Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks among Cisco Unified Communications Manager, Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager 5.2 as an Access Element – 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 as an Access Element and Cisco Unified Communications Manager using SIP trunks.

The results in these Application Notes should be applicable to other Avaya Servers and Media Gateways that support Avaya Aura™ Communication Manager.

Testing was conducted via the Interoperability Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager as an Access Element and Cisco Unified Communications Manager (Cisco UCM) using SIP trunks.

2. Overview

The sample network is shown in **Figure 1**. Communication Manager supports the Avaya 9620 IP Telephone (H.323) and Avaya 2420 Digital Telephone. The Cisco UCM supports the Cisco 7911G IP Telephone (SIP) and the Cisco 7911G IP Telephone (SCCP). SIP trunks are used to connect these two systems to Session Manager. All inter-system calls are carried over these SIP trunks. 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 Session Manager is managed by a separate Avaya Aura™ System Manager, which can manage multiple Session Managers.

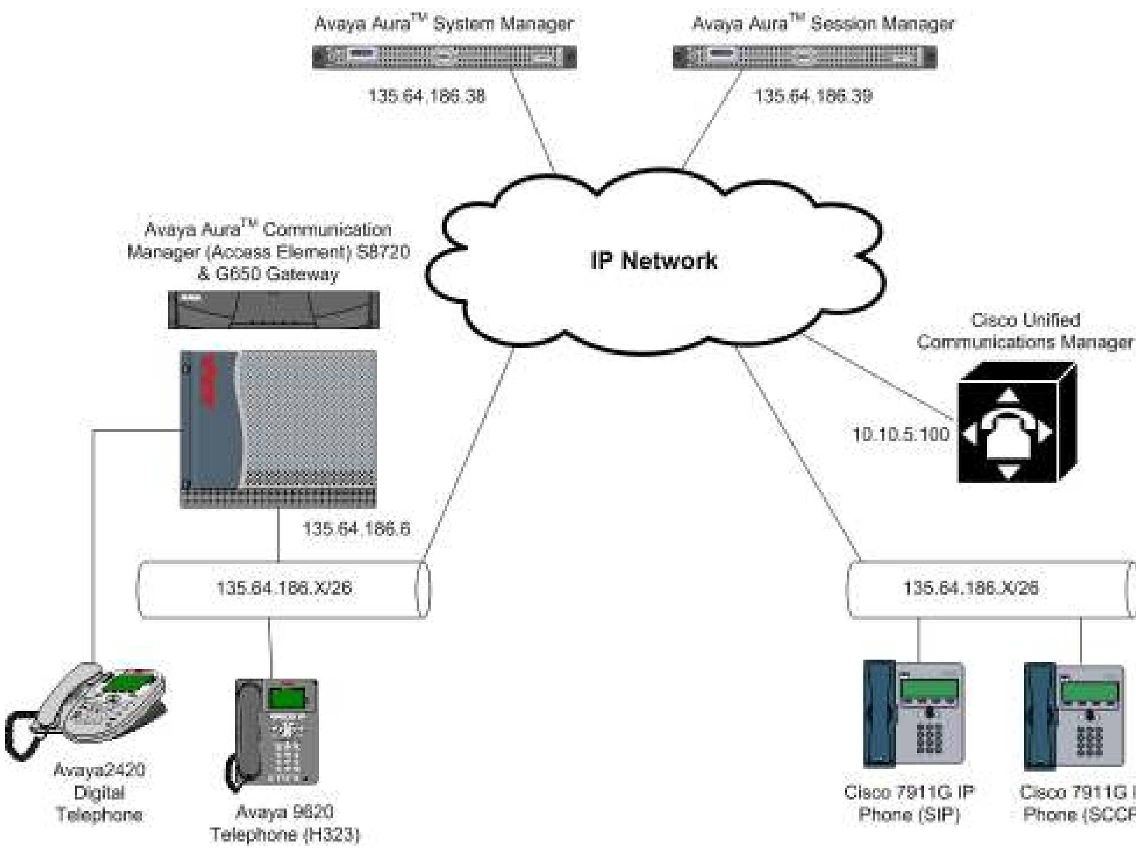


Figure 1: Connection of CM and CUCM via Session Manager using SIP Trunks

All telephones in the 135.64.186.x/26 IP network are either registered with Communication Manager or Cisco Unified Communication Manager. Avaya phones are registered to Avaya Aura™ Communication Manager and Cisco phones to Cisco UCM. Avaya Digital and H.323 stations use extensions 300xx. Cisco UCM registered stations use extensions 3500x. Two separate SIP trunks are provisioned to the Session Manager to manage call control for calls between the two systems – one from Communication Manager and one from Cisco UCM.

3. Equipment and Software Validated

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

Equipment	**Software/Firmware**
Avaya S8720 Media Server	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack • TN2312BP IP Server Interface • TN2602AP IP Media Pro • TN2224CP Digital Line	 HW01 FW034 HW15 FW047 HW08 FW049 HW08 FW015
Avaya S8510 Server with SM100 Card	Avaya Aura™ Session Manager 5.2
Avaya S8510 Server	Avaya Aura™ System Manager 5.2
Avaya 9620 IP Telephone (H.323)	3.002
Avaya 2420 Digital Telephone	-
Cisco Unified Communications Manager	7.0.2.10000-18
Cisco 7911G SIP Telephone	SIP11.8-4-3S
Cisco 7911G SCCP Telephone	SCCP11.8-4-3S

4. Configure Avaya Aura™ Communication Manager

This section shows the configuration of 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 Communication Manager, please consult with references **[4]** and **[5]**. The procedures include the following areas:

- Verify Communication Manager license
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec Set
- Administer SIP Signaling Group and Trunk Group
- Administer Route Pattern
- Administer Public Unknown Numbering
- Administer Dial Plan and AAR Analysis
- Save Changes

4.1. Verify Communication Manager License

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  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 30     0
           Maximum Concurrently Registered IP Stations: 18000  9
             Maximum Administered Remote Office Trunks: 0      0
Maximum Concurrently Registered Remote Office Stations: 0      0
              Maximum Concurrently Registered IP eCons: 0      0
  Max Concur Registered Unauthenticated H.323 Stations: 0      0
                        Maximum Video Capable Stations: 10     1
                   Maximum Video Capable IP Softphones: 10     4
                       Maximum Administered SIP Trunks: 100    55
```

4.2. Administer System Parameters Features

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? y
                                    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: none
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n
```

4.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for the Communication Manager and Session Manager that will be used for connectivity. In the sample network, **clan1a3** and **135.64.186.6** are entered as **name** and **IP Address** for the CLAN card in Communication Manager running on the Avaya S8720 Server. In addition, **SM100** and **135.64.186.40** are entered for Session Manager.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
Gateway001          135.64.186.1
MBTCM               135.64.186.68
MX6200              135.64.186.15
SM100               135.64.186.40
clan1a3             135.64.186.6
clan1b3             135.64.186.7
default             0.0.0.0
mpro1a2             135.64.186.8
mpro1b2             135.64.186.9
onexmobile          135.64.186.30
procr               135.64.186.10
silstackaes         135.64.186.28
```

4.4. Administer IP Network Region and Codec Set

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 3 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 3 to use ip-codec-set 3.

```
change ip-network-region 3                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 3
Location:           Authoritative Domain: silstack.com
    Name: To ASM
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 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
```

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 3                                          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
```

4.5. Administer SIP Signaling Group and Trunk Group

4.5.1. SIP Signaling Group

In the test configuration, signal group 140 along with trunk group 145 were used to reach Session Manager. Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system. Use the values defined in **Section 4.3** and **4.4** for **Near-end Node Name**, **Far-End Node-Name** and **Far-End Network Region**. The **Far-end Domain** is left blank so that the signaling group accepts any authoritative domain.

```
add signaling-group 140                                          Page   1 of   2

                                   SIGNALING GROUP

 Group Number: 140             Group Type: sip
                         Transport Method: tcp
  IMS Enabled? n
     IP Video? n



   Near-end Node Name: clan1a3              Far-end Node Name: SM100
 Near-end Listen Port: 5063               Far-end Listen Port: 5063
                                       Far-end Network Region: 3
Far-end Domain:

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

4.5.2. SIP Trunk Group

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 145.

```
add trunk-group 145                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 145                  Group Type: sip           CDR Reports: y
  Group Name: To Session Manager          COR: 1        TN: 1        TAC: 145
   Direction: two-way       Outgoing Display? y
 Dial Access? n                               Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                   Signaling Group: 140
                                                 Number of Members: 10
```

Navigate to page 3 and enter **public** for **Numbering Format**.

```
add trunk-group 145                                             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
```

Navigate to page 4 and enter **101** for **Telephone Event Payload Type**

```
add trunk-group 145                                             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
```

4.6. Administer Route Pattern

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 **Section 4.8**. Configure this route pattern to route calls to trunk group number **145** configured in **Section 4.5.2.** Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern.

```
change route-pattern 140                                        Page   1 of   3
                    Pattern Number: 140 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: 145  0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    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
```

4.7. Administer Public Unknown Numbering

Use the **change public-unknown-numbering** command to define the calling party number to be sent out through the SIP trunk. Add an entry for the trunk group defined in **Section 4.5**. In the sample network configuration below, all calls originating from a 5-digit extension beginning with 300 and routed to trunk group 145 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  300            145                       5          Maximum Entries: 240
```

4.8. Administer Dial Plan and AAR Analysis

Configure the dial plan for dialing 5-digit extensions beginning with **350** to stations registered with Cisco UCM. Use the **change dialplan analysis** command to define **Dialed String 350** 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
     300          5    ext
     350          5    aar
     8            1    fac
     9            1    fac
     *            3    fac
     #            3    fac
```

Use the **change aar analysis n** command where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 350** to use **Route Pattern 140**

```
change aar analysis 350                                           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
    350                    5    5     140      aar          n
    7                      7    7     254      aar          n
    8                      7    7     254      aar          n
    9                      7    7     254      aar          n
```

4.9. Save Changes

Use the **save translation** command to save all changes.

```
save translation

                               SAVE TRANSLATION

           Command Completion Status                          Error Code

           Success                                            0
```

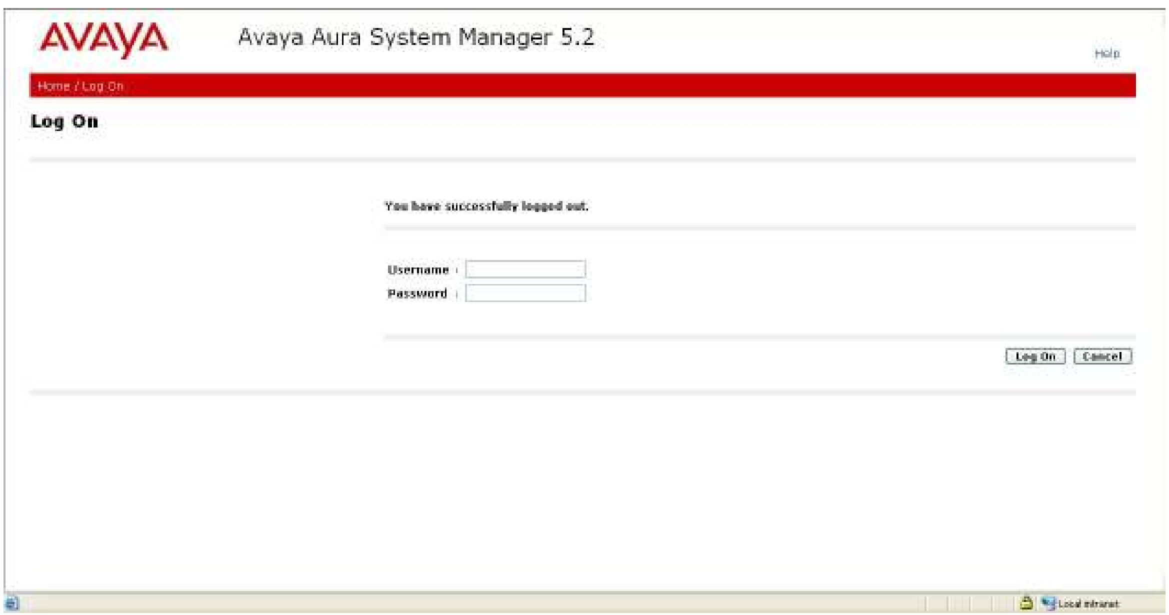
5. Configuring Avaya Aura™ Session Manager

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

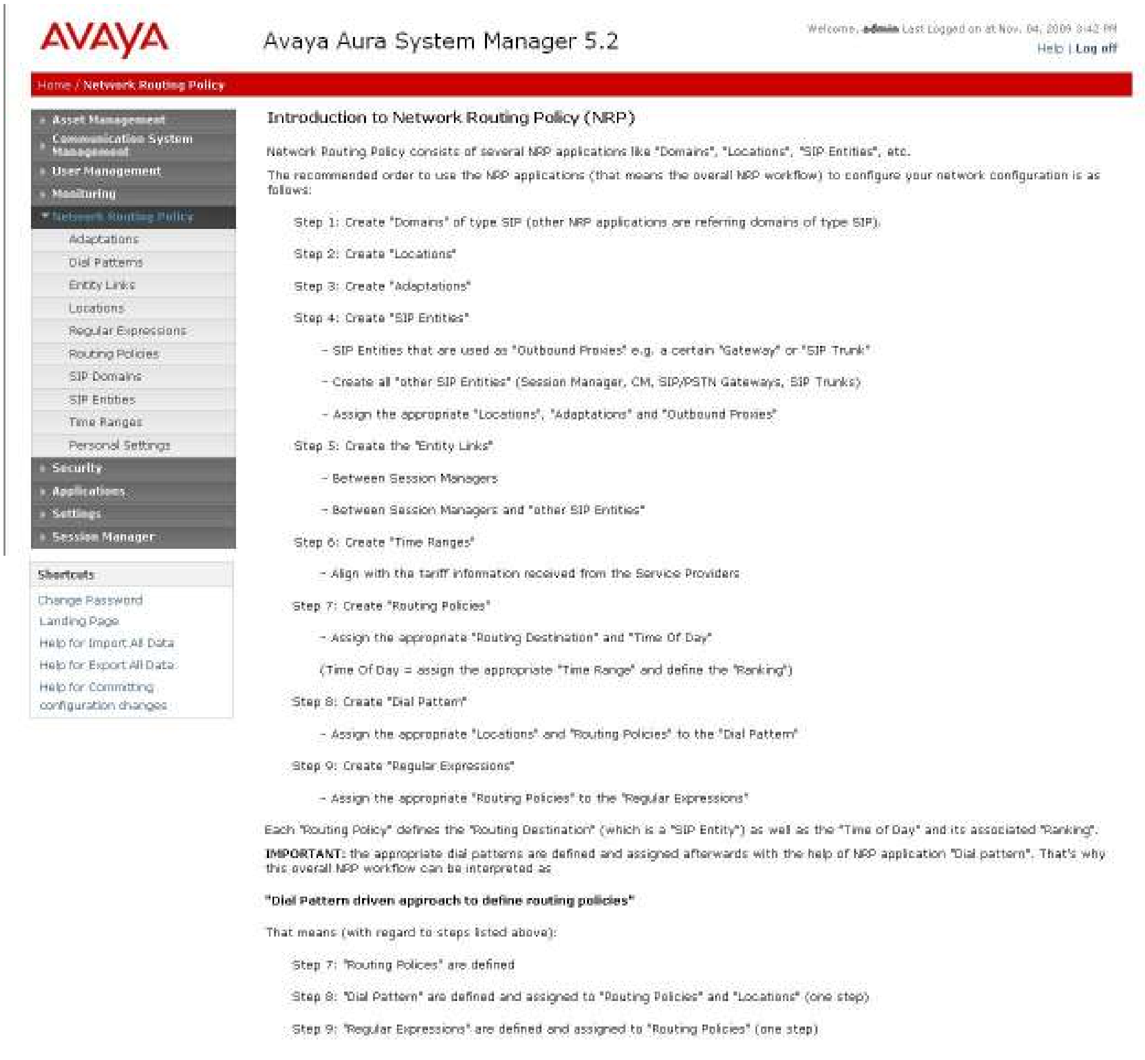
- Login to Session Manager
- Administer SIP domain
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Session Manager

5.1. Login to Session Manager

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



By selecting **Network Routing Policy** from the left panel menu, a short procedure for configuring Network Routing Policy is shown on the right panel.



5.2. Administer SIP Domain

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.

Complete the following options:

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

Click **Commit** to save changes.

Verify the domain is created as in screenshot below.

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

5.3. Administer Adaptations

Create an adaptation entry for an incoming call from Cisco UCM. For the Cisco UCM adaptation, enter the following information:

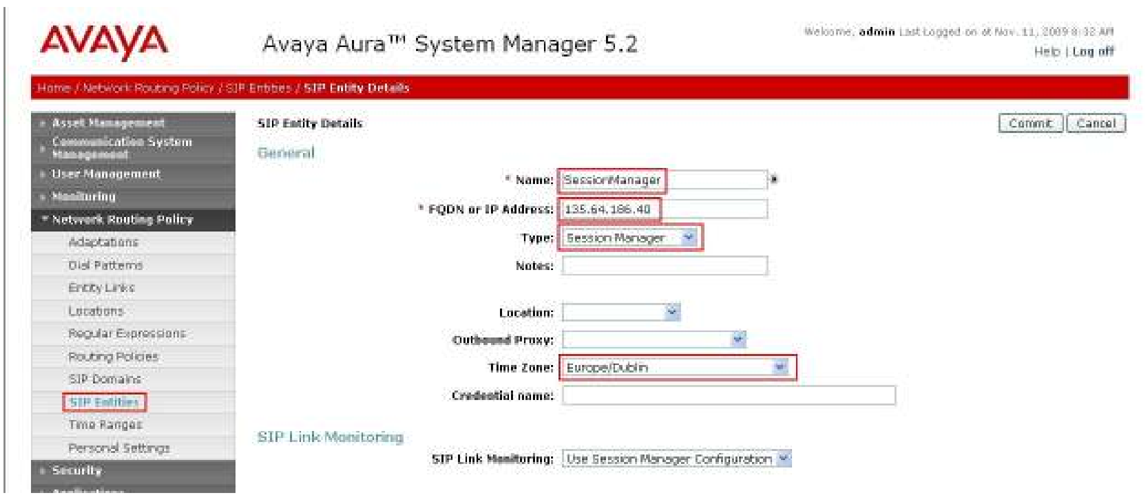
Name	CiscoUCM-7, an informative name for the adaptation
Adaptation Module	Enter **CiscoAdapter 10.10.5.100**, where 10.10.5.100 is the Cisco UCM IP address.
Digit Conversion for incoming Calls to SM	Matching Pattern 350 with a minimum and maximum of 5 digits long, which is the dial pattern for a station registered with Cisco UCM. Delete Digits has value **0** to indicate no digits are to be deleted.

5.4. Administer SIP Entities

A SIP Entity must be added for 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). Enter the following for each SIP Entity:

Under **General:**

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

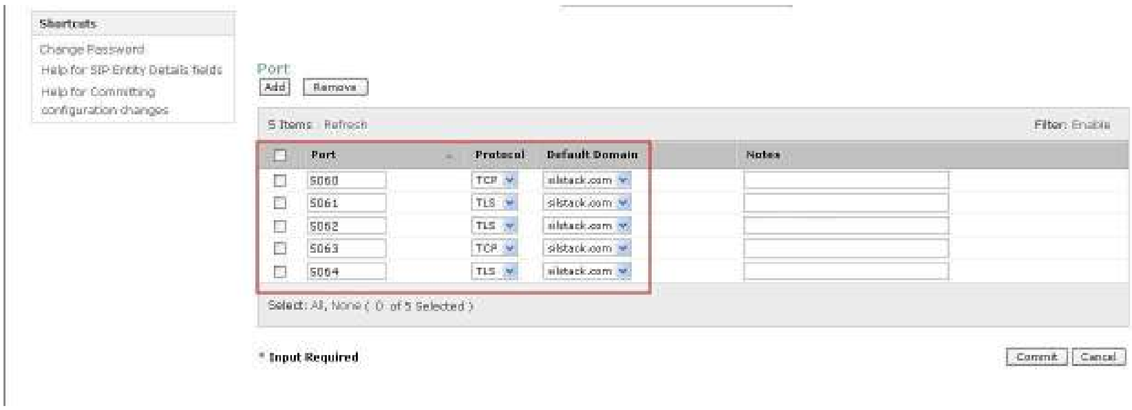


Under **Port**, click **Add,** and then edit the fields in the resulting new row

Port Port number on which the system listens for SIP requests

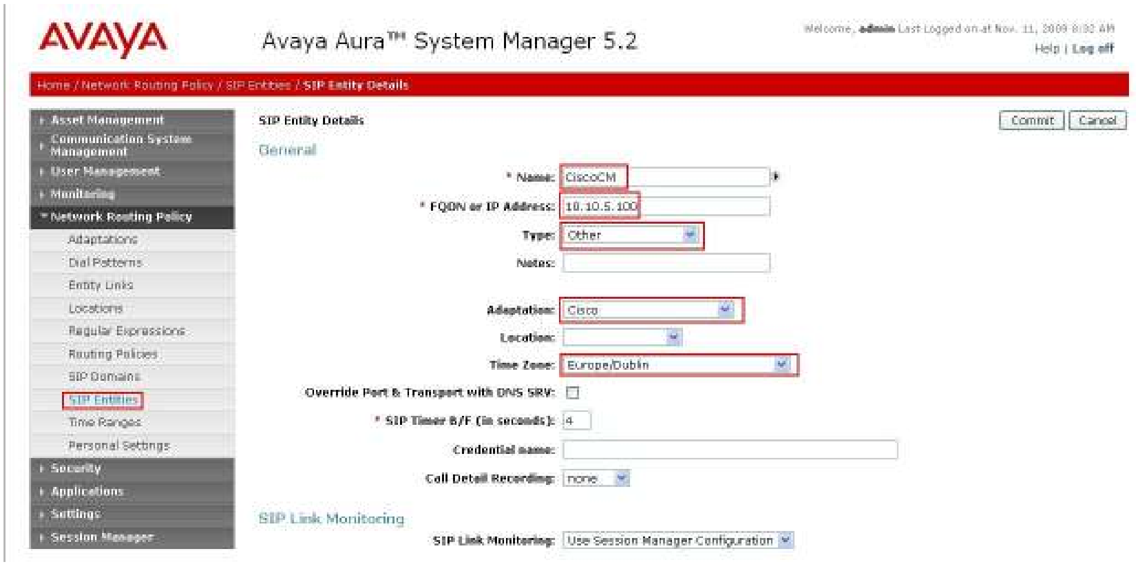
Protocol Transport protocol to be used to send SIP requests

The following screen shows the Port definitions for the Session Manager SIP Entity.



The following screen shows the SIP Entity for Communication Manager.

The following screen shows the SIP Entity for Cisco UCM.

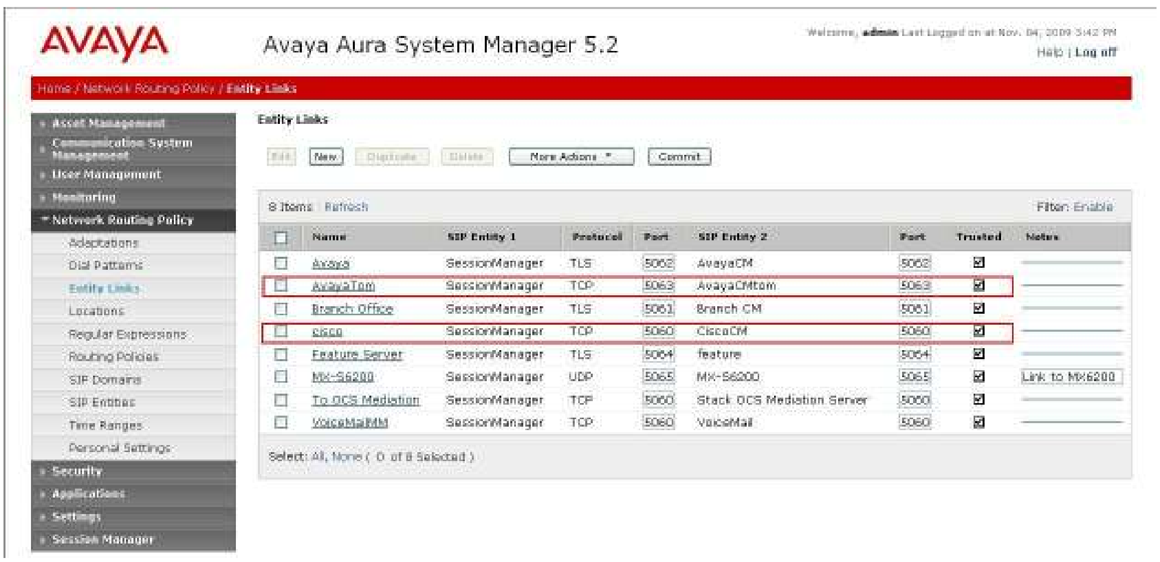


5.5. Administer Entity Links

A SIP trunk between a 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). Fill in the following fields in the new row that is displayed.

Name	An informative name
SIP Entity 1	Select SessionManager
Port	Port number to which the other system sends its SIP requests
SIP Entity 2	The other SIP Entity for this link, created in **Section 5.4**
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.



5.6. Administer Time Ranges

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. **Always**)
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)

5.7. Administer Routing Policies

Create routing policies to direct how calls will be routed to a system. Two routing policies must be added; one for 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).

Under **General**

Enter an informative **Name**

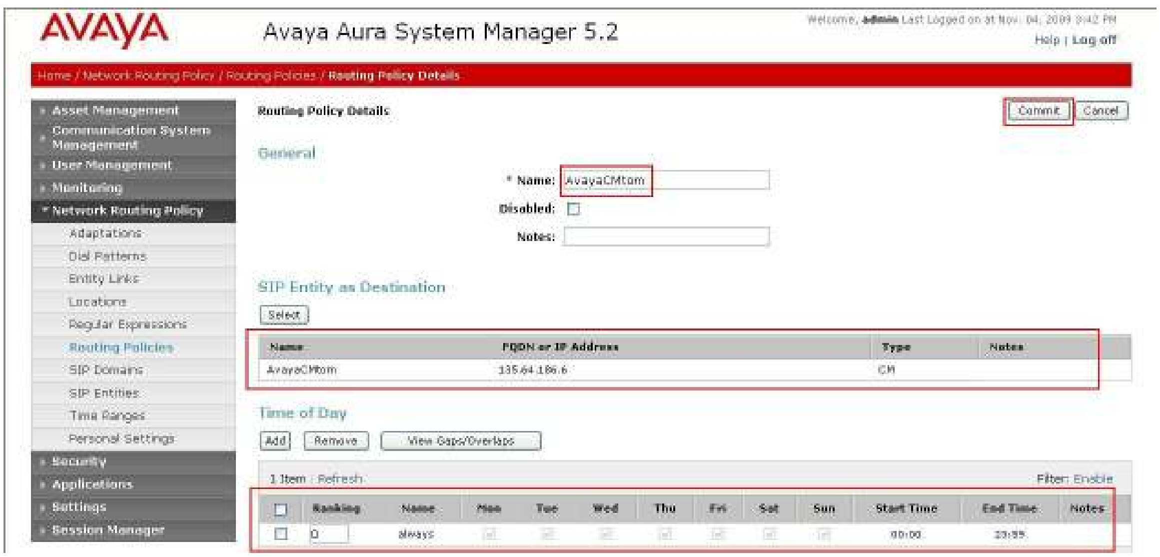
Under **SIP Entity as Destination**

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

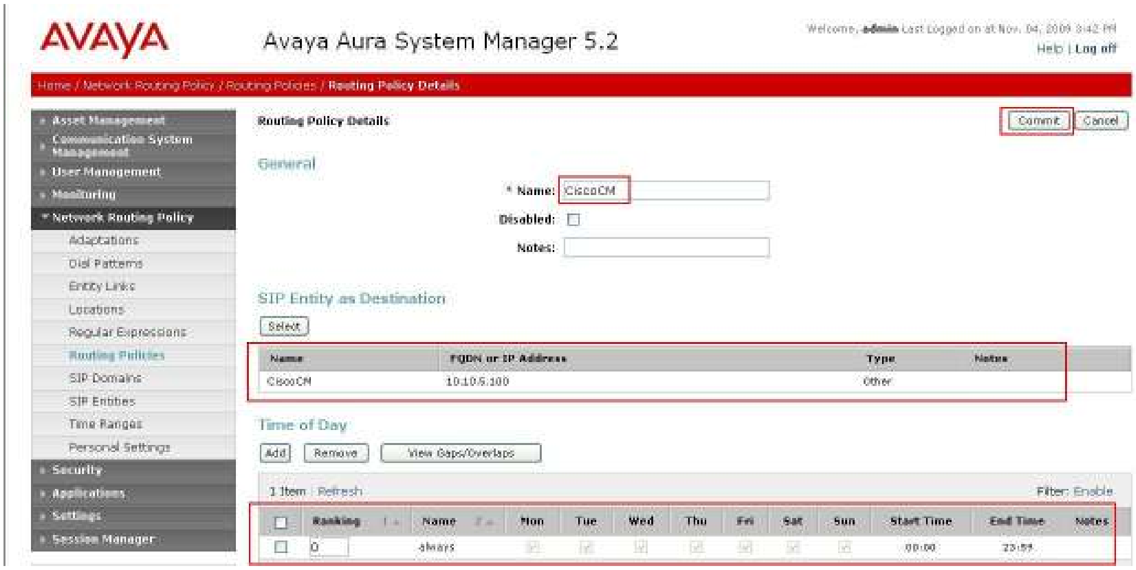
Under **Time of Day**

Click **Add**, and then select the time range configured in the previous step.

The following is screen shows the **Routing Policy Details** for Communication Manager.



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

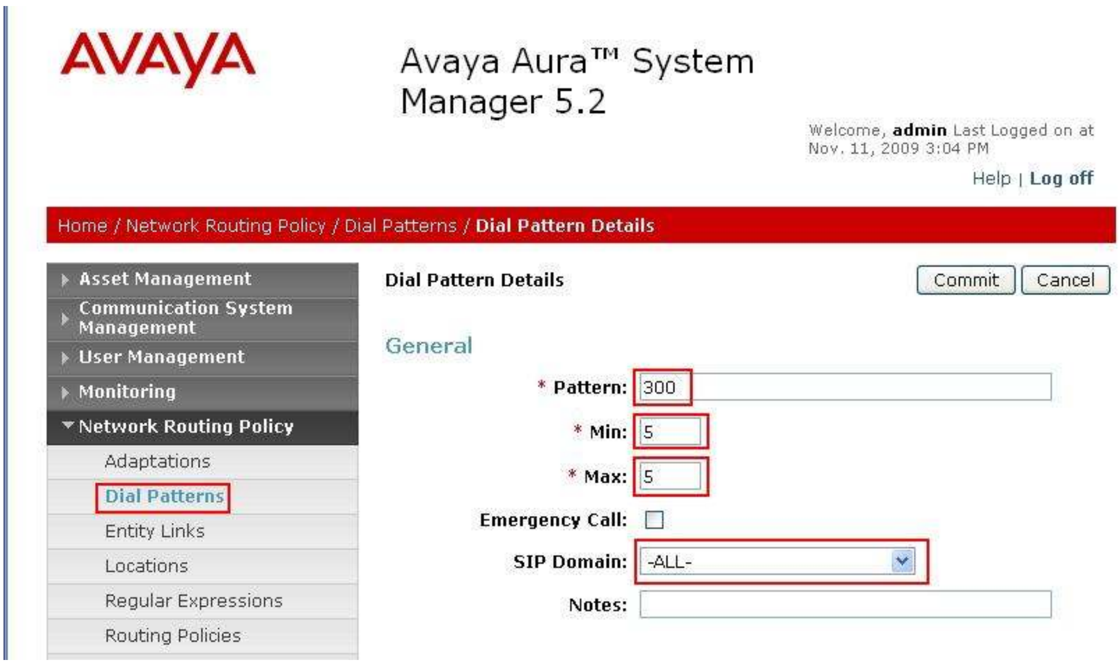


5.8. Administer Dial Patterns

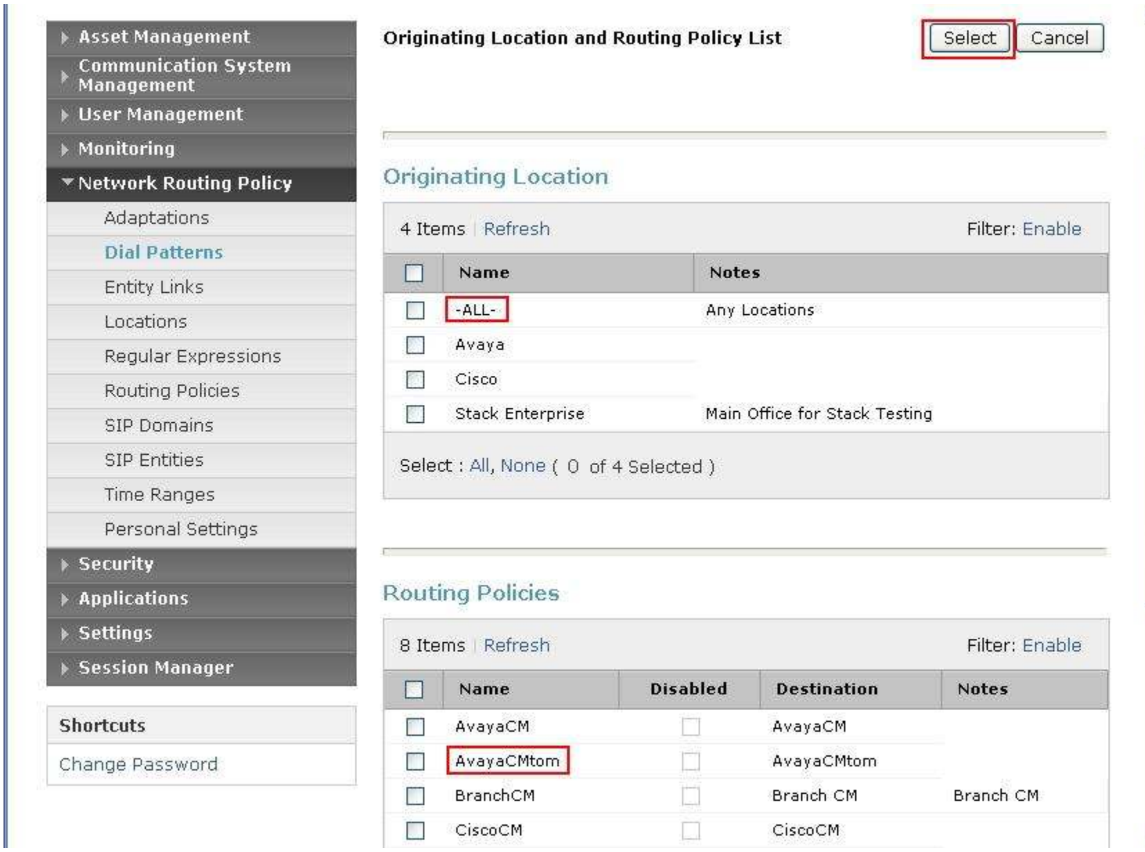
A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, 5-digit extension beginning with **300** reside on Communication Manager, and 5-digit extension beginning with **350** reside on Cisco UCM. For Communication Manager Dial Pattern configuration, select **Dial Patterns** on the left panel menu and then click on the **New** button (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
SIP Domain	Select **ALL**



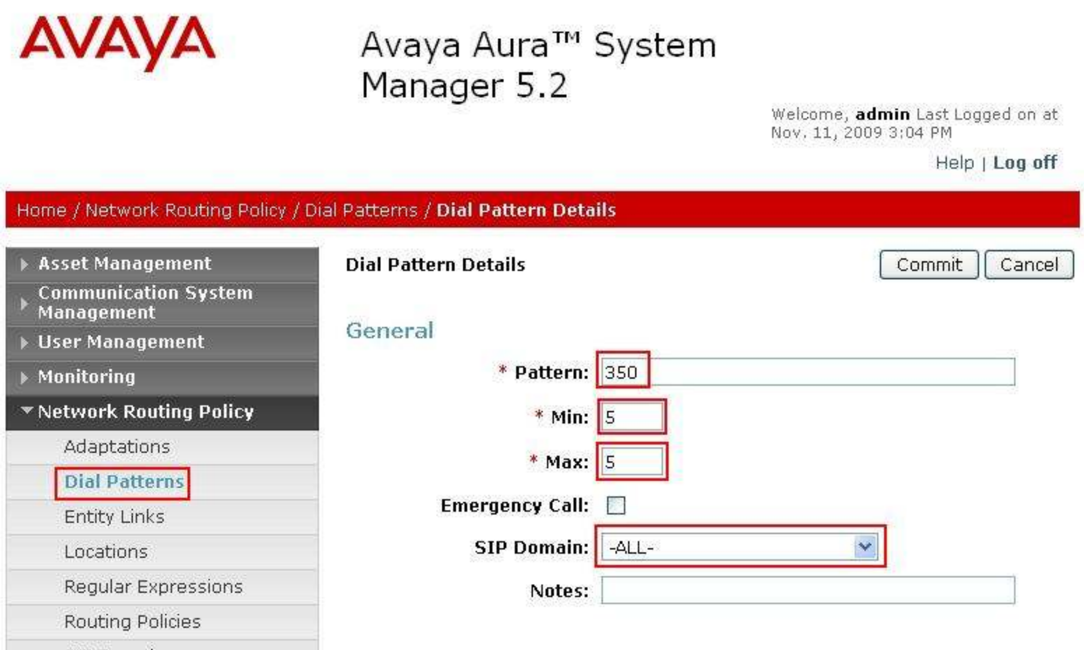
Navigate to **Originating Locations and Routing Policies** and select **Add** (not shown). Under **Originating Location** select all locations by checking the box next to **ALL** and under **Routing Policies** select a Routing Policy by checking the box next to **AvayaCMtom.** Click **Select** button to confirm the chosen options. You will then be returned to the Dial Pattern screen (shown above), select **Commit** button to save.



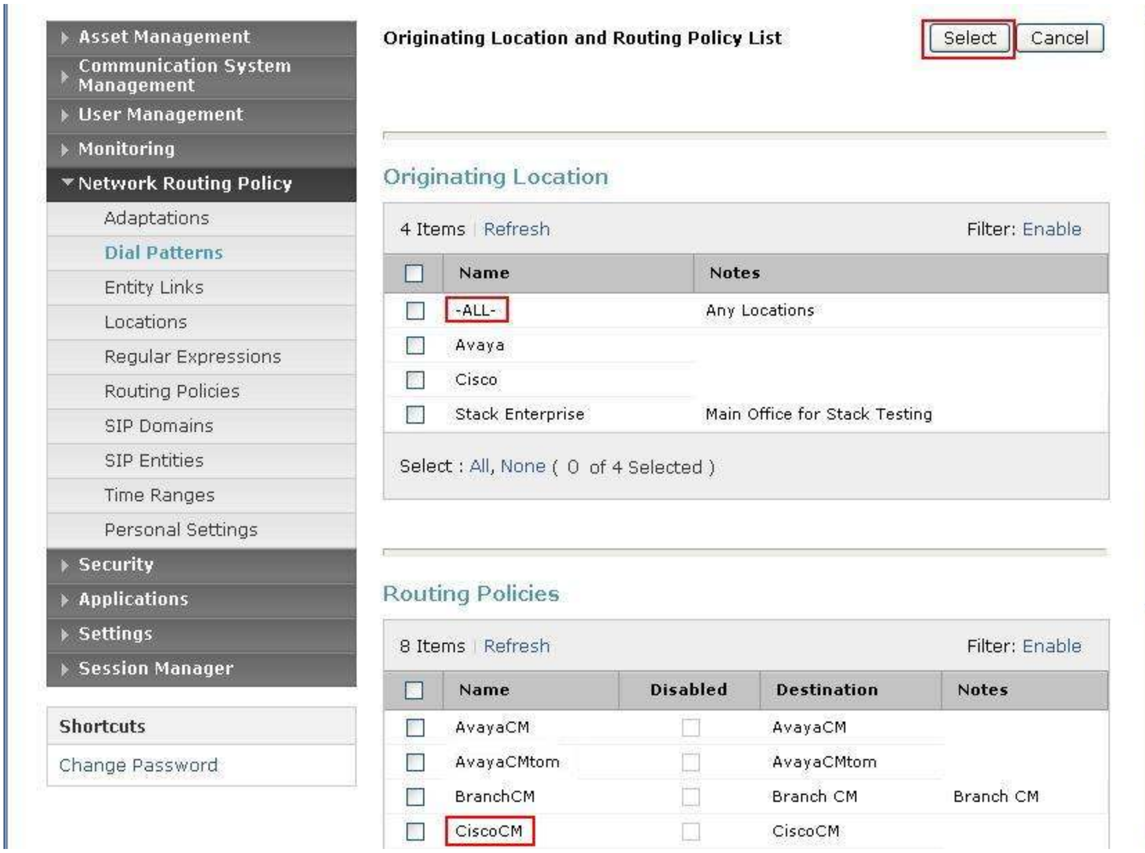
To configure Cisco UCM Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

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
SIP Domain	Select **ALL**



Navigate to **Originating Locations and Routing Policies** and select **Add** (not shown). Under **Originating Location** select **ALL** and under **Routing Policies** select **CiscoCM.** Click **Select** button to confirm the chosen options. You will then be returned to the Dial Pattern screen (shown above), select **Commit** button to save.



5.9. Administer Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the Session Manager menu on the left and select **Session Manager Administration**. Then click **Add**, and fill in the fields as described below and shown in the following screen:

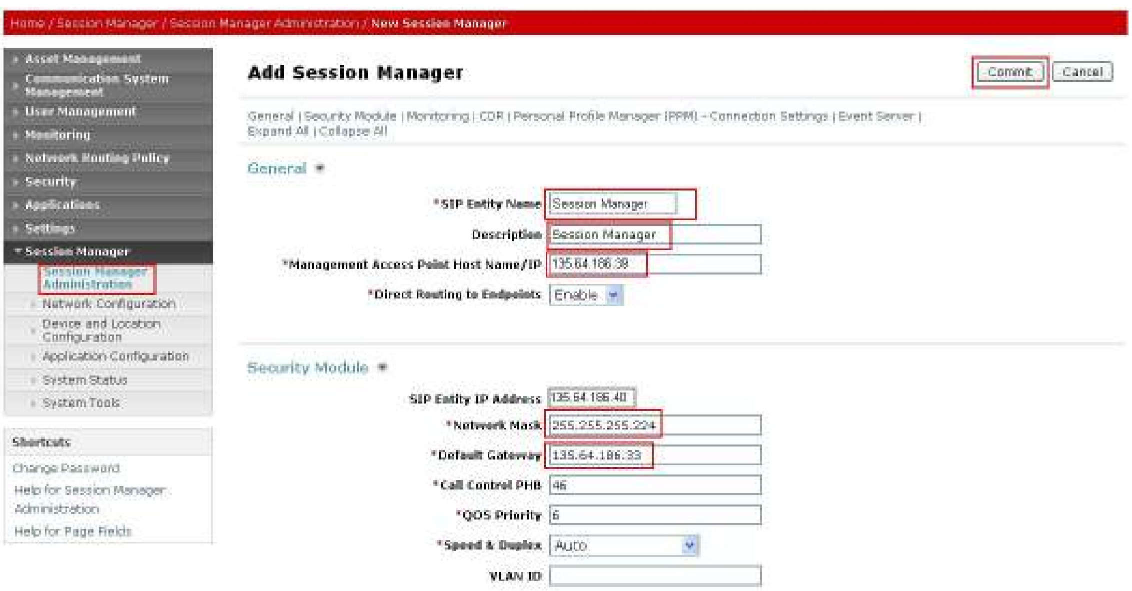
Under **General:**

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP** Enter the IP address of the SessionManager management interface.

Under **Security Module:**

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.



6. Configure Cisco UCM

This section provides the procedures for configuring Cisco UCM. 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]**. The procedures include configuration of the following items:

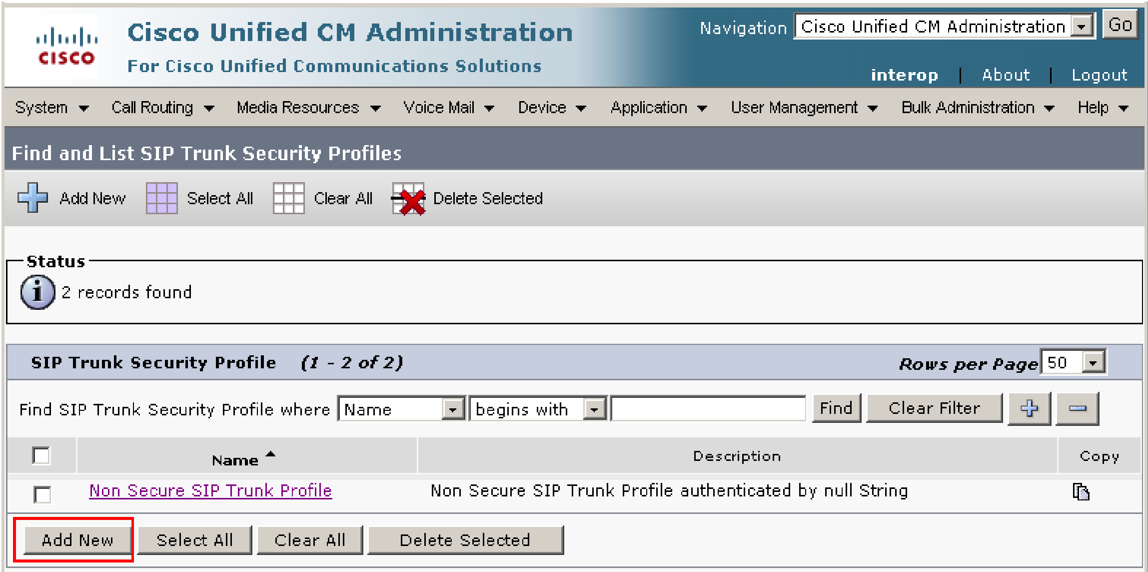
- Login to Cisco UCM
- Administer SIP Trunk Security Profile
- Administer SIP Trunk
- Administer Route Pattern
- Administer Phone

6.1. Login to Cisco UCM

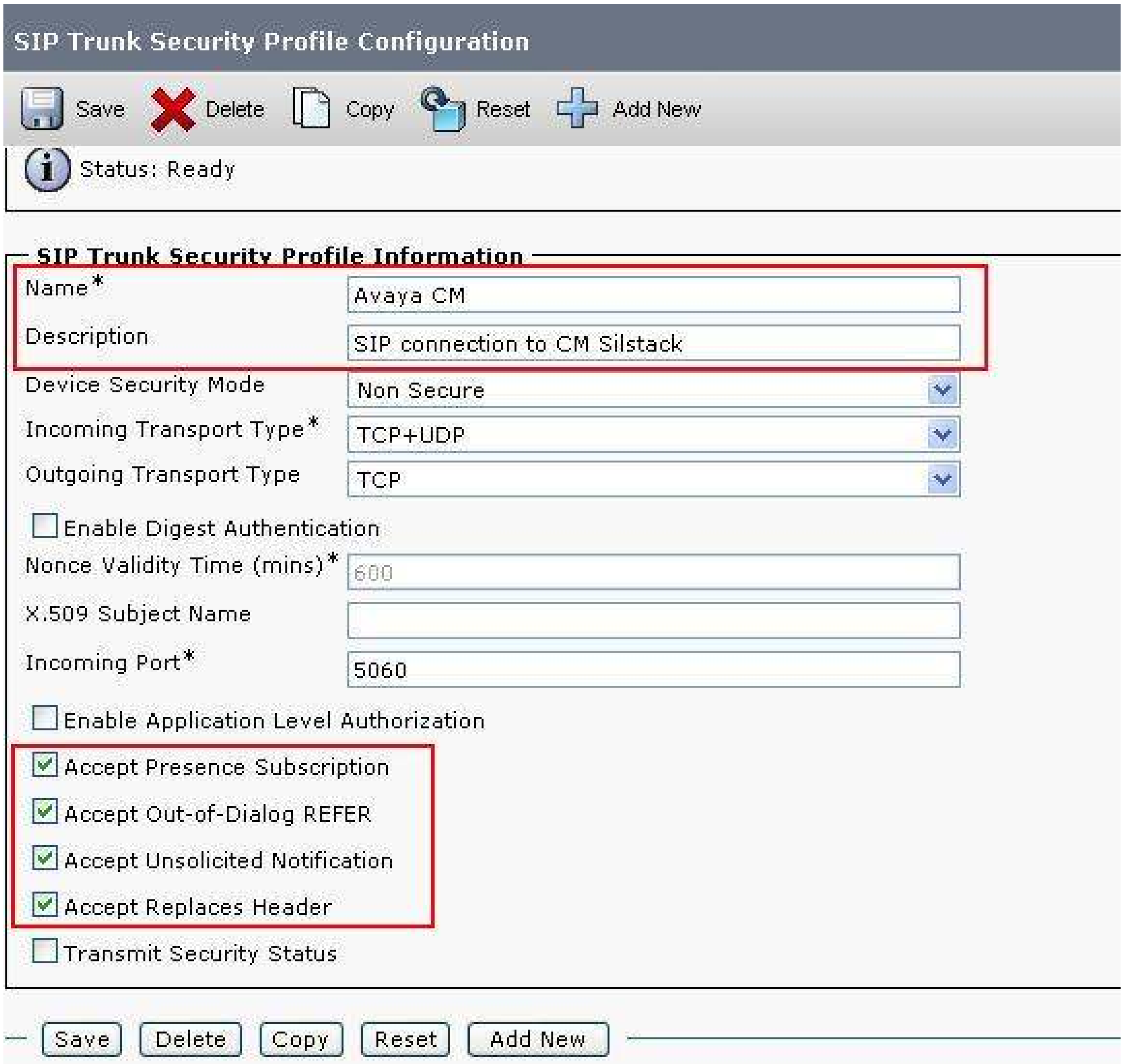
Open Cisco Unified CM Administration by entering the IP address of the CUCM into the Web Browser address field, and log in using an appropriate Username and Password.

6.2. Administer SIP Trunk Security Profile

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

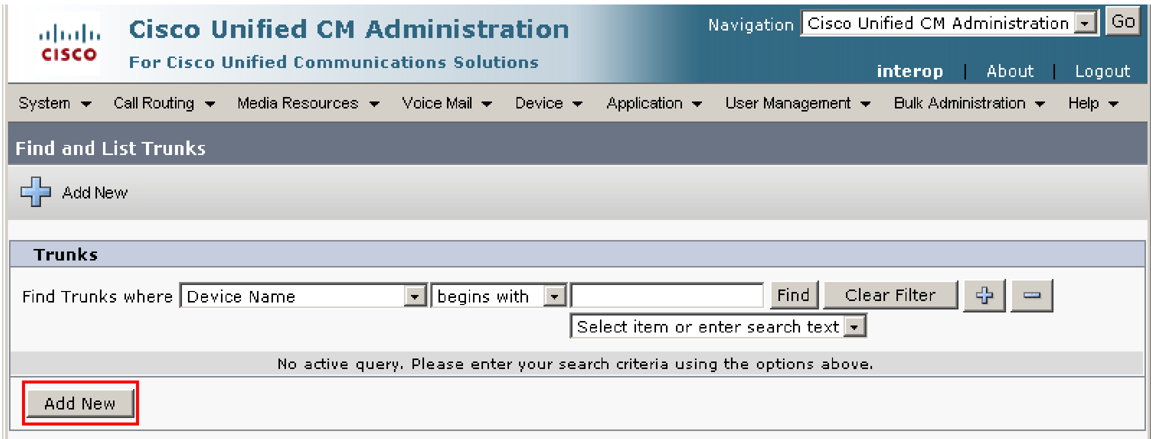


The following is a screen capture of the **SIP Trunk Security Profile Configuration** used in the sample network. Configure the highlighted areas and click **Save** to commit the changes.

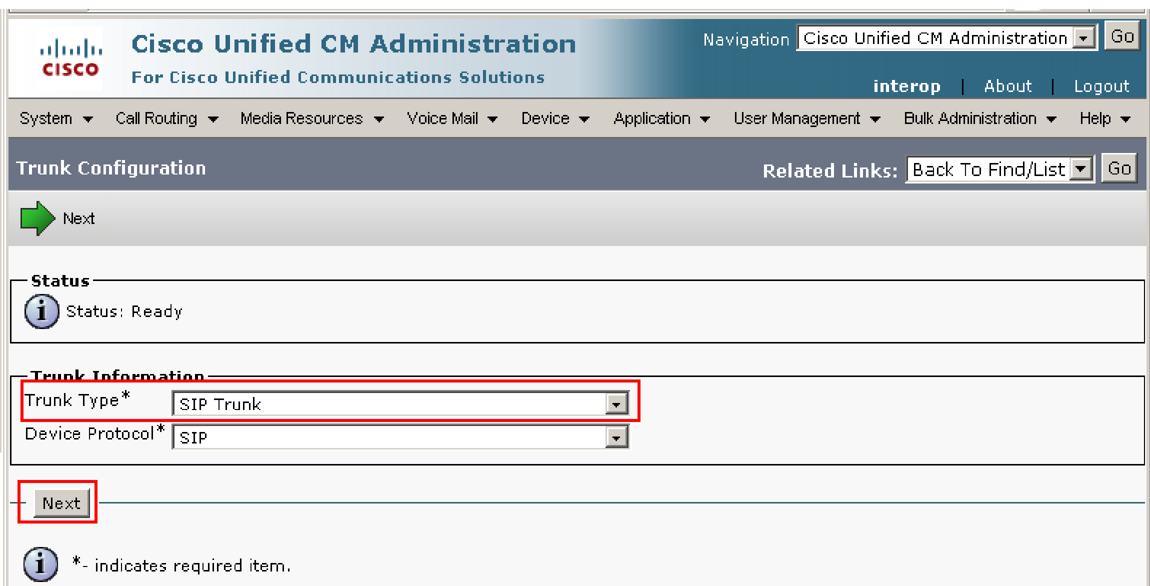


6.3. Administer SIP Trunk

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

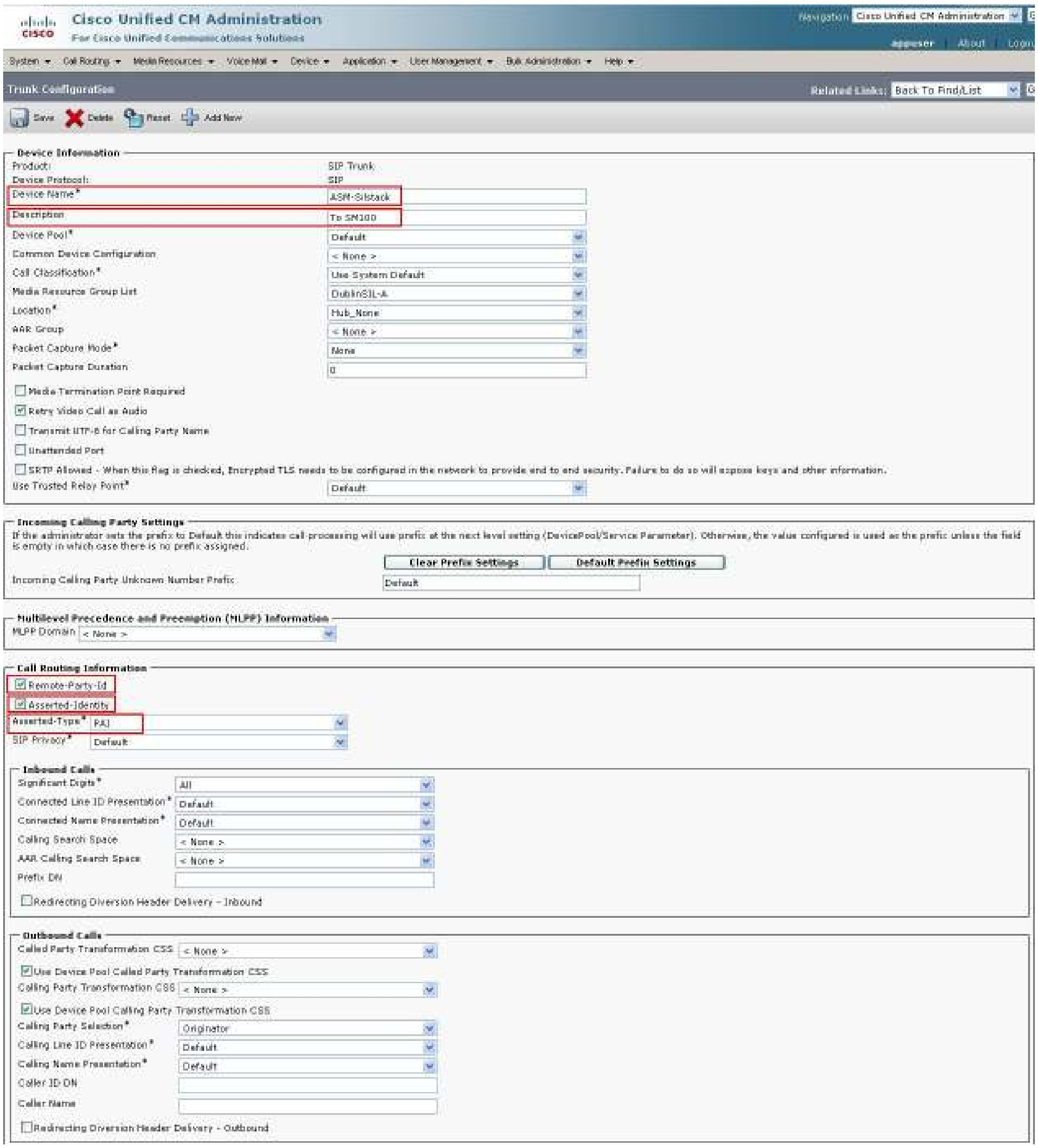


Select **SIP Trunk** as the **Trunk Type** and the **Device Protocol** field will automatically be changed to SIP. Click **Next** to continue.



Enter the appropriate information for the SIP Trunk. The following screen shows the configuration used in the sample network.

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



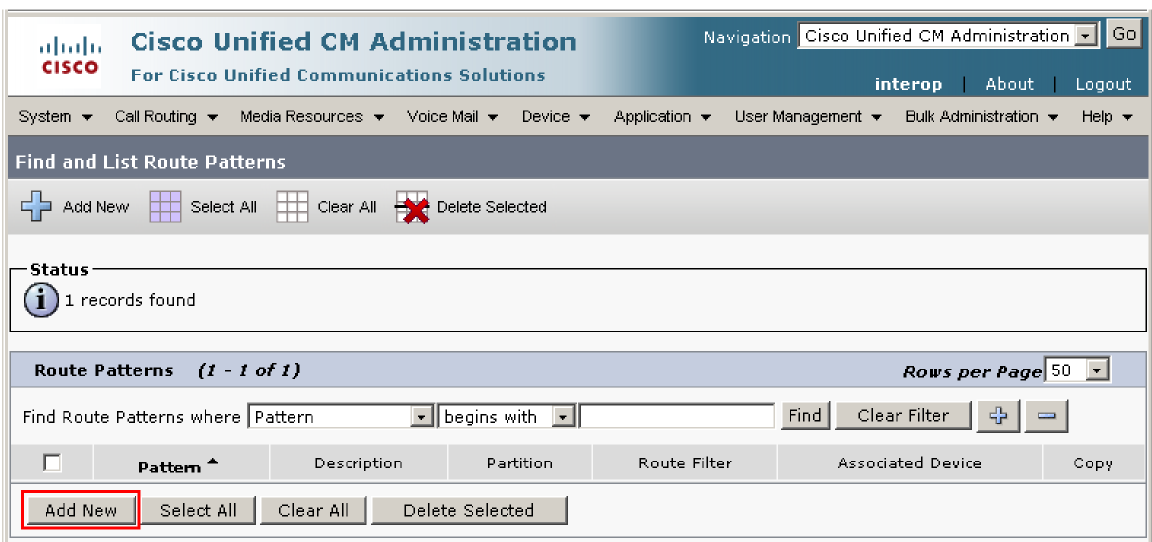
Navigate to SIP Information section and enter following configuration:

Destination Address	IP address of the Session Manager
Destination Port	Destination port number use for SIP communication
SIP Trunk Security Profile	Profile configured at **Section 6.2**
DTMF Signaling Method	Select **RFC 2833**

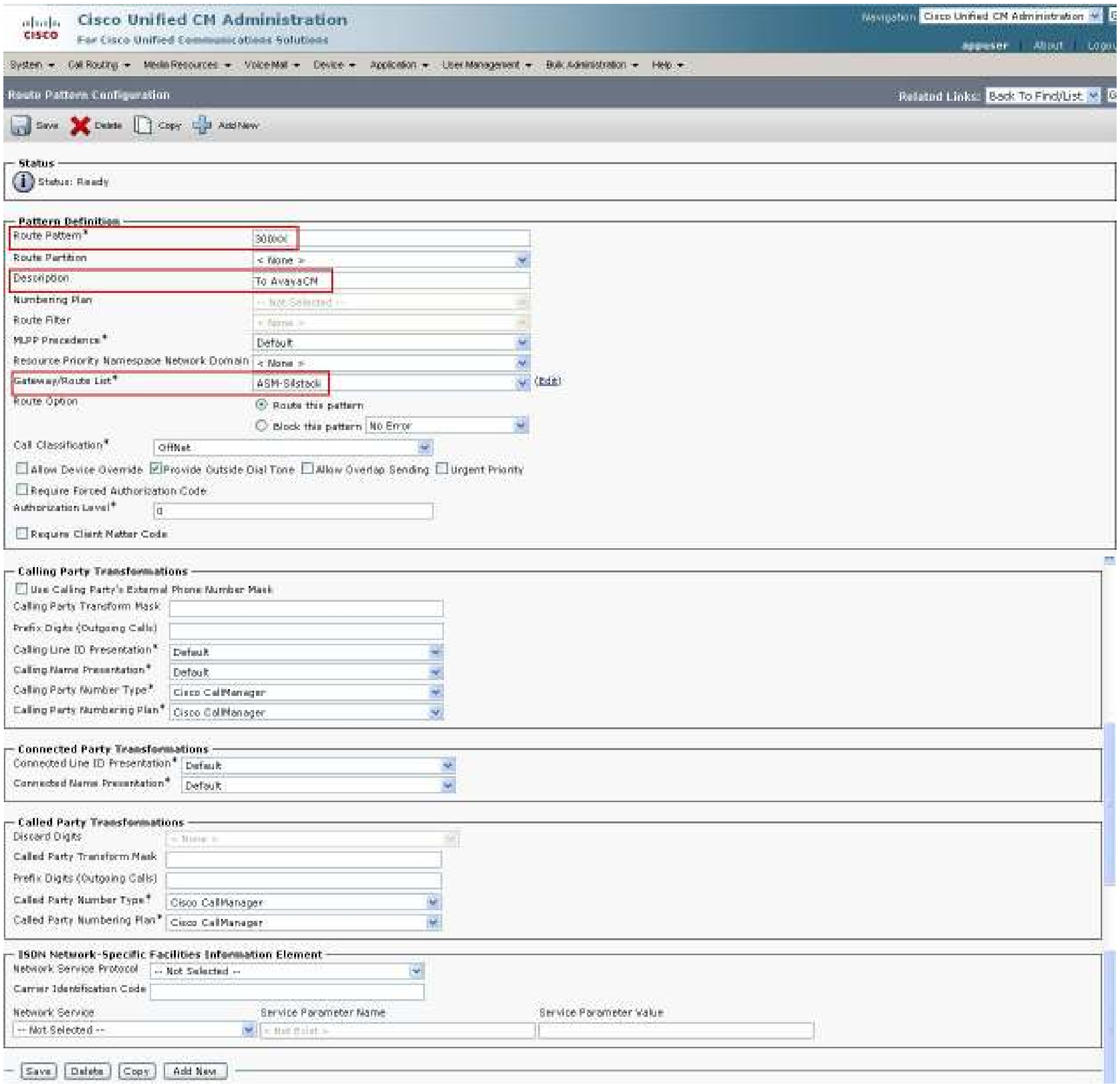
Click **Save** to complete.

6.4. Administer Route Pattern

Select **Call Routing → Route/Hunt → Route Pattern** then click **Add New** to add a new route pattern for extension 300xx which are for telephones registered with Communication Manager.

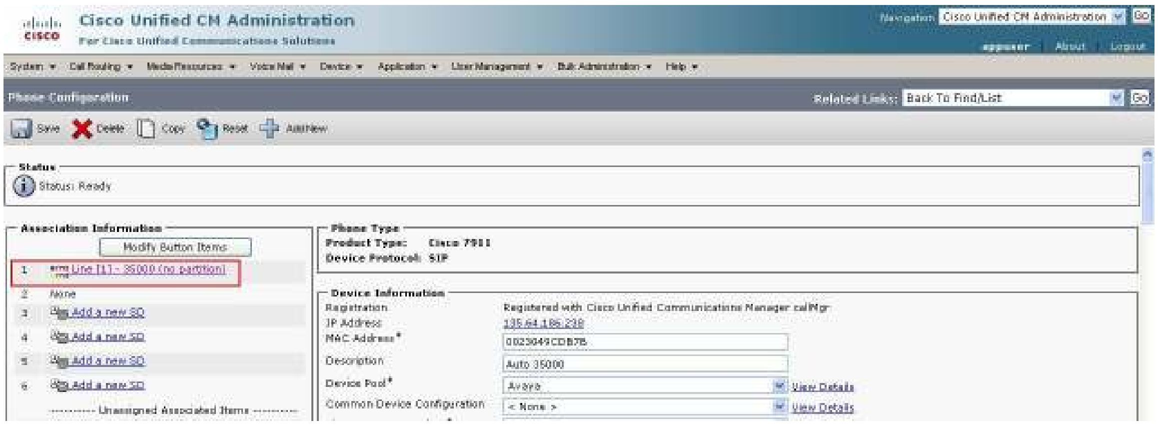


The following screen shows the route pattern used in the sample network. The route pattern **300xx** will cause all 5 digit calls beginning with 300 to be routed through the **ASM-Silstack** SIP Trunk defined in **Section 6.3.** Click **Save** to complete.

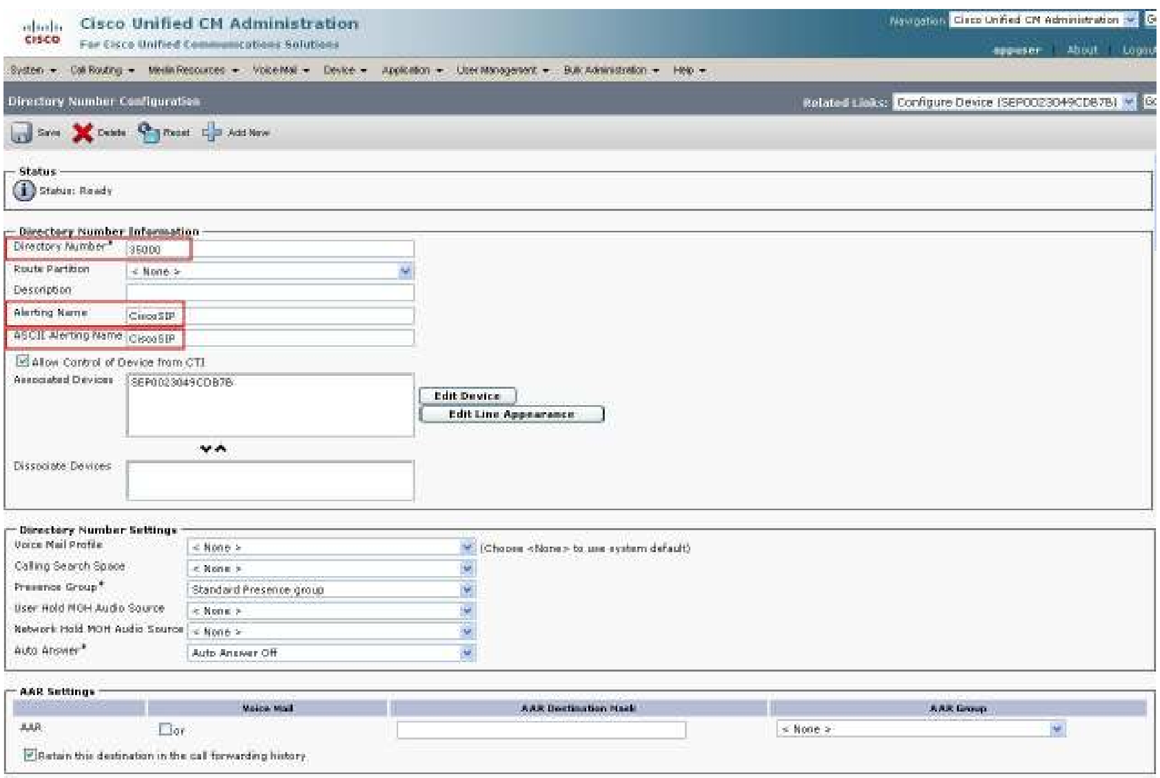


6.5. Administer Phone

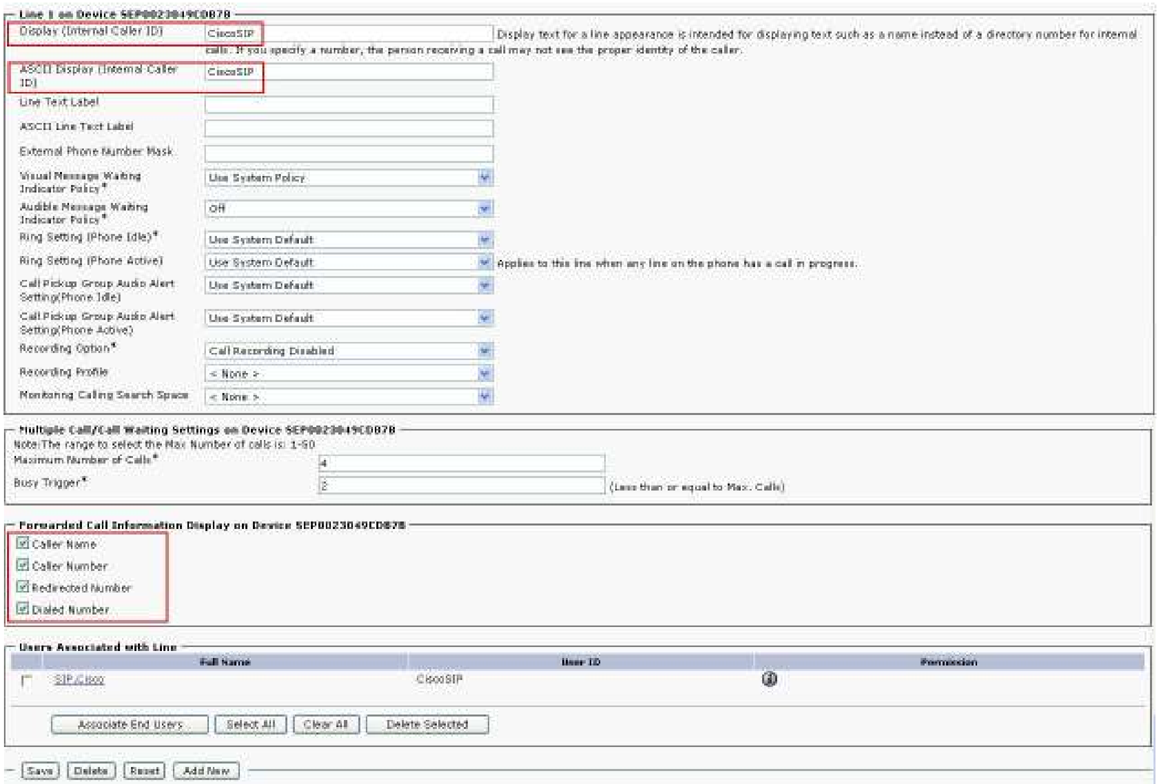
Select **Device → Phone** then click on the Device that needs to be administered. The following screen shows the display after a device has been selected. Click on the line for the device as highlighted in the screen below.



The following screen shows the display after the line has been selected. Enter information for **Alerting Name** and **ASCII Alerting Name.**



Navigate to **Line 1 on Device** section and enter information for **Display (Internal Caller ID)** and **ASCII Display (Internal Caller ID)**. This will be displayed on the called party phone on all outgoing calls. Check all boxes in **Forwarded Call Information Display on Device** section. Click **Save** to complete.



7. Verification

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

7.1. Communication Manager

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 145

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0145/001 T00036   in-service/idle    no
0145/002 T00037   in-service/idle    no
0145/003 T00038   in-service/idle    no
0145/004 T00039   in-service/idle    no
0145/005 T00040   in-service/idle    no
0145/006 T00041   in-service/idle    no
0145/007 T00042   in-service/idle    no
0145/008 T00043   in-service/idle    no
0145/009 T00044   in-service/idle    no
0145/010 T00045   in-service/idle    no
```

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.

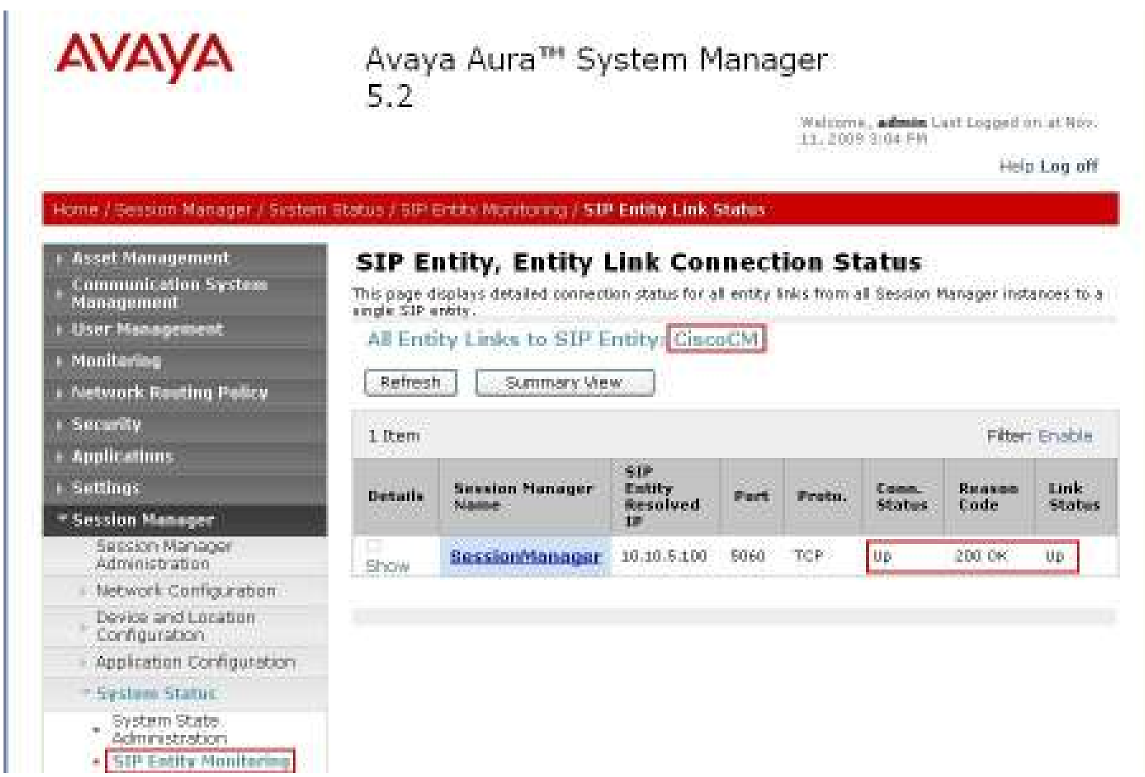
```
status signaling-group 140
                         STATUS SIGNALING GROUP

        Group ID: 140                             Active NCA-TSC Count: 0
      Group Type: sip                              Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

7.2. Session Manager

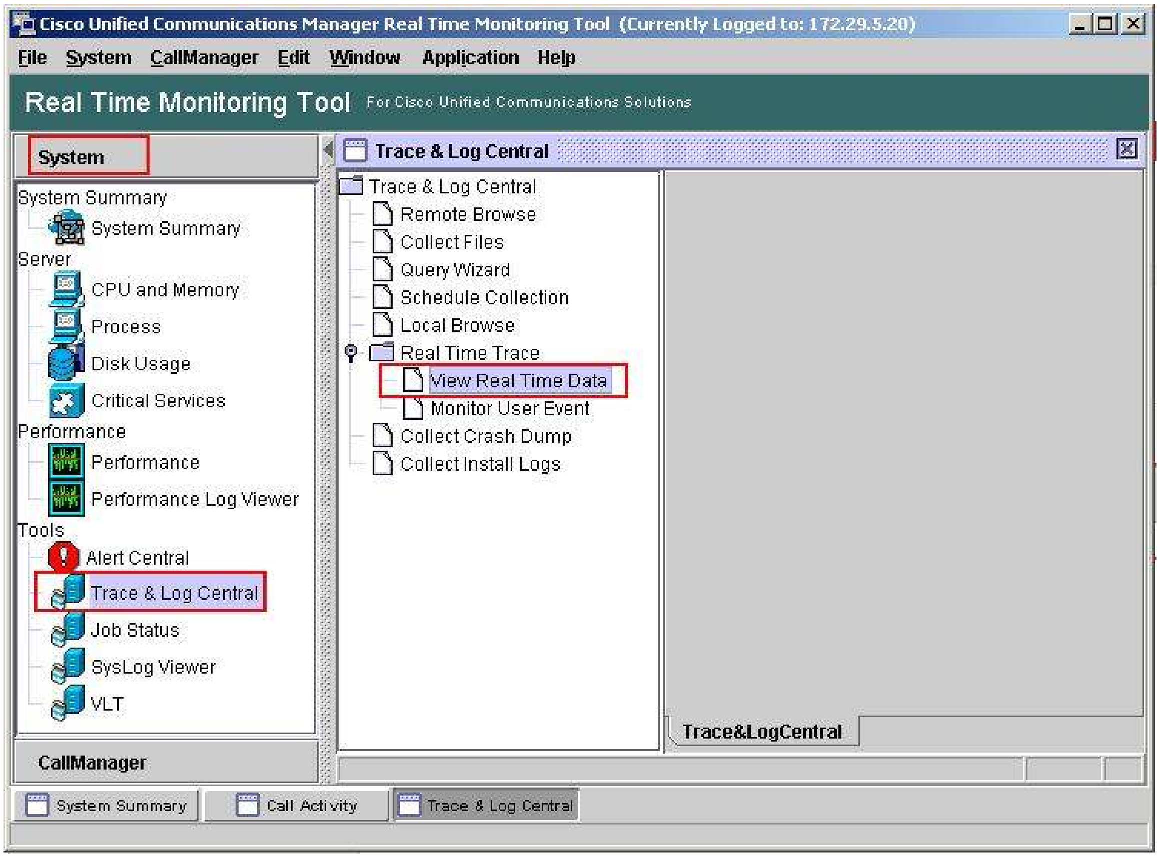
Select **Session Manager → System Status → SIP Entity Monitoring**. Verify as shown below that none of the SIP entities for Avaya or Cisco links are down, indicating that they are all reachable for routing.

Click on the SIP Entity Names AvayaCMtom and CiscoCM, shown in the previous screen, and verify that the connection status is **Up**, as shown in screenshots below.



7.3. Cisco Unified Communications Manager

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.



7.4. Verified Scenarios

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

- Basic calls between various telephones on Communication Manager and Cisco UCM can be made in both directions using G.711MU, G.729, and G.729AB. For G.729 interoperability, the IP codec set on 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 are shown below.
    - Unattended transfer
    - Attended transfer
    - Hold/Unhold
    - Consultation hold
    - Call forwarding
    - Conference

8. 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 observed:

- For G.729 interoperability, make sure both G.729 and G729AB are part of the audio codec selection in Communication Manager.
- For proper displaying of calling party information, Cisco UCM must be configured with the Internal Caller ID name as described in **Section 6.5**.
- With direct media shuffling enabled, a one-way audio issue was observed when a conference call was initiated by a Cisco phone to two Avaya H.323 phones. No audio was being sent towards the H.323 phones in the conference. A workaround is to disable direct media shuffling.

9. Additional References

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

[1] *Avaya Aura™ Session Manager Overview*, Doc # 03-603323, Issue 2

[2] *Administering Avaya Aura™ Session Manager*, Doc # 03-603324, Issue 2

[3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc # 03-603325, Issue 2

[4] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 9

[5] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Issue 5.0

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