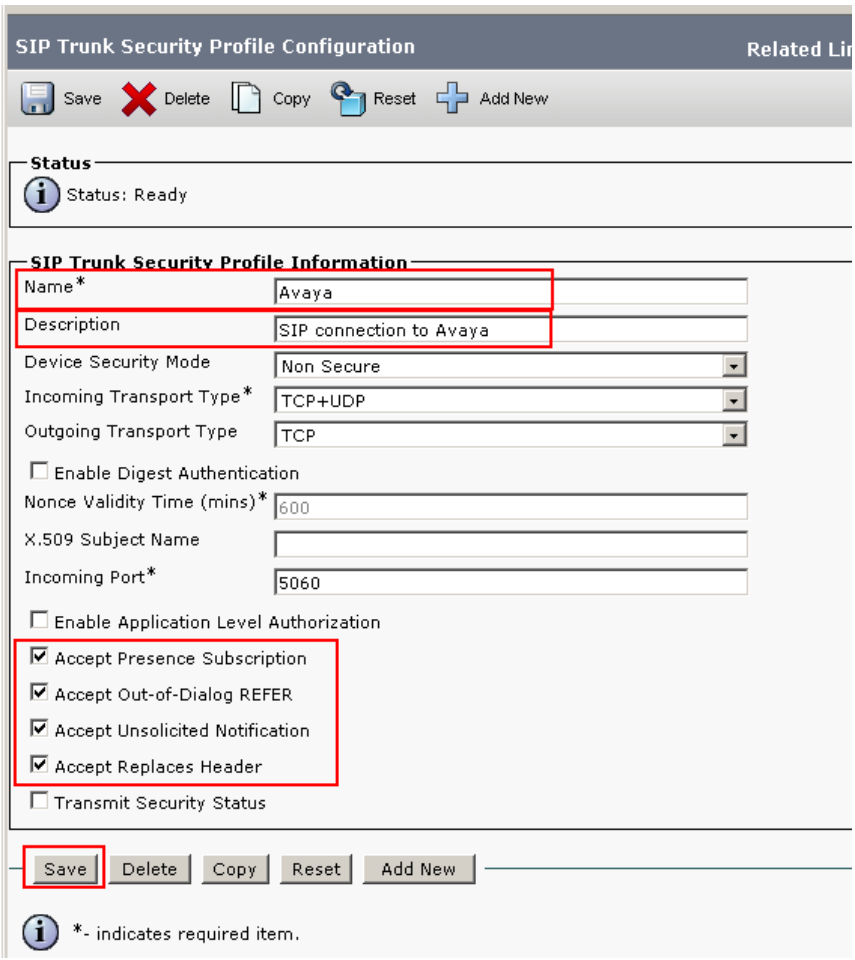
1. Open Cisco Unified CM Administration by entering the IP address of the CUCM into the Web Browser address field, and log in using an appropriate Username and Password.



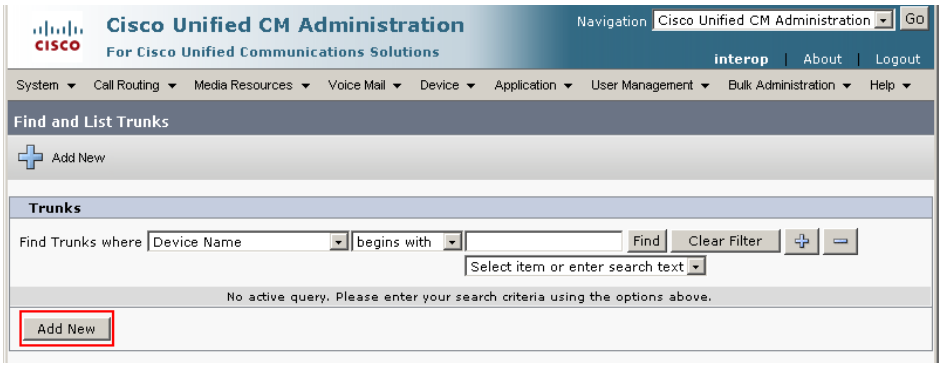
2. Select **System → Security Profile → SIP Trunk Security Profile** from the top menu then click **Add New** to add a new SIP Trunk Security Profile.



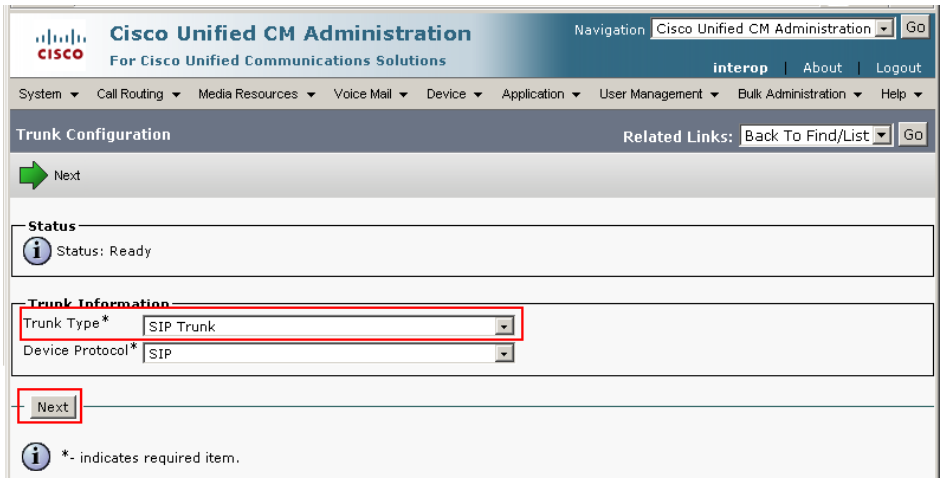
The following is a screen capture of the SIP Trunk Security Profile used in the sample network. Configure the highlighted areas and click **Save** to commit the changes.



3. Add a new SIP trunk by selecting **Device → Trunk** from the top menu then click **Add New** to begin adding a new SIP trunk.

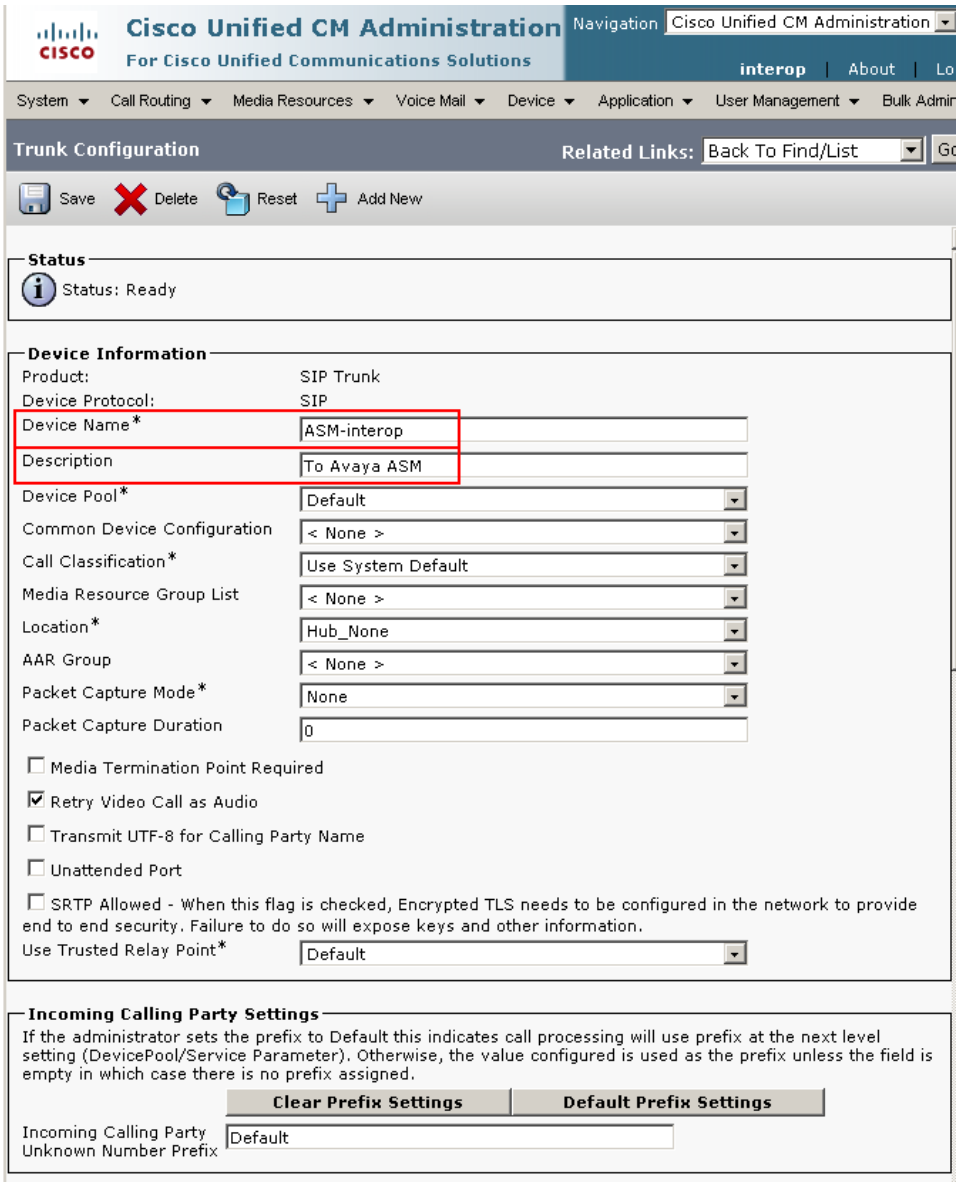


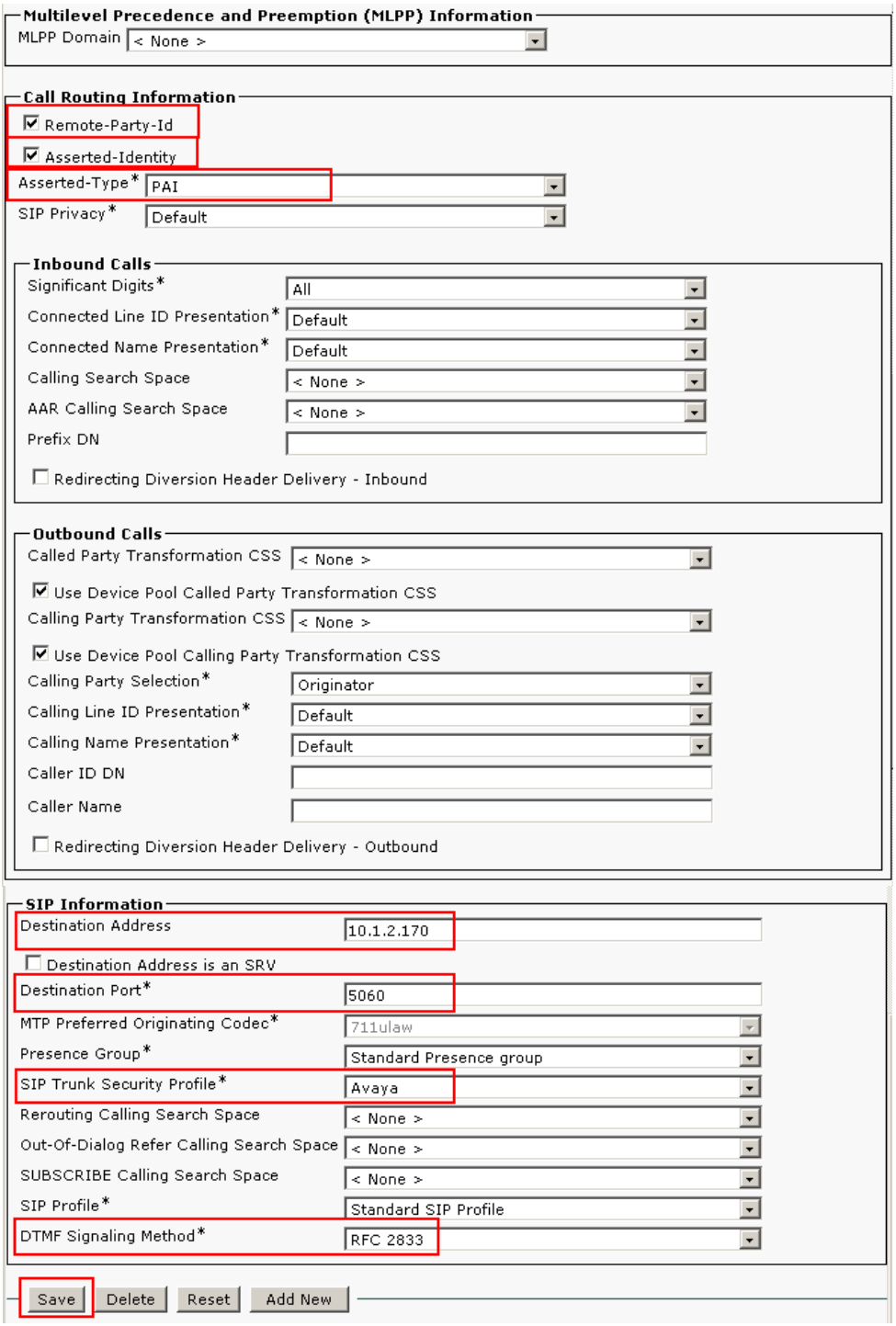
Select **SIP Trunk** as the **Trunk Type** and the **Device Protocol** field will automatically be change to SIP. Click **Next** to continue.



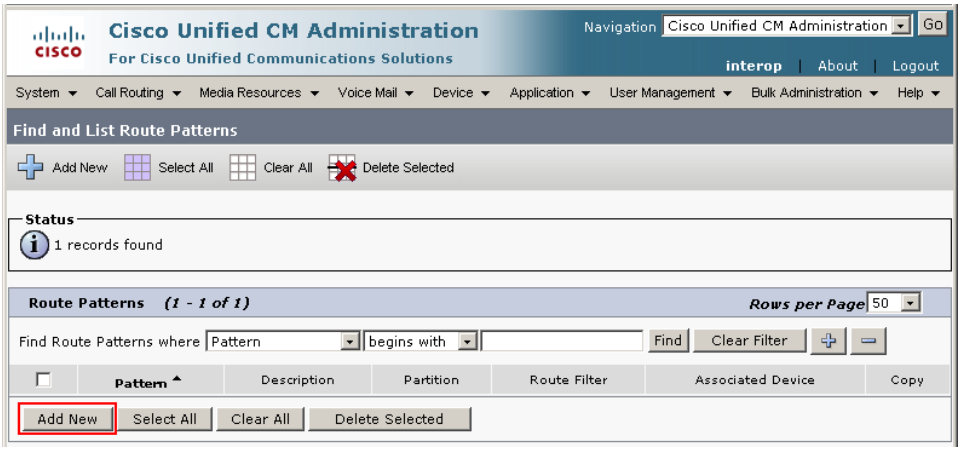
Enter the appropriate information for the SIP Trunk. The following screen shows the configuration used in the sample network. Click **Save** to complete.

Device Name	An informative name
Description	Any note for this trunk
Remote-Party-Id	checked to send
Asserted-Identity	Checked to send caller information
Asserted-Type	Select "**PAI**" for P-Asserted-Identity
Destination Address	IP address of Avaya Aura™ Session Manager
Destination Port	Destination port number use for SIP communication
SIP Trunk Sec. Profile	Profile configured at **Step 2**
DTMF Signaling Method	Select "RFC 2833"

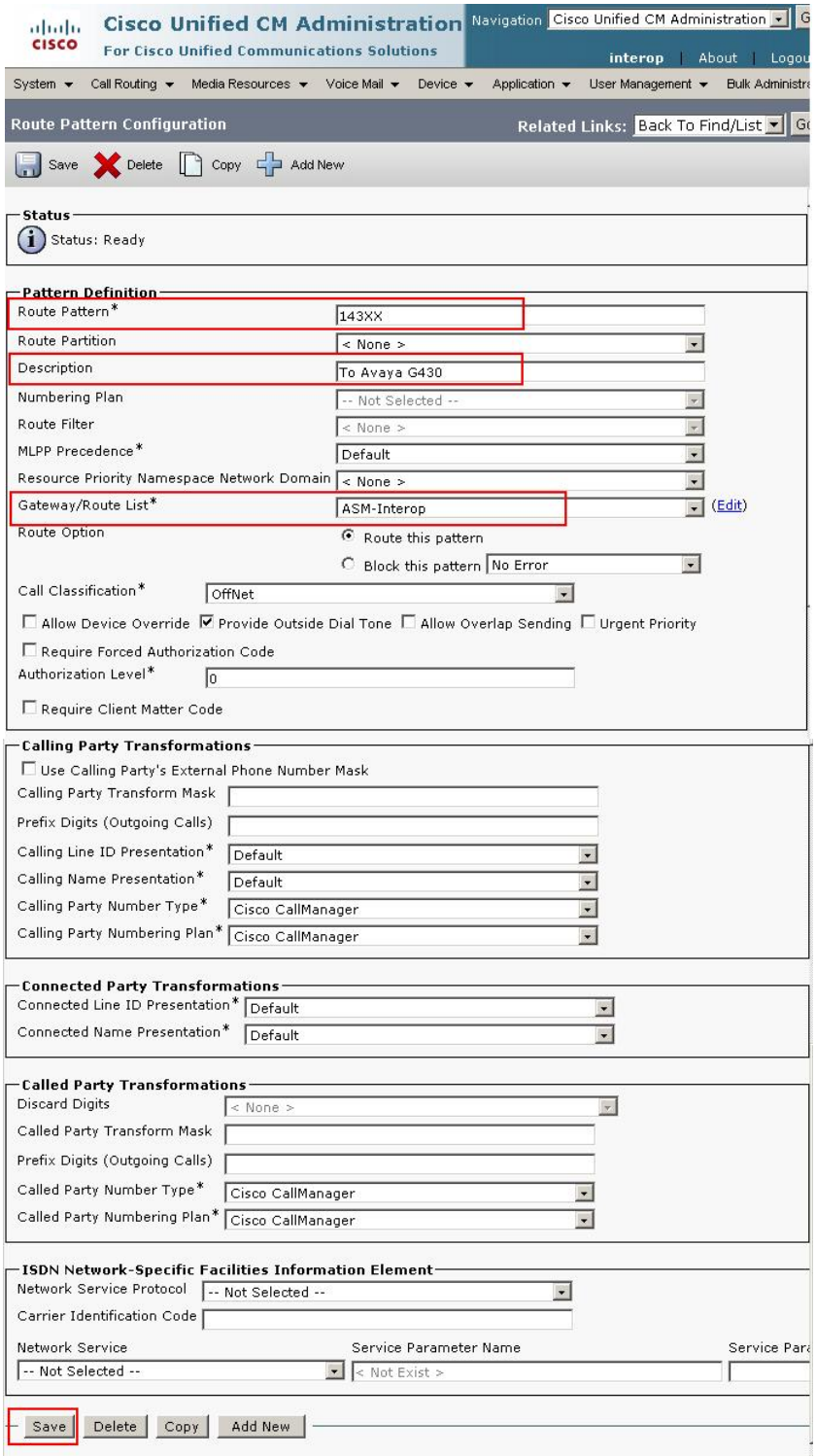




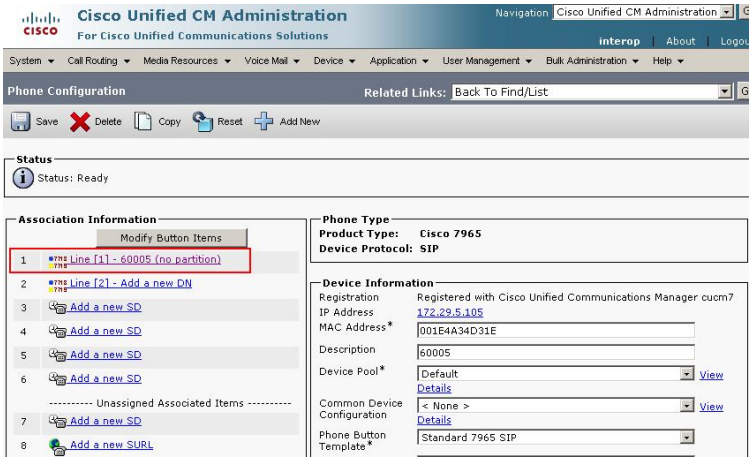
4. Select **Call Routing → Route/Hunt → Route Pattern** then click **Add New** to add a new route pattern for extension 143xx which are for telephones registered with Avaya Aura™ Communication Manager.



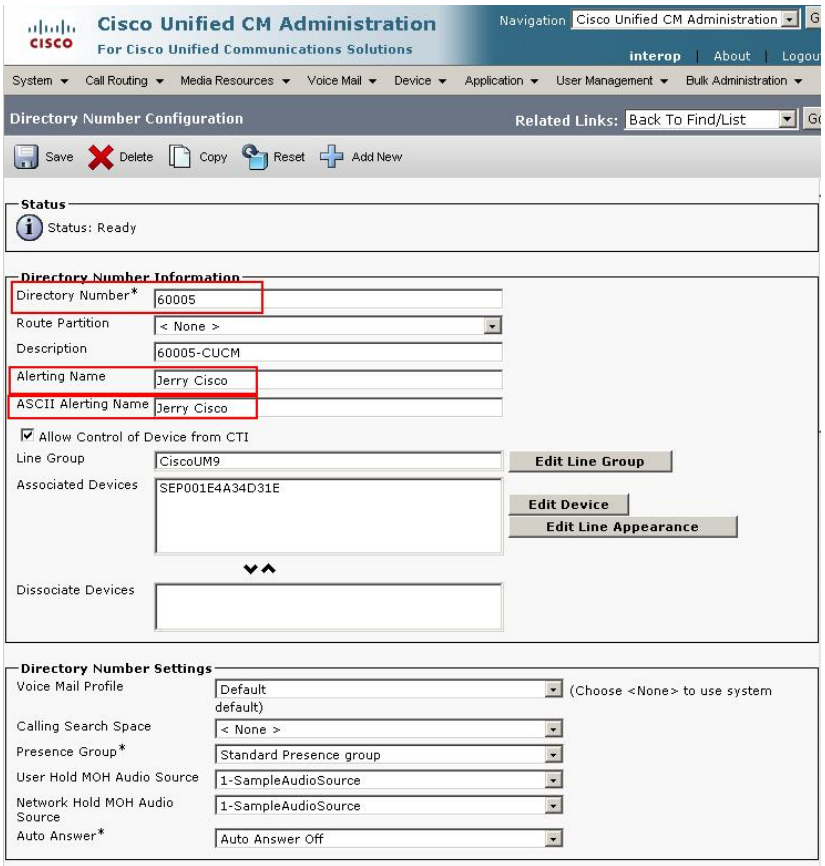
The following screen shows the route pattern used in the sample network. The route pattern "143xx" will cause all 5 digit calls beginning with "143" to be routed through the "ASM-Interop" SIP Trunk defined in **Step 3**. Click **Save** to complete.

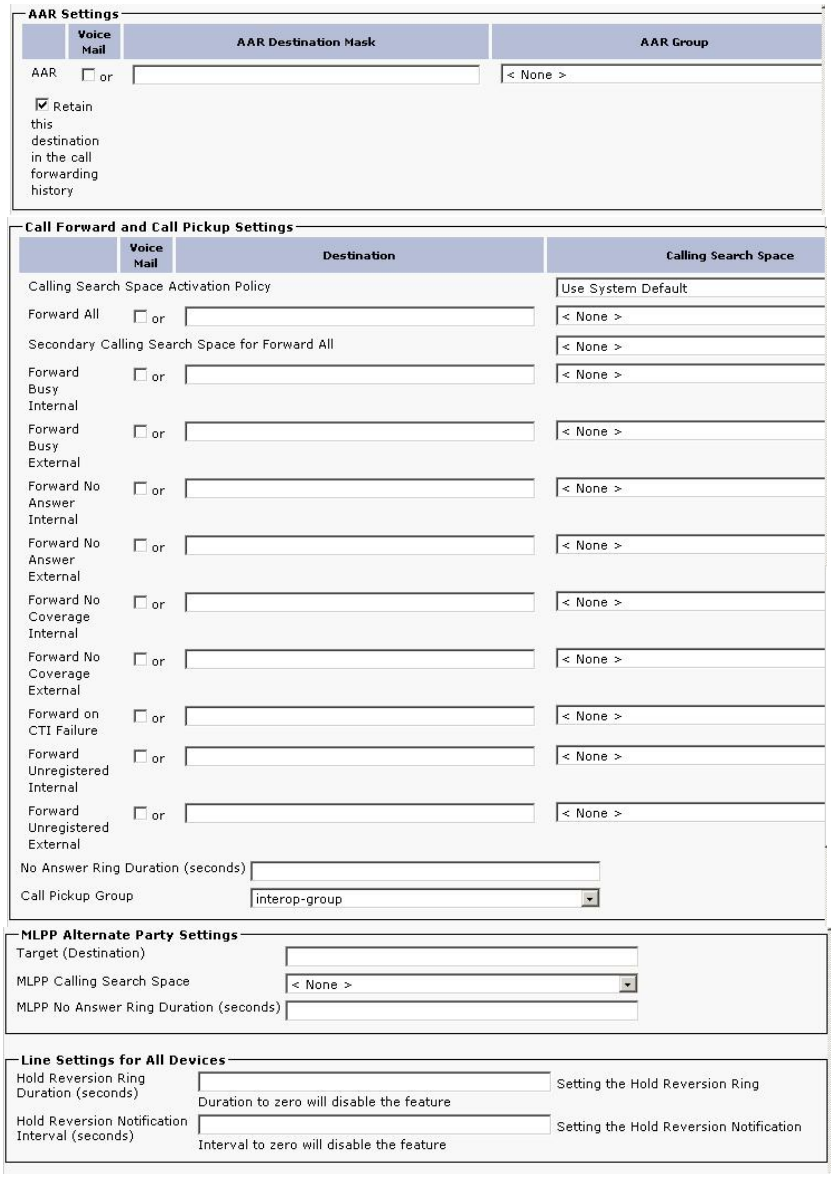


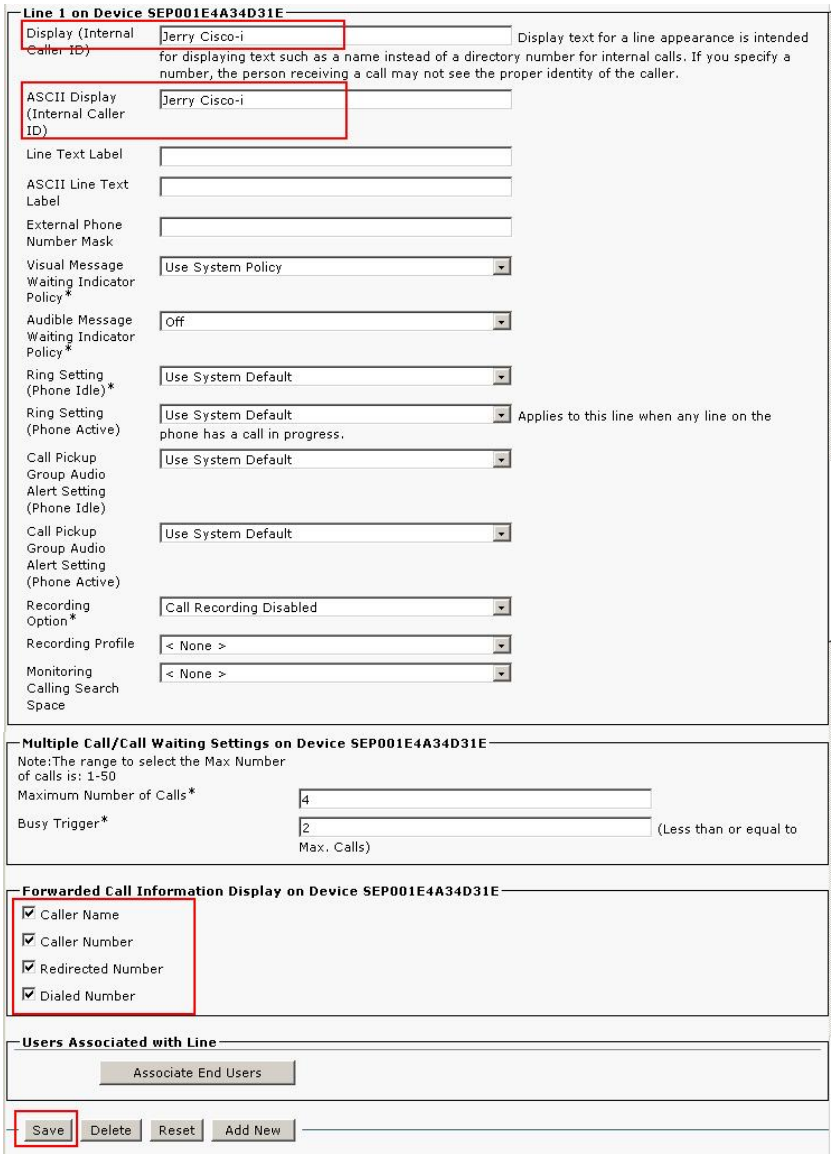
5. Select **Device → Phone** then click on the Device that needs to be administered. The following screen shows the display after a device has been selected. Click on the line for the device as highlighted in the screen below



The following screen shows the display after the line has been selected.
Note: The **Display (Internal Caller ID)** and **ASCII Display (Internal Caller ID)** will be display on called party phone on all outgoing calls. Click **Save** to complete.







8. Verification

This section provides the tests that can be performed on Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, and Cisco UCM to verify proper their proper configuration.

8.1. Verify Avaya Aura™ Communication Manager

1. Verify the status of the SIP trunk group by using the "status trunk n" command, where "n" is the trunk group number being investigated. Verify that all trunks are in the "in-service/idle" state as shown below.

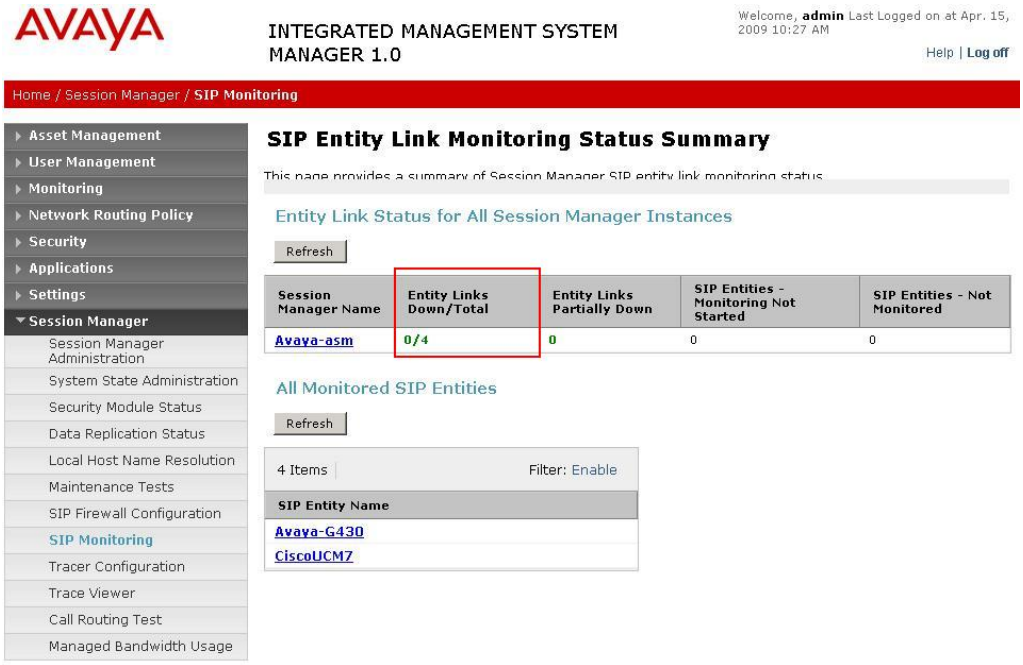
```
status trunk 25

                            TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0025/001 T00007   in-service/idle    no
0025/002 T00008   in-service/idle    no
0025/003 T00009   in-service/idle    no
0025/004 T00010   in-service/idle    no
0025/005 T00011   in-service/idle    no
0025/006 T00012   in-service/idle    no
0025/007 T00013   in-service/idle    no
0025/008 T00014   in-service/idle    no
0025/009 T00015   in-service/idle    no
0025/010 T00016   in-service/idle    no
```

2. Verify the status of the SIP signaling-group by using the "status signaling-group n" command, where "n" is the signaling group number being investigated. Verify that the signaling group is in the "in-service" state as shown below.

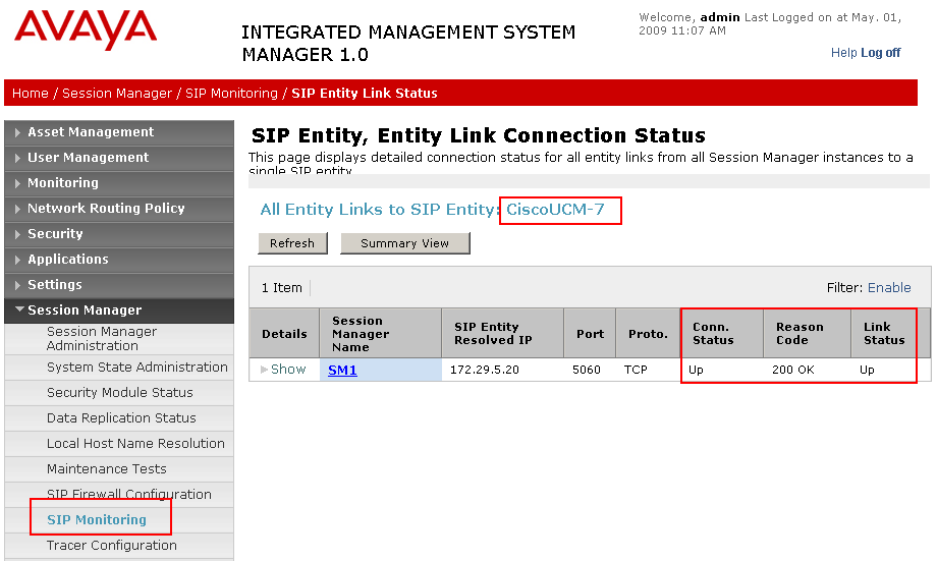
```
status signaling-group 25
                         STATUS SIGNALING GROUP

       Group ID: 25                              Active NCA-TSC Count: 0
     Group Type: sip                              Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
    Group State: in-service
```

8.2. Verify Avaya Aura™ Session Manager

1. Expand the **Avaya Aura™ Session Manager** field on the left panel menu and click on **SIP Monitoring**. Verify as shown below that none of the links for SIP entities are down, indicating that they are all reachable for routing.

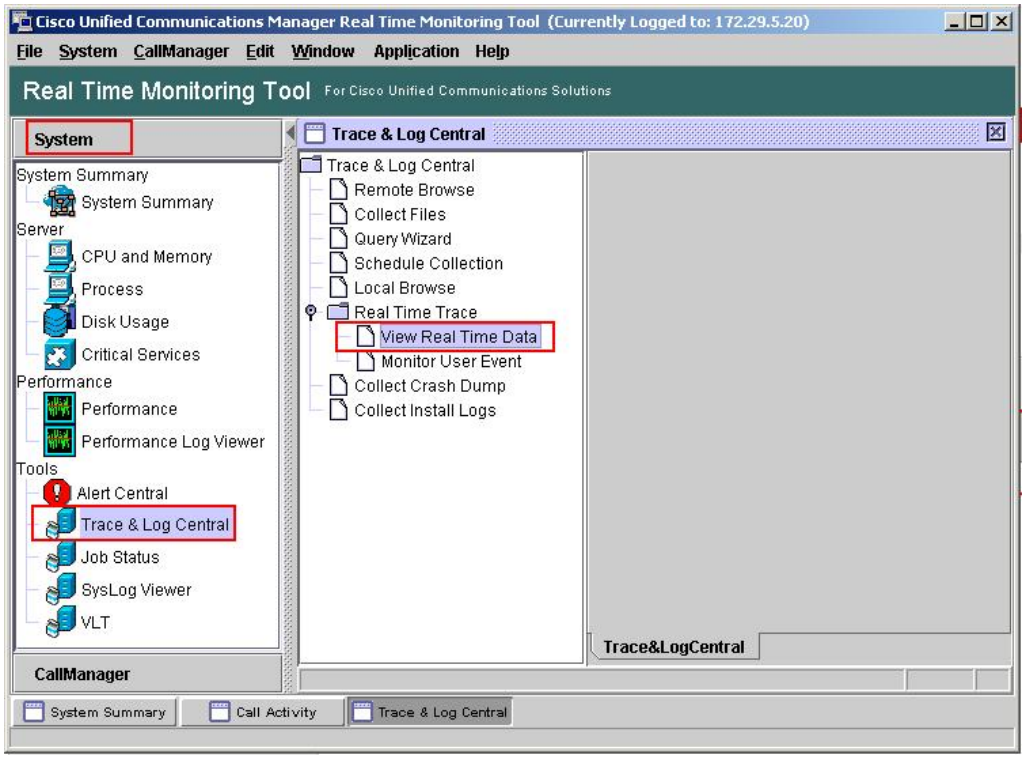


2. Select the SIP Entity Name entities, shown in the previous screen, and verify that the connection status is "Up", as shown below for CiscoUCM7.



8.3. Verify Cisco Unified Communications Manager

1. The Real Time Monitoring Tool (RTMT) can be use to monitor events on Cisco Unified CM. This tool can be downloaded by selecting **Application → Plugins** from the top menu of the Cisco Unified CM Administration Web interface. For further information on this tool, please consult with reference [8]. The following screen shows where user can view and perform real time data capture.



8.4. Verified Scenarios

The following scenarios have been verified for the configuration described in these Application Notes.

- Basic calls between various telephones on Avaya Aura™ Communication Manager and Cisco Unified Communications Manager can be made in both directions using G.711MU, G.729, and G.729AB. For G.729 interoperability, the IP codec set on Avaya Aura™ Communication Manager must include a version of the G.729 that Cisco UCM supports.

- Proper display of the calling and called party name and number information was verified for all telephones with the basic call scenario.

- Supplementary calling features were verified. The feature scenarios involved additional endpoints on the respective systems, such as performing an unattended transfer of the SIP trunk call to a local endpoint on the same site, and then repeating the scenario to transfer the SIP trunk call to a remote endpoint on the other site. The supplementary calling features verified were shown below. Note that calling/called party name and number display may not be consistent in some cases.

    - Unattended transfer
    - Attended transfer
    - Hold/Unhold
    - Consultation hold
    - Call forwarding
    - Conference

9. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager can interoperate with Cisco Unified Communications Manager using SIP trunks via Avaya Aura™ Session Manager. The following is a list of interoperability items to note:

- For G.729 interoperability, make sure both G.729 and G729AB are part of the audio codec selection in Avaya Aura™ Communication Manager.
- For proper displaying of calling party information, Cisco UCM must be configured with the Internal Caller ID name as described in Section 7, Step 5.
- With direct media "shuffling" enabled, a "one-way" audio issue was observed when a call initiated by a Cisco SIP Telephone to an Avaya IP telephone was put on hold and then released on the Cisco SIP telephone side. When the Cisco SIP telephone released the hold, the Cisco SIP telephone sent media traffic to the Avaya G430 Media Gateway instead of directly to the Avaya IP telephone as instructed by Avaya Aura™ Communication Manager in the SDP portion of the final ACK message. The workaround is to disable direct media between the Cisco SIP telephones and Avaya IP telephones. This issue does not exist if the call is initiated from Avaya or if the Hold/Release is done from an Avaya IP Telephone. In addition, it is worth noting that this issue does not exist between Avaya IP telephones and Cisco IP telephones (SCCP).

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 # 03-300509May 2009

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

[6] *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*, Release 7.0(1), Part Number: OL-15405-01
[7] *Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communication Manager Business Edition*, Release 7.0(1), Part Number: OL-15409-01
[8] *Cisco Unified Real-Time Monitoring Tool Administration Guide*, Release 7.0(1), Part Number: OL-14994-01

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