Avaya Solution & Interoperability Test Lab

Configuring SIP trunks between Avaya Aura® Session Manager Release 6.2, Avaya Aura® Communication Manager Release 5.2.1 and Cisco Unified Communications Manager Release 8.6.2 – Issue 1.0

Abstract

These Application Notes describe a sample configuration of a network that provides SIP trunks between Avaya Aura® Session Manager Release 6.2, Avaya Aura® Communication Manager Element Server Release 5.2.1 and Cisco Unified Communications Manager Release 8.6.2.

- Avaya Aura® Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura® Communication Manager serves as an Element Server within the Avaya Aura® architecture and supports H.323 and Digital.
- Cisco Unified Communications Manager provides SIP trunks for connecting to other telephony systems and supports SCCP and SIP endpoints.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested for this solution.

1. Introduction

These Application Notes describe a sample configuration of a network that provides SIP trunks between Avaya Aura® Session Manager Release 6.2, Avaya Aura® Communication Manager Release 5.2.1 and Cisco Unified Communications Manager (CUCM) Release 8.6.2.

This document focuses on the configuration of the SIP trunks and call routing. Detailed administration of other aspects of Communication Manager, Session Manager or Cisco Unified Communications Manager will not be described. See the appropriate documentation listed in **Section 10** for more information.

2. Interoperability Testing

Avaya Aura® Communication Manager serves as an Element Server within the Avaya Aura® architecture and supports Avaya 9600 Series and 96x1 Series H.323 and 2410 Digital endpoints.

Testing was limited to station to station calls and supplemental features. Voice messaging was not tested. Interoperability was verified for SIP trunks between Avaya Aura® Session Manager Release 6.2, Avaya Aura® Communication Manager Release 5.2.1 and Cisco Unified Communications Manager Release 8.6.2.

2.1. Test Description and Coverage

Interoperability testing included making bi-directional calls between several different types of stations on both telephony systems with various features including hold, transfer, conference and forwarding.

An adaptation for the SIP entity was created to mitigate implementation deltas between the solutions tested.

2.2. Test Results and Observations

Overall test results were excellent. There were some minor issues in media behavior that were corrected by checking the Media Termination Point (MTP) box in CUCM SIP Trunk configuration. With media shuffling disabled, these tests passed.

3. Reference Configuration

A SIP trunk is used to connect Avaya Aura® Session Manager and Cisco Unified Communications Manager (CUCM), which routes calls between them based on the dialed number. In addition, a SIP trunk is configured between the Avaya Aura® Communication Manager and the Avaya Aura® Session Manager. Cisco 7965, 7962 and 7941 were configured as SIP endpoints. Cisco 7965, 7942, 7961 and Cisco IP Communicator were configured as SCCP endpoints. Cisco SIP and SCCP endpoints were registered to Cisco Unified Communications Manager.

As shown in **Figure 1**, CUCM 8.6.2 supports Cisco 7900 Series SCCP and SIP IP telephones. CUCM is connected over a SIP trunk to Avaya Aura® Session Manager Release 6.2, using the SIP Signaling network interface on Session Manager.

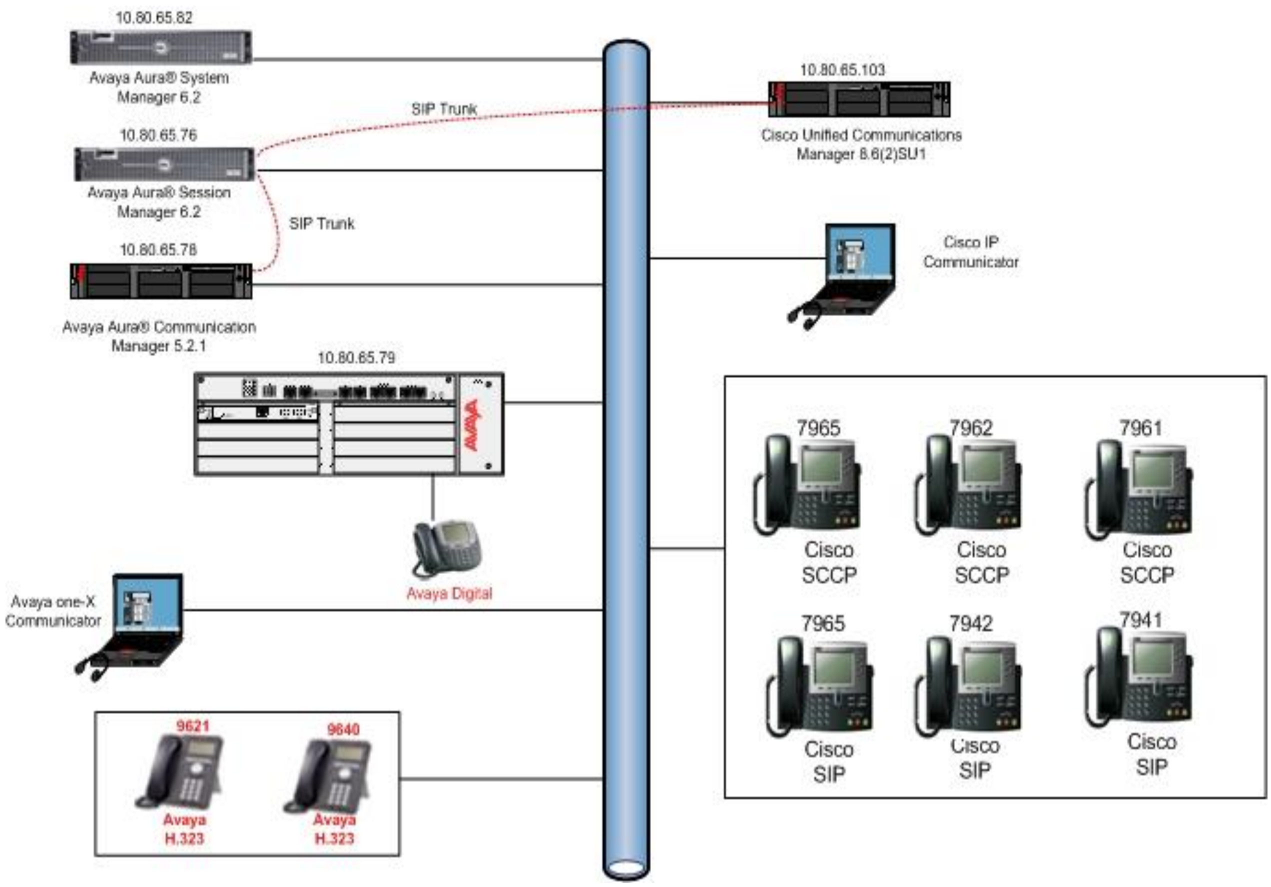


Figure 1 – Connection of Cisco Unified Communications Manager and Avaya Aura® Communication Manager via Avaya Aura® Session Manager using SIP Trunks

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Equipment/Software	Release/Version
Avaya Aura® Session Manager on HP® DL 360 G7 Server	6.2.1.0.621010
Avaya Aura® System Manager on Dell® R610 Server	6.2.12.1871
Avaya Aura® Communication Manager on Avaya S8500 Server	5.2.1 SP 1201 (R015x.02.1.016.4)
Avaya G430 Media Gateway	30.22.0
Avaya 9640 H.323 Telephone	3.0.04
Avaya 9621G H.323 Telephone	H.323 6.0.2.0 (S9621_41HALBR6_2r039H_V4r52.tar)
Avaya 2410 Digital Telephone	N/A
Avaya one-X Communicator	6.1.3.08 SP3 patch2
Cisco Unified Communications Manager	8.6.2.21900-5 (8.6(2)SU1)
Cisco 7965 Unified IP Telephone	SIP45.9-2-3S
Cisco 7965 Unified IP Telephone	SCCP45.9-2-3S
Cisco 7942 Unified IP Telephone	SCCP42.9-2-3S
Cisco 7962 Unified IP Telephone	SIP42.9-2-3S
Cisco 7941 Unified IP Telephone	SIP41.9-2-3S
Cisco 7961 Unified IP Telephone	SCCP41.9-2-3S
Cisco IP Communicator	8.6.1.0

5. Configure Avaya Aura® Communication Manager

This section describes the steps needed to configure Communication Manager to route and receive calls over the SIP trunk to Session Manager to support calls between Communication Manager and Cisco Unified Communications Manager. These instructions assume the Avaya G430 Media Gateway is already configured for Communication Manager. For more information describing these additional administration steps, see **References [6]** through **[8]** in **Section 10.**

This section describes the administration of Communication Manager using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity.

The following administration steps will be described:

- Verify System Capabilities and Communication Manager License
- Configure Trunk-to-Trunk Transfers
- Configure IP Codec Set
- Configure IP Network Region
- Configure IP Node Names and IP Addresses
- Configure SIP Signaling Groups and Trunk Groups
- Configure Route Pattern
- Administer Private Numbering Plan and Uniform Dialplan
- Administer Dialplan
- Administer AAR Analysis

After completing these steps, the **save translation** command should be performed.

5.1. Verify System Capacities and Licensing

This section describes the procedures to verify the correct system capacities and licensing have been configured. If there is insufficient capacity or if a required feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

Step 1: Verify SIP Trunk Capacity is sufficient for the expected number of calls.

On **Page 2** of the **display system-parameters customer-options** command, verify an adequate number of SIP Trunk Members are administered for the system as shown below.

```
display system-parameters customer-options                  Page   2 of  11
                                OPTIONAL FEATURES
IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 0     0
…
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 100  20
…
```

Step 2: Verify AAR/ARS Routing features are Enabled on system.

To simplify the dialing plan for calls between telephony systems, verify the following AAR/ARS features are enabled on the system.

On **Page 3** of the **display system-parameters customer-options** command, verify the following features are enabled.

- **ARS?** Verify "**y**" is displayed.
- **ARS/AAR Partitioning?** Verify "**y**" is displayed.
- **ARS/AAR Dialing without FAC?** Verify "**y**" is displayed.

```
display system-parameters customer-options                    Page   3 of  10
                                OPTIONAL FEATURES

 A/D Grp/Sys List Dialing Start at 01? n                           CAS Main? y
Answer Supervision by Call Classifier? n                  Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? n
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                         DCS (Basic)? n
          ASAI Link Core Capabilities? y                   DCS Call Coverage? n
…
```

Step 3: Verify Private Networking feature is Enabled.

On **Page 5** of the **display system-parameters customer-options** command, verify the **Private Networking** feature is set to "**y**".

```
display system-parameters customer-options                    Page   5 of  10
                                OPTIONAL FEATURES
                                                          Uniform Dialing Plan? y
                    Private Networking? y    Usage Allocation Enhancements? y
              Processor and System MSP? y
                    Processor Ethernet? y               Wideband Switching? y
…
```

5.2. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when an incoming call to a SIP station is transferred to another SIP station. For simplicity, the **Trunk-to-Trunk Transfer** field on **Page 1** was set to "**all**" to enable all trunk-to-trunk transfers on a system wide basis.

Note: Enabling this feature poses significant security risk by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, a COS could be defined to allow trunk-to-trunk transfers for specific trunk group(s). For more information regarding how to configure Communication Manager to minimize toll fraud, see **Reference [8]** in **Section 10.**

```
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
…
```

5.3. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is the number used to identify the codec set.

Enter the following values:

- **Audio Codec**: Enter "**G.711MU**" and "**G.729**" as supported types.
- **Silence Suppression**: Retain the default value "**n**".
- **Frames Per Pkt**: Enter "**2**".
- **Packet Size (ms):** Enter "**20**".
- **Media Encryption**: Enter the value based on the system requirement. For the sample configuration, "**none**" was used.

```
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.729              n          2         20
 3:

     Media Encryption
 1: none
```

5.4. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is an available network region.

Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration. For the sample configuration, "**avaya.com**" was used.
- **Name:** Enter descriptive name.
- **Codec Set:** Enter the number of the IP codec set configured in **Section 5.3**.
- **Intra-region IP-IP Direct Audio:** Enter "**yes**".
- **Inter-region IP-IP Direct Audio:** Enter "**yes**".

```
change ip-network-region 1                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name: Main Network Region
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
…
```

5.5. Configure IP Node Names and IP Addresses

Use the **change node-names ip** command to add the node-name and IP Addresses for the "**procr**" interface on Communication Manager and the SIP signaling interface of Session Manager, if not previously added.

In the sample configuration, the node-name of the SIP signaling interface for Session Manager is "**asm1-r62**" with an IP address of "**10.80.65.76**".

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                  IP Address
asm1-r62              10.80.65.76
default               0.0.0.0
procr                 10.80.65.78
```

5.6. Configure SIP Signaling Groups and Trunk Groups

This section provides the configuration of SIP trunk between Communication Manager and Session Manager to support sending and receiving calls to/from stations supported by CUCM.
In the sample configuration, trunk group "**10**" and signaling group "**10**" were used for connecting to Session Manager.

Step 1: Add Signaling Group for SIP Trunk

Use the **add signaling-group n** command, where **n** is an available signaling group number.
Enter the following values and use default values for remaining fields.

- **Group Type:** Enter "**sip**".
- **IMS Enabled:** Enter "**n**".
- **Transport Method:** Enter "**tcp**".
- **Near-end Node Name:** Enter "**procr**" node name from **Section 5.5**.
- **Far-end Node Name:** Enter node name for the first Session Manager defined in **Section 5.5**.
- **Near-end Listen Port:** Verify "**5060**" is used.
- **Far-end Listen Port:** Verify "**5060**" is used.
- **Far-end Network Region**: Enter network region defined in **Section 5.4**.
- **Far-end Domain:** Enter domain name for **Authoritative Domain** field defined in **Section 5.4**.
- **DTMF over IP:** Verify "**rtp-payload**" is used.

```
add signaling-group 10                                    Page   1 of   2
                                SIGNALING GROUP

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

   Near-end Node Name: procr                   Far-end Node Name: asm1-r62
 Near-end Listen Port: 5060                  Far-end Listen Port: 5060
                                          Far-end Network Region: 1
Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
           DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 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):
```

Step 2: Add SIP Trunk Group

Add the corresponding trunk group controlled by the signaling group defined in **Step 1** using the **add trunk-group n** command where **n** is an available trunk group number.

Enter the following values and use default values for remaining fields.

- **Group Type:** Enter "**sip**".
- **Group Name:** Enter a descriptive name.
- **TAC:** Enter an available trunk access code.
- **Direction:** Enter "**two-way**".
- **Outgoing Display?** Enter "**n**".
- **Service Type:** Enter "**tie**".
- **Signaling Group:** Enter the number of the signaling group added in **Step 1.**
- **Number of Members:** Enter the number of members in the SIP trunk (must be within the limits for number of SIP trunks configured in **Section 5.1**).

Note: once the **add trunk-group** command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

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

Group Number: 10                    Group Type: sip          CDR Reports: y
  Group Name: trk to asm1-r62       COR: 1        TN: 1        TAC: #10
Direction: two-way        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                     Signaling Group: 10
                                                   Number of Members: 20
```

On **Page 3**, enter the following values and use default values for remaining fields.

- **Numbering Format** Enter "**private**".
- **Show ANSWERED BY on Display** Enter "**y**".

```
add trunk-group 10                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y

                     Numbering Format: private
                                              UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n

 Show ANSWERED BY on Display? y
```

On **Page 4**, enter the following values and use default values for remaining fields.

- **Support Request History** Enter "**y**".
- **Telephone Event Payload Type** Enter "**101**".

```
add trunk-group 10                                            Page   4 of  21
                                     PROTOCOL VARIATIONS

                      Mark Users as Phone? y
            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
```

5.7. Configure Route Pattern

This section provides the configuration of the route pattern used in the sample configuration for routing calls to stations supported by Cisco Unified Communications Manager.

Use **change route-pattern n** command where **n** is an available route pattern.

Enter the following values and use default values for remaining fields.

- **Grp No** Enter a row for the trunk group defined in **Section 5.6**.
- **FRL** Enter "**0**".
- **Numbering Format** Enter "**lev0-pvt**".

In the sample configuration, route pattern "**10**" was created as shown below.

```
change route-pattern 10                                    Page   1 of  3
                        Pattern Number: 10  Pattern Name: sip trk to asm1
                          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: 10   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                           lev0-pvt  none
2: y y y y y n  n            rest                                     none
3: y y y y y n  n            rest                                     none
…
```

5.8. Administer Private Numbering Plan

Extension numbers used for SIP Users registered to Session Manager or for stations supported by Cisco Unified Communications Manager must be added to either the private or public numbering table on Communication Manager. For the sample configuration, private numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **Reference [7]** in **Section 10**.

Use the **change private-numbering n** command, where **n** is the length of the private number.

Fill in the indicated fields as shown below.

- **Ext Len**: Enter length of extension numbers. In the sample configuration, "4" was used.
- **Ext Code**: Enter leading digit (s) from extension number. In the sample configuration, "**40**" was used for SIP stations on Communication Manager and "**30**" was used for stations supported by Cisco Unified Communications Manager.
- **Trk Grp(s):** Enter trunk group defined in **Section 5.6**.
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.
- **Total Length:** Enter "**4**".

```
change private-numbering 1                                   Page   1 of   2
                            NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private           Total
Len Code             Grp(s)      Prefix            Len
 4  30               10                             4    Total Administered: 3
 4  40               10                             4       Maximum Entries: 540
```

5.9. Administer Uniform Dialplan

This section provides the configuration of the Uniform Dialplan pattern used in the sample configuration for routing calls between the telephony systems.

Note: Other methods of routing may be used.

Use the **change uniform-dialplan n** command where **n** is the first digit of the number assigned to a station supported by Cisco Unified Communications Manager. In the sample configuration, the numbers on the CUCM system start with digits "**30**".

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Matching Pattern** Enter the number Communication Manager matches to dialed numbers. Accepts up to seven digits.
- **Len** Enter the number of user-dialed digits the system collects to match to this Matching Pattern value.
- **Del** Enter number of digits to delete before routing the call.
- **Net** The server or switch network used to analyze the converted number. The converted digit-string is routed either as an extension number or through its converted AAR address, its converted ARS address, or its ENP node number. In the sample configuration "**aar**" was used.
- **Conv** Enables or disables additional digit conversion.

```
change uniform-dialplan 1                                  Page    1 of   2
                          UNIFORM DIAL PLAN TABLE
                                                            Percent Full: 0


    Matching                      Insert                   Node
    Pattern              Len  Del   Digits     Net   Conv   Num
    30                    4    0               aar     n
```

5.10. Administer Dial Plan

Use the **change dialplan analysis** command.

In the sample configuration, 4-digit extension numbers starting with "**30**" are used for stations supported by Cisco Unified Communications Manager.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Dialed String** Enter digit pattern for extension numbers on CUCM system.
- **Total Length** Enter length of extension numbers.
  For the sample configuration, "**4**" was used.
- **Call Type** Enter "**ext**".

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

    Dialed    Total   Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length  Type      String    Length Type      String    Length Type
   30           4     ext
   40           4     ext
   *            3     fac
   #            3     dac
```

5.11. Administer AAR Analysis

Use the **change aar analysis n** command.

In the sample configuration, 4-digit extension numbers starting with "**30**" are used for stations supported by Cisco Unified Communications Manager.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Dialed String** Enter digit pattern for extension numbers on CUCM system.
- **Total Min** Enter minimum length of extension numbers.
  For the sample configuration, "**4**" was used.
- **Total Max** Enter maximum length of extension numbers.
  For the sample configuration, "**4**" was used.
- **Call Type** Enter "**unku**".

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

    Dialed           Total     Route    Call   Node  ANI
    String          Min  Max  Pattern   Type   Num   Reqd
    30              4    4     10       unku         n
    40              4    4     10       unku         n
```

5.12. Save Translations

Configuration of Communication Manager Element Server is complete. Use the **save translation** command to save these changes.

Note: After making a change on Communication Manager which alters the dial plan or numbering plan, synchronization between Communication Manager and System Manager must be completed and SIP telephones must be re-registered.

See **Section 6.8** for more information on how to perform an on-demand synchronization.

6. Configure Avaya Aura® Session Manager

This section describes the procedures for configuring Avaya Aura® Session Manager to route calls between Communication Manager and CUCM.

These instructions assume other administration activities have already been completed such as defining SIP entities for Session Manager, defining the network connection between System Manager and Session Manager and defining SIP users. For more information on these additional actions, see **References [3]** and **[5]** in **Section 10.**

The following administration activities will be described:

- Define SIP Domain
- Configure Adaptation Module for calls to Cisco Unified Communications Manager.
- Define SIP Entities for both telephony systems.
- Define Entity Links, which describe the SIP trunk parameters used by Session Manager when routing calls between SIP Entities.
- Define Routing Policies and Dial Patterns which control routing between SIP Entities.
- Synchronize Changes with Avaya Aura® Communication Manager.

Note: Some administration screens have been abbreviated for clarity.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL "**http://<ip-address>/SMGR**", where "**<ip-address>**" is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

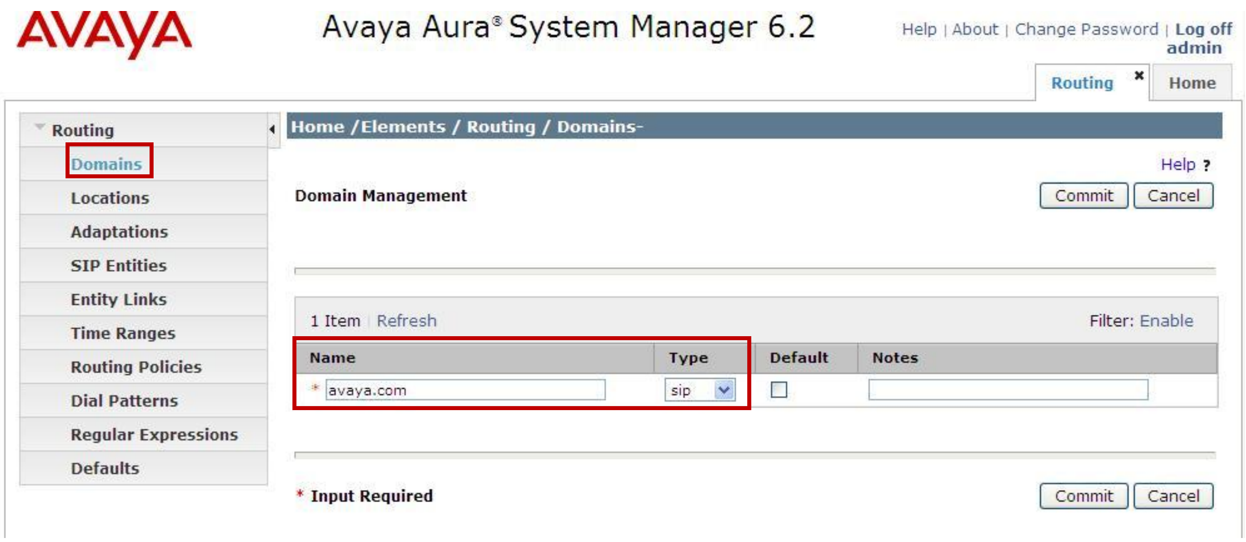
6.1. Define SIP Domains

Expand **Elements → Routing** and select **Domains** from the left navigation menu.

Click **New** (not shown)**.** Enter the following values and use default values for remaining fields**.**

- **Name** Enter the Authoritative Domain Name specified in **Section 5.4**. For the sample configuration, "**avaya.com**" was used.
- **Type** Select "**sip**" from drop-down menu.
- **Notes** Add a brief description. [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



Repeat to create a domain for CUCM called "cucm.com".

6.2. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to modify SIP messages before or after routing decisions are made. For example, Adaption Modules are used to support interoperability with third party SIP products such as Cisco Unified Communications Manager.

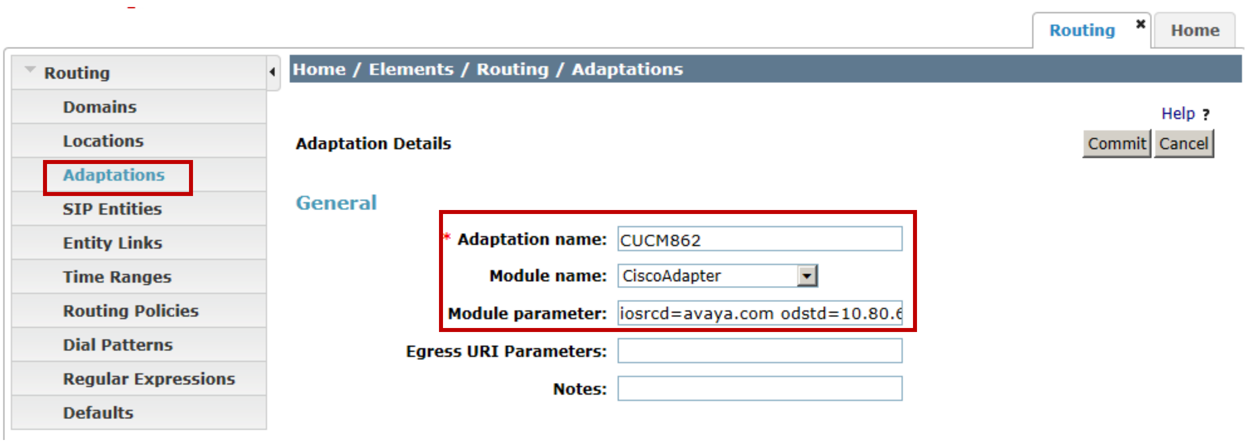
Expand **Elements** → **Routing** and select **Adaptations** from the left navigational menu.

Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module.
- **Module Name:** Select "**CiscoAdapter**" from drop-down menu.
- **Module parameter**: Enter "**iosrcd=<domain>**" where <domain> is the domain defined in **Section 6.1**.
  Enter "**odstd=<IP address>**" where <IP address> is address for Cisco Unified Communications Manager system.
  Note: iosrcd is the abbreviation for **Ingress Override Source Domain** parameter and odstd is the abbreviation for **Override Destination Domain** parameter. For more information on use of module parameters, see **Reference [5]** in **Section 10**.
- **Notes:** Enter a brief description. [Optional]

Click **Commit.** The Adaptation Module defined for sample configuration is shown below.

Note: Digit conversion was not required for sample configuration.



6.3. Define SIP Entities

A SIP Entity must be added for each telephony system connected over a SIP trunk to Session Manager.

Expand **Elements → Routing** and select **SIP Entities** from the left navigation menu.

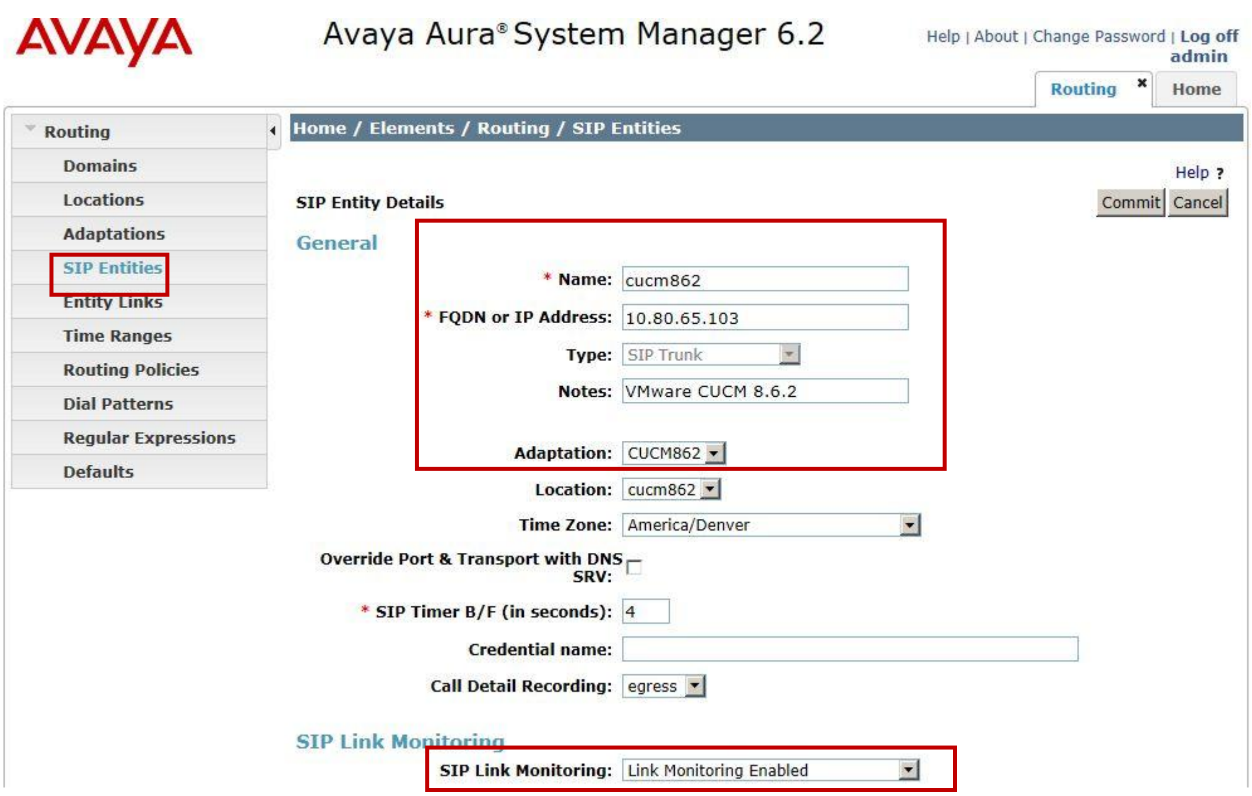
Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields to define a SIP Entity for CUCM system**.**

- **Name:** Enter an identifier for new SIP Entity.
- **FQDN or IP Address:** Enter IP address of CUCM system.
- **Type:** Select "**SIP Trunk**".
- **Adaptation:** Select the Adaptation Module configured for CUCM in **Section**.**6.2**
- **Notes:** Enter a brief description. [Optional].

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Link Monitoring Enabled**".

Click **Commit** to save SIP Entity definition. The following screen shows the SIP Entity defined for the Cisco Unified Communications Manager system.



Repeat this step to define a SIP Entity for Communication Manager.

6.4. Define Entity Links

A SIP trunk between Session Manager and each telephony system is described by an Entity Link.

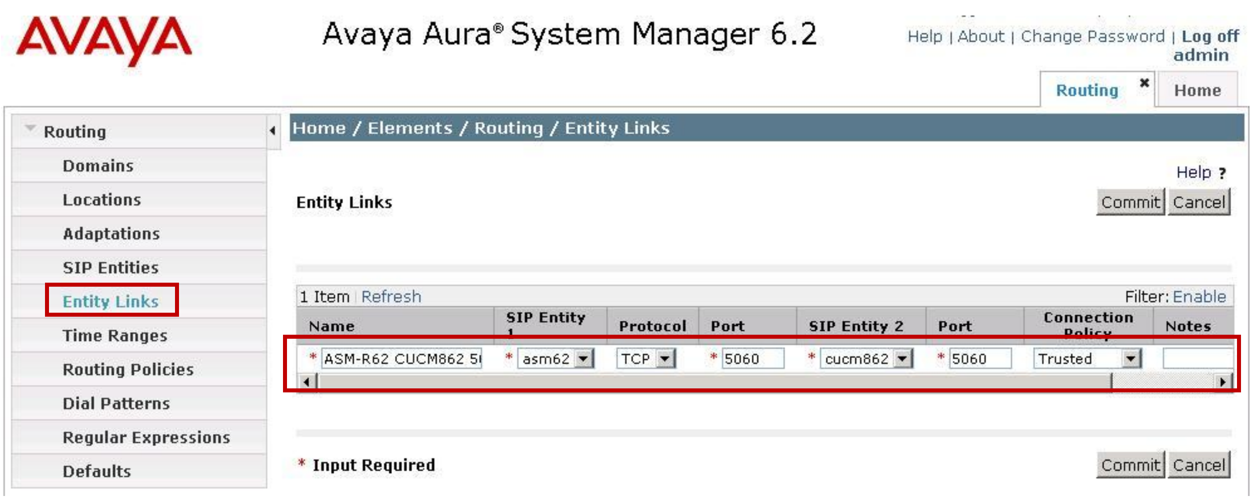
To add an Entity Link, expand **Elements → Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to CUCM system.
- **SIP Entity 1** Select SIP Entity defined for Session Manager. See **Reference [5]** in **Section 10** for more information.
- **SIP Entity 2** Select the SIP Entity defined in **Section 6.3** for CUCM system.
- **Protocol** After selecting both SIP Entities, select "**TCP"** as the required Protocol.
- **Port** Verify **Port** for both SIP entities is "**5060**".
- **Trusted** Enter .
- **Notes** Enter a brief description. [Optional].

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Session Manager and Cisco Unified Communications Manager.



Repeat this step to define an Entity Link between Session Manager and Communication Manager using the same port number as specified in **Section 5.6 Step 1**.

6.5. Define Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4.** Two routing policies must be added, one for Cisco Unified Communications Manager and a second policy for Communication Manager Element Server.

To add a routing policy, expand **Elements → Routing** and select **Routing Policies.**

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier for policy being added for CUCM system.
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional].

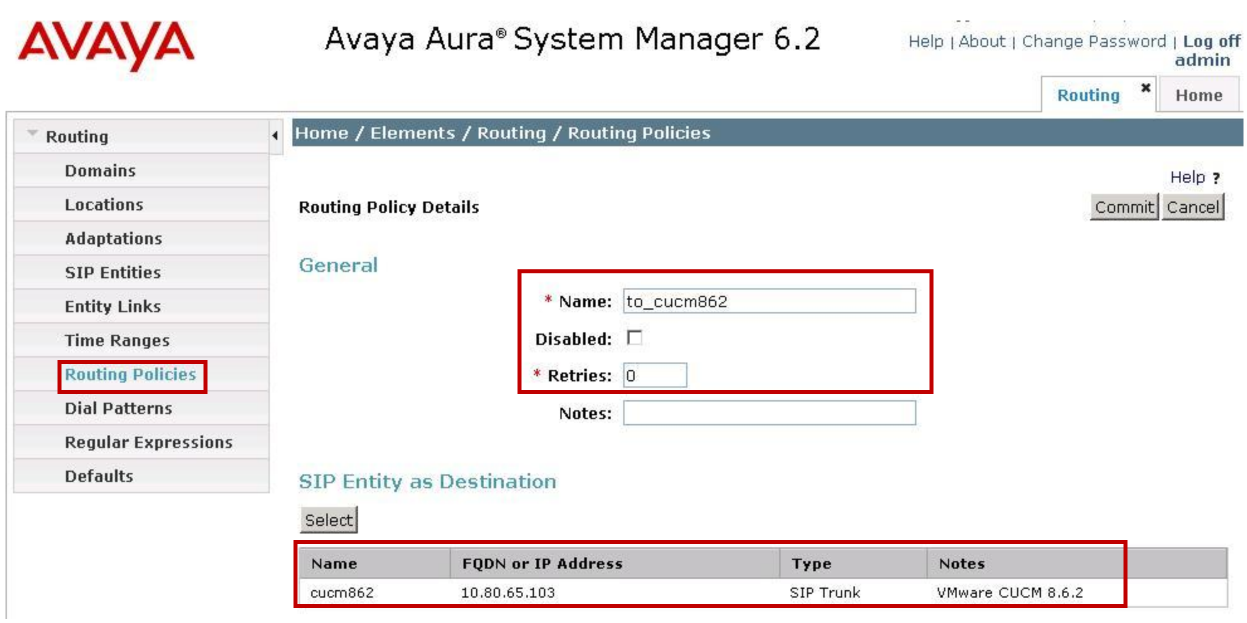
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- Select the SIP Entity defined for CUCM system in **Section 6.3** and click **Select.**
- The selected SIP Entity displays on the **Routing Policy Details** page.

Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: the routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy defined in the sample configuration for routing calls to CUCM system.



Repeat this step to define a Routing Policy for routing calls to Communication Manager.

6.6. Define Dial Pattern

Define dial patterns to direct calls to the appropriate telephony system. In the sample configuration, 4-digit extensions beginning with "30" reside on Cisco Unified Communications Manager and 4-digit extensions beginning with "40" reside on Avaya Aura® Communication Manager.

To define a dial pattern, expand **Elements → Routing** and select **Dial Patterns.**

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

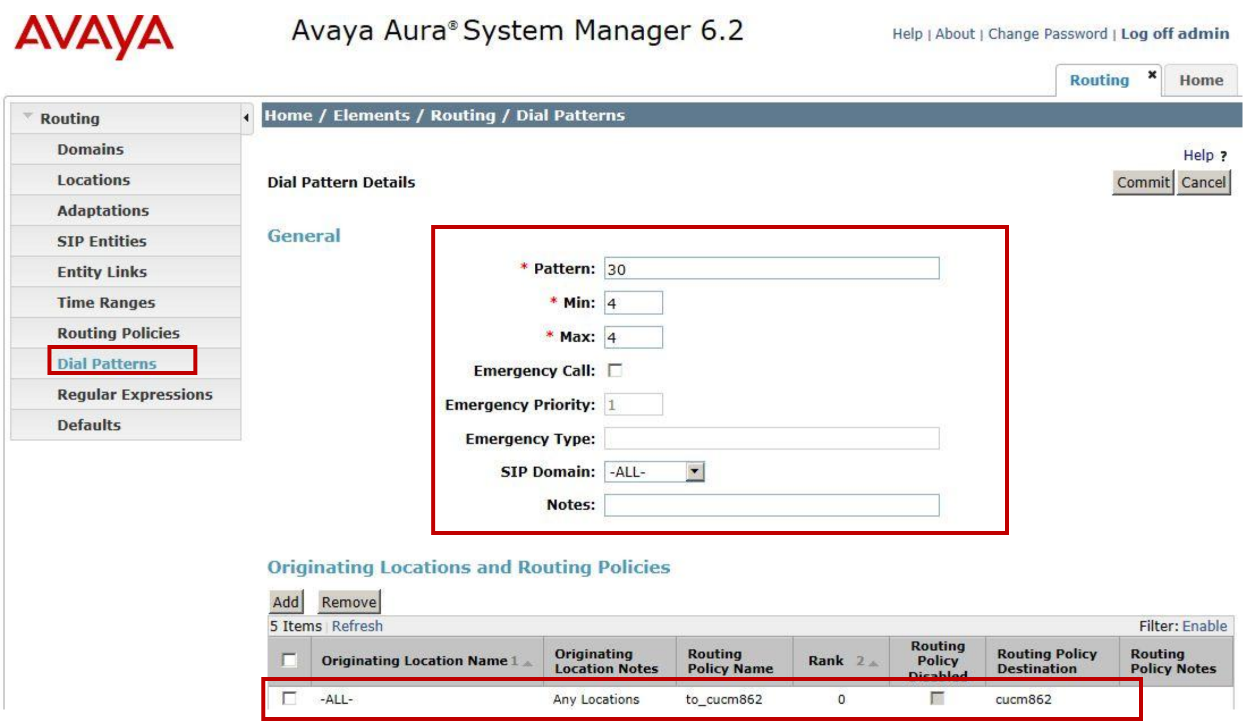
- **Pattern:** Enter dial pattern associated with CUCM system.
- **Min:** Enter the minimum number digits that must to be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select "**ALL**" if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add.**
The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select "**ALL**" .
- In **Routing Policies** table, select the appropriate Routing Policy defined for CUCM system in **Section 6.5.**
- Click **Select** to save these changes and return to **Dial Patterns Details** page.

Click **Commit** to save the new definition.

The following screen shows the Dial Pattern defined for routing calls to Cisco Unified Communications Manager.



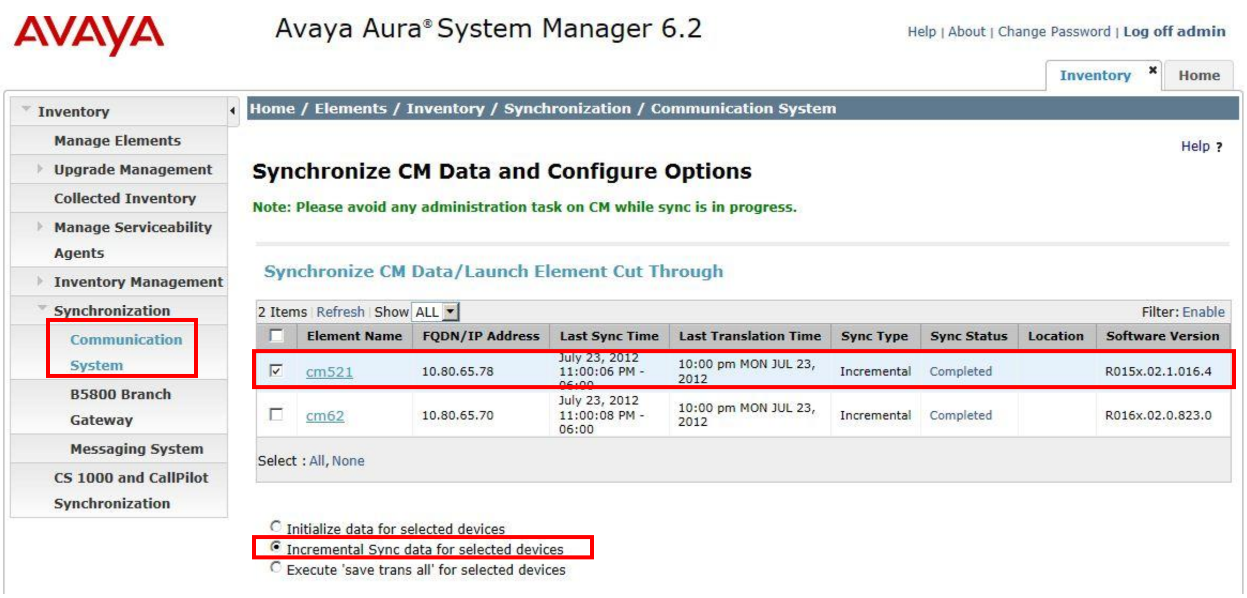
Repeat this step to define the Dial Pattern for routing calls to Communication Manager.

6.7. Synchronize Changes with Avaya Aura® Communication Manager

If changes are made on Communication Manager which alters the dial plan or numbering plan, perform on-demand synchronization to synchronize the data between System Manager and Communication Manager.

Expand **Elements → Inventory → Synchronization** and select **Communication System.**

On the **Synchronize CM Data and Configure Options** page, expand the **Synchronize CM Data/Launch Element Cut Through** table and select the row associated with Communication Manager Element Server as shown below.



Click ⦿ to select **Incremental Sync data for selected devices** option. Click **Now** (not shown) to start the synchronization.

Use the **Refresh** button in the table header to verify status of the synchronization.

Verify synchronization successfully completes by verifying the status in the **Sync. Status** column is "**Completed**".

7. Configure Cisco Unified Communications Manager

This section describes the relevant configuration of the SIP Trunk and call routing between Cisco Unified Communications Manager and Session Manager.

The following administration activities will be described:

- Verify Audio Codec Configuration
- Configure Media Termination Point
- Configure SIP Trunk Security Profile
- Configure SIP Trunk Security Profile
- Define Avaya SIP Profile
- Configure SIP Trunk to Session Manager
- Define Routing Pattern

These instructions assume the basic configuration of the Cisco Unified Communications Manager system has already been completed and the system is configured to support the SCCP (IP) and SIP telephones and associated Media Resources. For more information on how to administer these other aspects of Cisco Unified Communications Manager, see **Reference [18]** in **Section 10.**

Note: Some administration screens have been abbreviated for clarity.

Cisco Unified Communications Manager is configured using the **Cisco Unified CM Administration** web administration GUI.

Access the GUI using the URL "**http://<IP Address>:8443/ccmadmin/showHome.do**" where "**<ip-address>**" is the IP address of Cisco Unified Communications Manager.

Select the "**Cisco Unified CM Administration**" application from the **Navigation** drop-down menu.

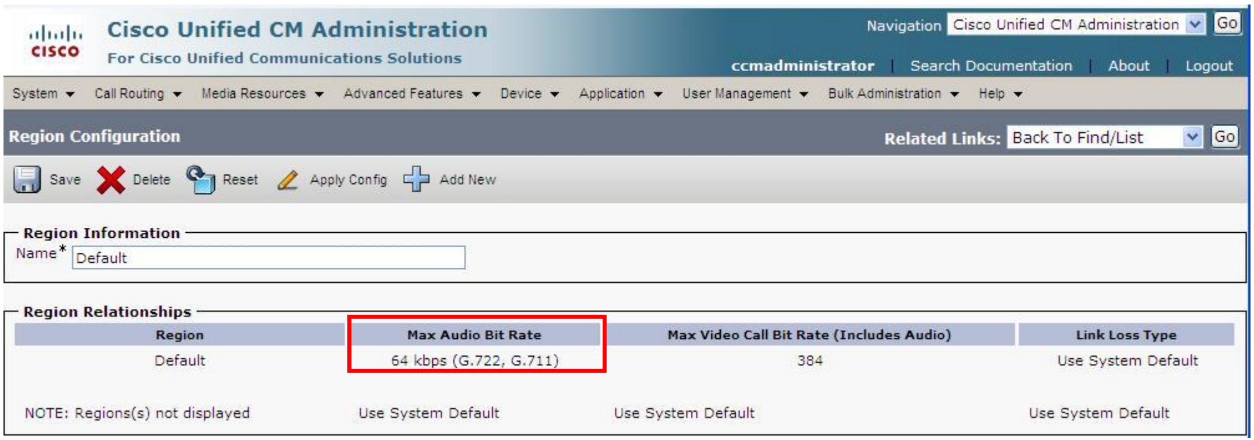
Click **Go** and login with the appropriate credentials as shown below.

7.1. Verify Audio Codec Configuration

The Audio Codec settings defined for CUCM system should match the set of Audio Codecs defined for Communication Manager in **Section 5.3**.

Expand **System** menu and select **Region.** Click **Find** (not shown) and select **Default** region.

Verify "**64 kbps (G.722, G.711)**" is displayed in the **Max Audio Bit Rate** field as shown below.



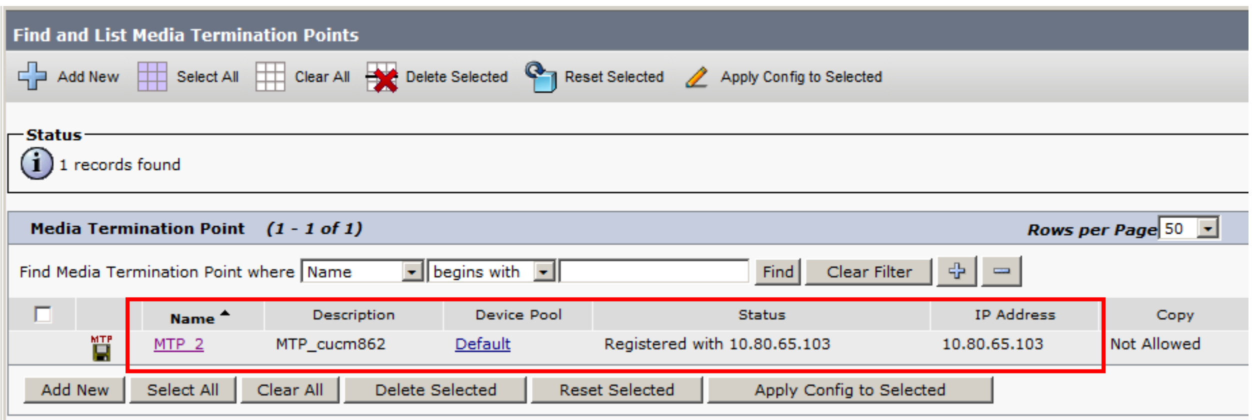
7.2. Configure Media Termination Point

Media Termination Points extend supplementary services, such as hold, transfer, call park, and conferencing that are otherwise not available when a call is routed to a SIP endpoint.

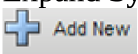
Expand **Media Resources (not shown)** and select **Media Termination Point.** Click **Find** to list available Media Termination Points. Verify at least one media termination points has been defined and verify the following fields:

- **Device Pool** Verify "**Default**" is selected.
- **Status** Verify "**Registered with <IP Address>**" is displayed where "**<IP Address>**" is the IP address of the CUCM system.
- **IP address** Verify IP address of Cisco Unified Communications Manager system.

In the sample configuration, the IP address of the Cisco Unified Communications Manager system is "**10.80.65.103**" and the default media termination point is "**MTP_2**" as shown below.



7.3. Configure Avaya SIP Trunk Security Profile

Expand **System → Security** (not shown) and select **SIP Trunk Security Profile.** Click 

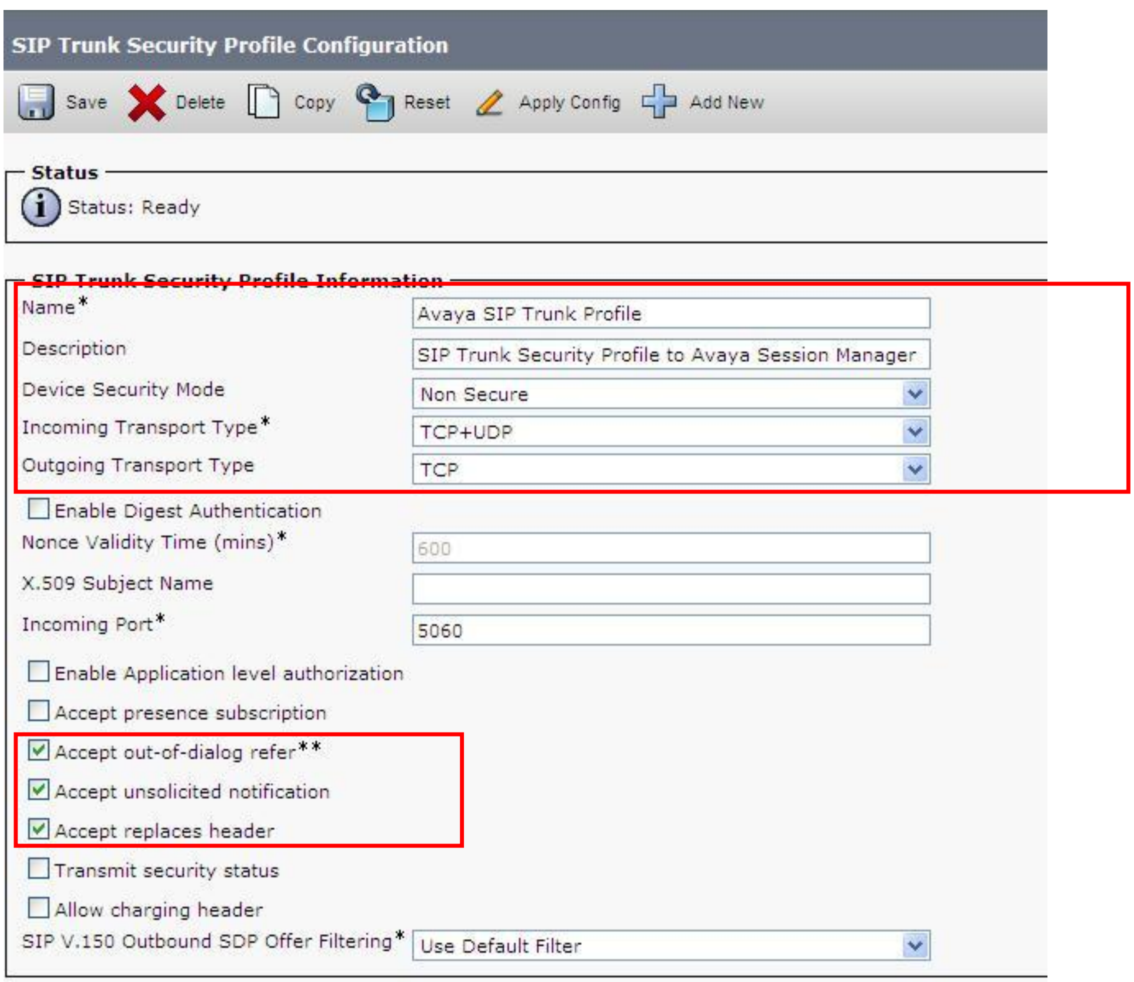
to configure a SIP Trunk Security Profile.

Enter the following values and use defaults for remaining fields:

- **Name** — Enter name.
- **Description** — Enter a brief description.
- **Device Security Mode** — Verify "**Non Secure**" is selected.
- **Incoming Transport Type** — Verify "**TCP+UDP**" is selected.
- **Outgoing Transport Type** — Verify "**TCP**" is selected.
- **Accept Out-of-Dialog REFER** — Enter  .
- **Accept Unsolicited Notification** — Enter  .
- **Accept Replaces Header** — Enter  .

Click 

. The screen below shows the SIP Trunk Security Profile for the sample configuration.



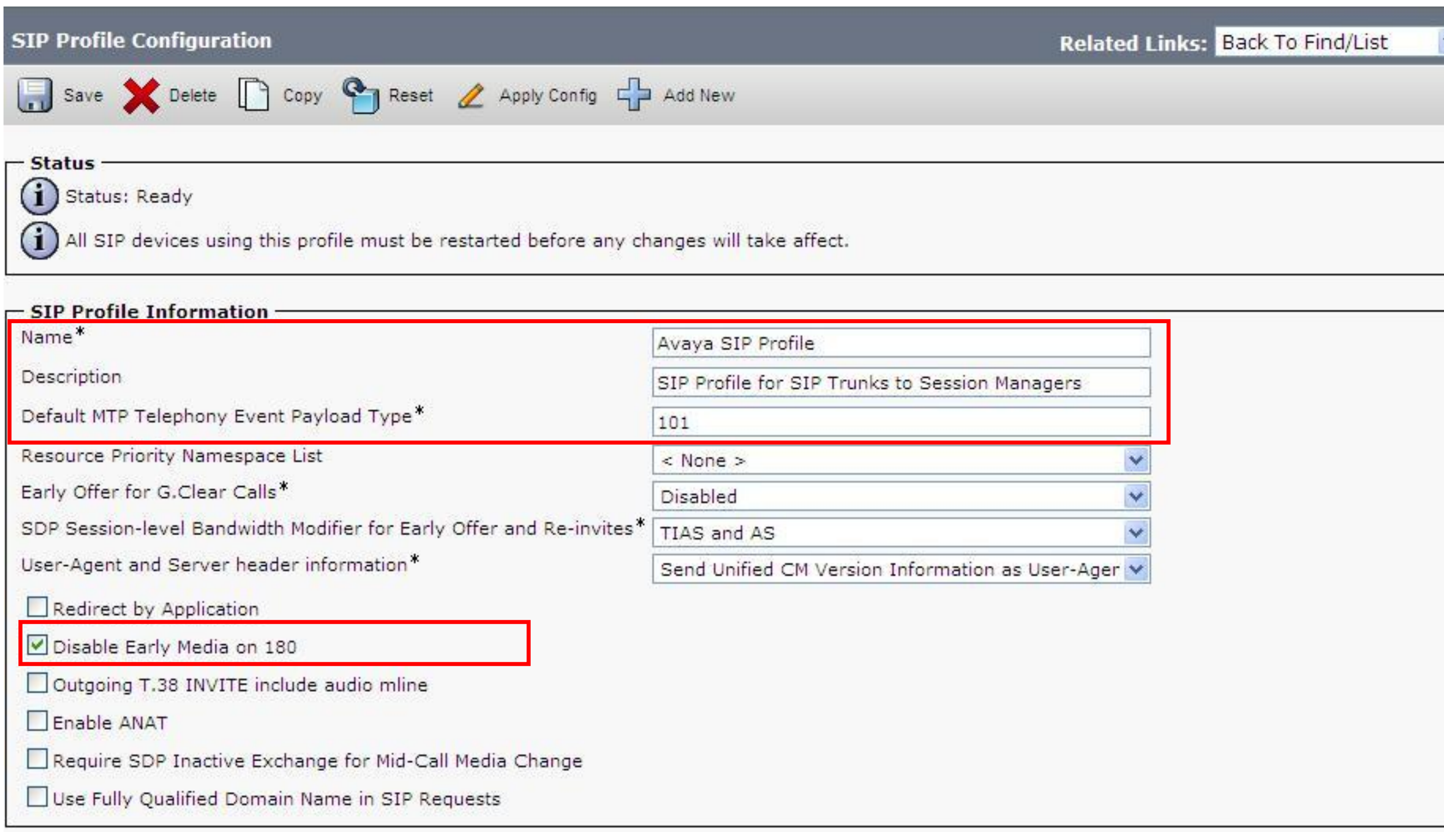
7.4. Define Avaya SIP Profile

Expand **Device → Device Settings** and select **SIP Profile.** Click Add New.

Under **SIP Profile Information** section, enter the following values and use defaults for remaining fields:

- **Name** Enter name.
- **Description** Enter a brief description.
- **Default MTP Telephony Event Payload Type** Enter "**101**".
- **Disable Early Media on 180** Enter ☑.

Click Save. The screen below shows SIP Profile for the sample configuration.



7.5. Define SIP Trunk to Avaya Aura® Session Manager

Expand **Device** select **Trunk** (not shown) Click 

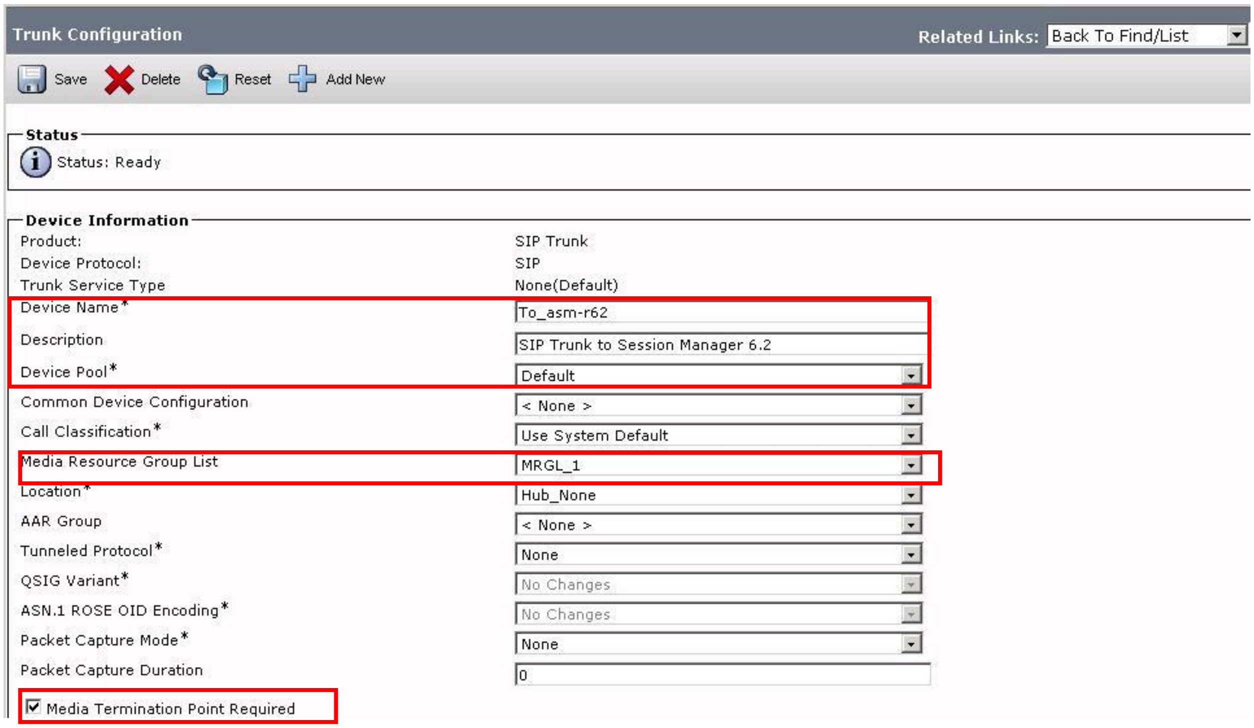
to define a SIP Trunk to Session Manager.

Under **Trunk Information** section, enter the following values as shown below and click **Next.**

- **Truck Type** Select "**SIP Trunk**".
- **Device Protocol** Defaults to "**SIP**".
- **Trunk Service Type** Defaults to "**None**".

Under **Device Information** section, enter the following values and use defaults for remaining fields as shown below:

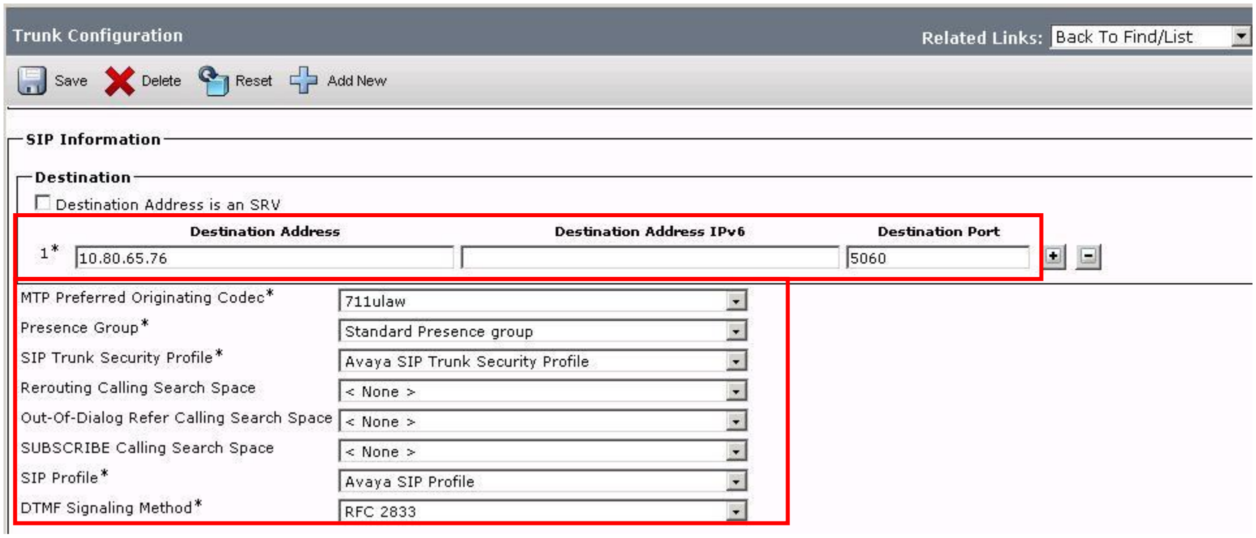
- **Device Name** — Enter name.
- **Description** — Enter a brief description.
- **Device Pool** — Select "**Default**".
- **Media Resource Group List** — Select previously defined Media Resource Group List. See **References [18]** thru **[20]** in **Section 10** for more information.
- **Media Termination Point Required** — Enter .



Scroll to **SIP Information** section, enter the following values and use defaults for remaining fields:

- **Destination Address** — Enter IP address of SIP signaling interface for Session Manager.
- **Destination Port** — Defaults to "**5060**".
- **MTP Preferred Originating Codec** — Select "**711ulaw**".
- **SIP Trunk Security Profile** — Select SIP Trunk Security Profile defined in **Section 7.3**.
- **SIP Profile** — Select SIP Profile defined in **Section 7.4**.
- **DTMF Signaling Method** — Select "**RFC 2833**".

Click **Save.** The screen below shows SIP Information defined for SIP Trunk to Session Manager for the sample configuration.



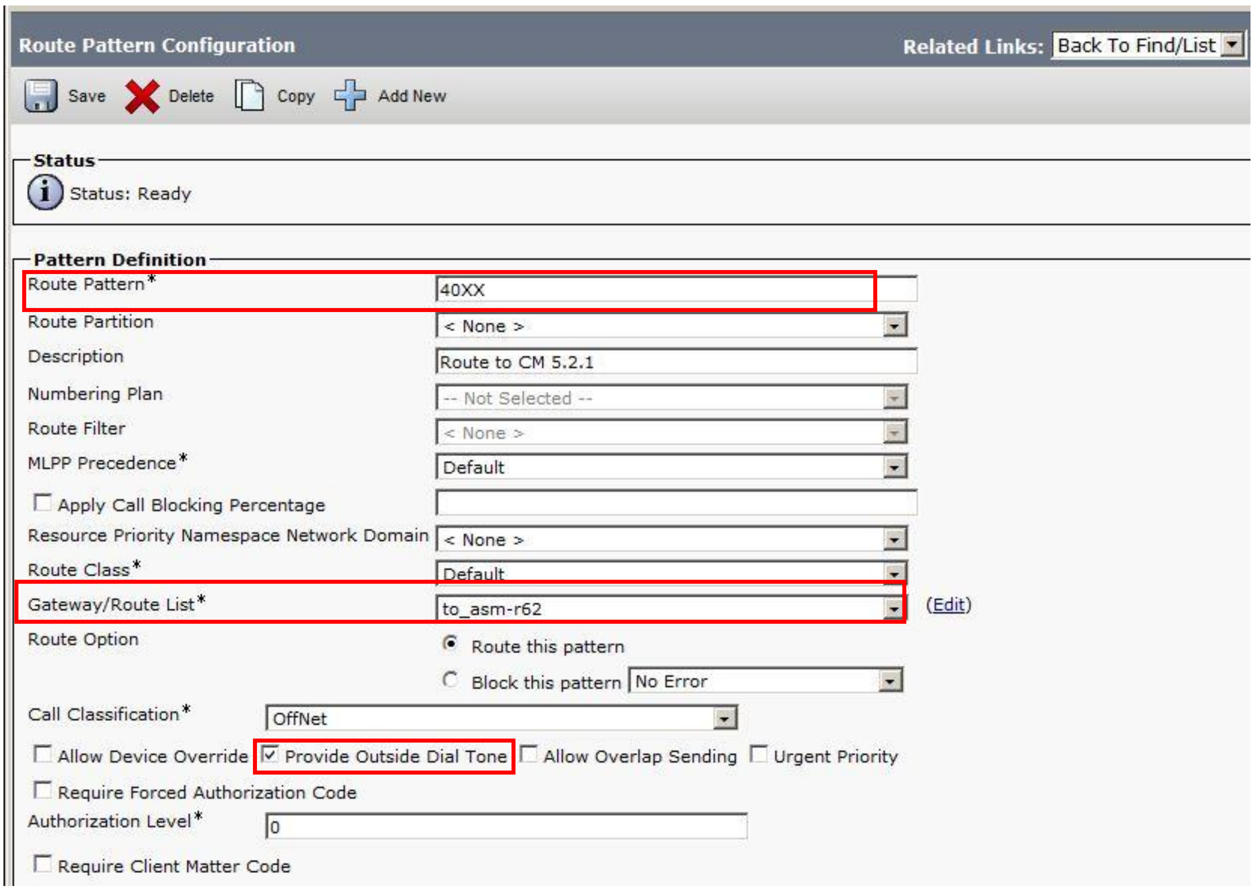
7.6. Define Routing Pattern

Expand **Call Routing → Route/Hunt** select **Route Pattern** (not shown).

Click  to configure new Route Pattern. Enter the following values as shown below and use defaults for remaining fields.

- **Route Pattern** Enter dialed digits for calls routed to Session Manager. For sample configuration, "**40XX**" was used.
- **Description** Enter brief description [Optional].
- **Gateway/Route List** Select name of SIP trunk defined in **Section 7.5.**
- **Provide Outside Dial Tone** Enter .

Click **.** The screen below shows Route Pattern defined for the sample configuration to route calls to Session Manager.



8. Verification Steps

8.1. Verify Avaya Aura® Session Manager Configuration

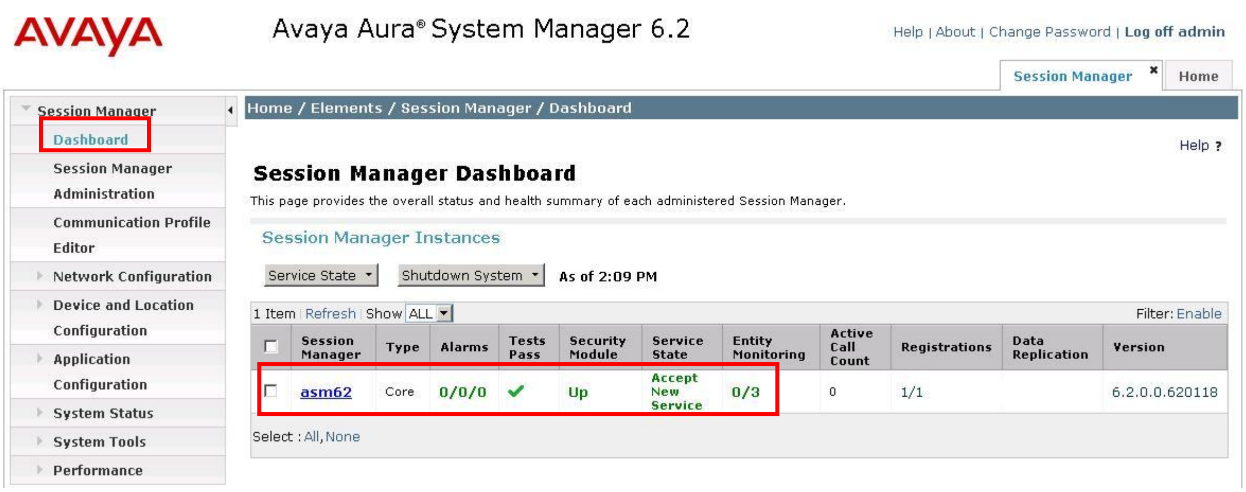
Step 1: Verify Avaya Aura® Session Manager is Operational

Expand **Elements → Session Manager** and select **Dashboard** to verify the overall system status of Session Manager.

In the sample configuration, "**asm62**" was the name of the SIP Entity defined for the Session Manager used for testing with Cisco Unified Communications Manager.

Verify the correct status of the following fields is displayed as shown below.

- **Tests Pass**
- **Security Module**
- **Service State**

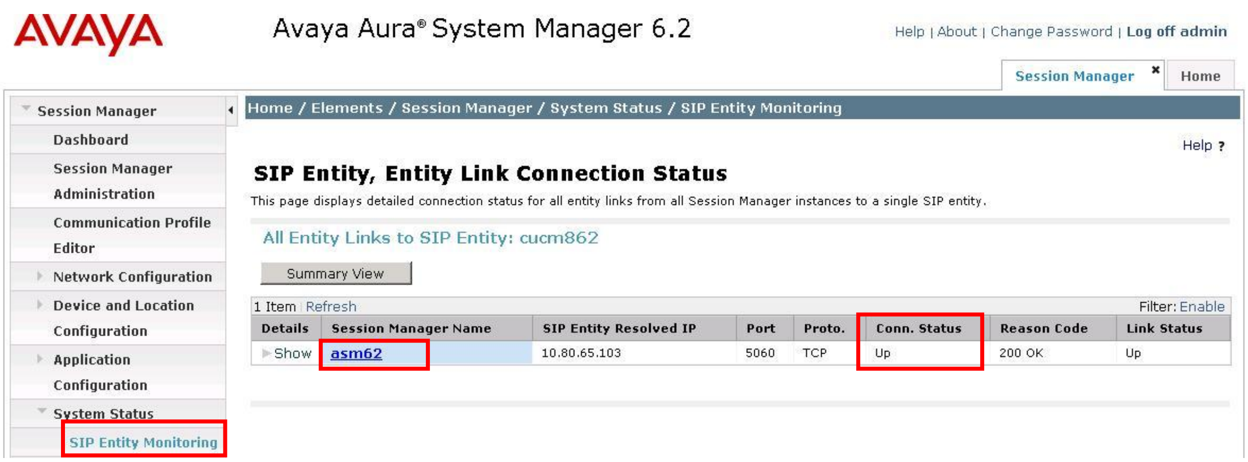


Step 2: Verify SIP Entity Link Status

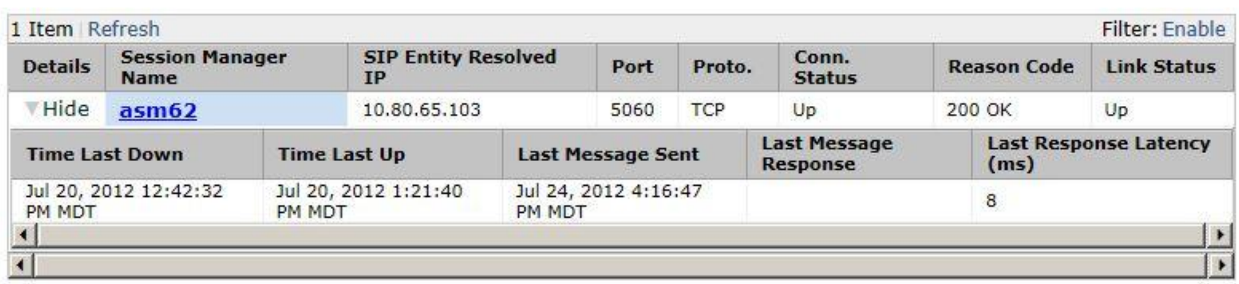
Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** to view more detailed status information for the specific SIP Entity Links used for calls between Communication Manager and Cisco Unified Communications Manager.

Select the SIP Entity for Cisco Unified Communications Manager from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

Verify the **Conn. Status** is "**Up**" as shown below:



Click **Show** to view more information associated with the Entity Link.



Repeat this step to verify the status of the Entity Link to Communication Manager.

8.2. Verify Avaya Aura® Communication Manager Operational Status

Step 1: Verify status of SIP trunk between Communication Manager and Session Manager.

Verify the status of the SIP trunk group by using the **status trunk n** command, where **n** is the trunk group number administered in **Section 5.6.**

Verify that all trunks in the trunk group are in the "**in-service/idle**" state as shown below:

```
status trunk 10
                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy
0010/001 T00001   in-service/idle    no
0010/002 T00002   in-service/idle    no
0010/003 T00003   in-service/idle    no
0010/004 T00004   in-service/idle    no
0010/005 T00005   in-service/idle    no
0010/006 T00006   in-service/idle    no
0010/007 T00007   in-service/idle    no
0010/008 T00008   in-service/idle    no
0010/009 T00009   in-service/idle    no
0010/010 T00010   in-service/idle    no
```

Verify the status of the SIP signaling group by using the **status signaling-group** command, where **n** is the signaling group number administered in **Section 5.6.**

Verify the status of the **Group State** field is "**in-service**" shown below:

```
status signaling-group 10
                         STATUS SIGNALING GROUP

        Group ID: 10
      Group Type: sip

     Group State: in-service
```

Step 2: Verify calls to stations supported by CUCM system are correctly routed over the SIP trunk to Session Manager.

Use the SAT command, **list trace tac #**, where **tac #** is the trunk access code for the SIP trunk group defined in **Section 5.6** to trace trunk group activity. For example, the trace below illustrates a call from an h.323 endpoint using "**4002**" on Communication Manager" to a SCCP station on Cisco Unified Communications Manager using "**3002**".

```
list trace tac #10                                           Page   1
                                LIST TRACE
time                data

18:41:36     Calling party station      4002 cid 0x835
18:41:36     Calling Number & Name 4002 4002, user
18:41:36     dial 3002 route:UDP|AAR
18:41:36     term trunk-group 10      cid 0x835
18:41:36     dial 3002 route:UDP|AAR
18:41:36     route-pattern  10 preference 1 location 1/ALL  cid 0x835
18:41:36     seize trunk-group 10 member 3    cid 0x835
18:41:36     Calling Number & Name NO-CPNumber NO-CPName
18:41:36 SIP>INVITE sip:3002@avaya.com;user=phone SIP/2.0
18:41:36     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:36     Setup digits 3002
18:41:36     Calling Number & Name 4002 4002, user
18:41:36 SIP<SIP/2.0 100 Trying
18:41:36     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:36     Proceed trunk-group 10 member 3    cid 0x835
18:41:36 SIP<SIP/2.0 180 Ringing
18:41:36     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:36     Alert trunk-group 10 member 3    cid 0x835
18:41:41 SIP<SIP/2.0 200 OK
18:41:41     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:41 SIP>ACK sip:3002@10.80.65.103:5060;transport=tcp SIP/2.0
18:41:41     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:41     active trunk-group 10 member 3    cid 0x835
18:41:41     G711MU ss:off ps:20
             rgn:1 [10.80.65.103]:26026
             rgn:1 [10.80.65.79]:2052
18:41:41     xoip options: fax:T38 modem:off tty:US  uid:0x50003
             xoip ip: [10.80.65.79]:2052
18:41:41 SIP>INVITE sip:3002@10.80.65.103:5060;transport=tcp SIP/2.0
18:41:41     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:41 SIP<SIP/2.0 100 Trying
18:41:41     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:41 SIP<SIP/2.0 200 OK
18:41:41     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:41     G711MU ss:off ps:20
             rgn:1 [10.80.64.50]:2920
             rgn:1 [10.80.65.103]:26030
18:41:41 SIP>ACK sip:3002@10.80.65.103:5060;transport=tcp SIP/2.0
18:41:41     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:41     G711MU ss:off ps:20
             rgn:1 [10.80.65.103]:26030
             rgn:1 [10.80.64.50]:2920
18:41:43 SIP>BYE sip:3002@10.80.65.103:5060;transport=tcp SIP/2.0
```

```
18:41:43     Call-ID: 0f0b4b11ad8e11f19d4feecfa00
18:41:43     idle station      4002 cid 0x835
             rgn:1 [192.45.130.100]:28544
             rgn:1 [10.80.111.170]:2054
```

8.3. Verify Cisco Unified Communications Manager Operational Status

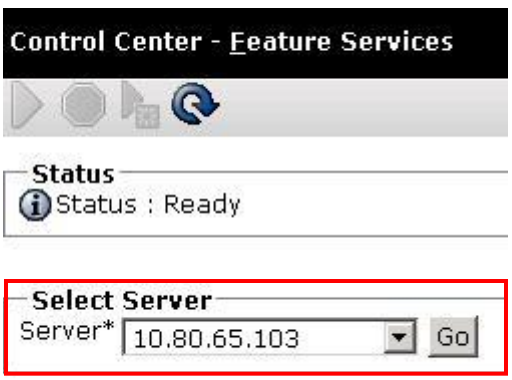
Step 1: Verify the operational status of the Cisco Unified Communications Manager system.

From the Cisco Unified CM Administration Home Page described in **Section 7**, select the "**Cisco Unified Serviceability**" application (not shown) to verify status of the Cisco system.

Expand **Tools** (not shown) and select **Control Center – Feature Services**.

Under **Select Server** section, select the IP address of the Cisco Unified Communications Manager system and click **Go** to view status of the system.

In the sample configuration, the IP address for the CUCM system is displayed as shown below.



Under **CM Services** section, verify the status of the **Cisco CallManager** and **Cisco IP Voice Media Streaming App** services as shown below. Verify the following fields:

- **Status** Verify "**Started**" is displayed.
- **Activation Status** Verify "**Activated**" is displayed.

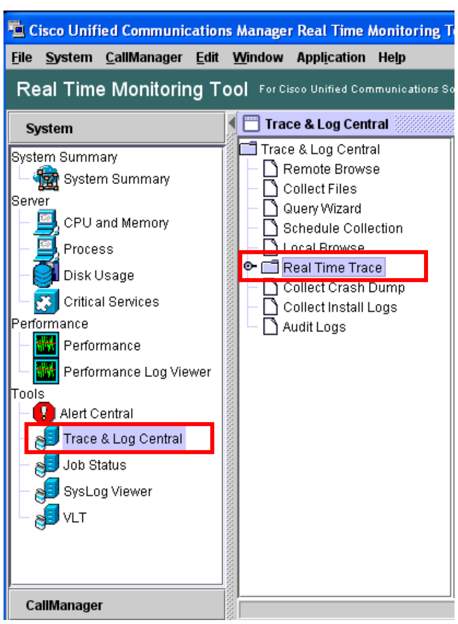
CM Services

	Service Name	Status	Activation Status
	Cisco CallManager	Started	Activated
	Cisco Messaging Interface	Not Running	Activated
	Cisco Unified Mobile Voice Access Service	Started	Activated
	Cisco IP Voice Media Streaming App	Started	Activated

Step 2: Use the Real Time Monitoring Tool (RTMT) to monitor events on CUCM system.

This tool can be downloaded by expanding **Application → Plugins** from the Cisco Unified CM Administration web interface. For further information, see **Reference [18**] in **Section 10**.

Start the tool. Expand **Tools** on left panel and select **Trace & Log Central**. Under **Trace and Log Central** section, select **Real Time Trace** to start a real time data capture as shown below.



8.4. Call Scenarios Verified

Verification scenarios for the configuration described in these Application Notes included the following call scenarios:

Station to Station Calls:

- Using G.711 audio codec, verify displays and talk path for calls between different types of stations on Avaya Aura® Communication Manager and stations on Cisco Unified Communications Manager.
- Using G.729 audio codec, verify displays and talk path for calls between different types of stations on Avaya Aura® Communication Manager and stations on Cisco Unified Communications Manager.
- Verify a second call can be made between different types of stations on Avaya Aura® Communication Manager and stations on Cisco Unified Communications Manager after the first call is abandoned.

Supplemental Calling Features:

- Verify calls from different types of stations on Avaya Aura® Communication Manager to a station on Cisco Unified Communications Manager can be placed on hold.
- Verify calls from different types of stations on Avaya Aura® Communication Manager to a station on Cisco Unified Communications Manager can be transferred to another station on the same switch or back across the SIP trunk to a station on the remote switch.
- Verify calls from different types of stations on Avaya Aura® Communication Manager to a station on Cisco Unified Communications Manager can create a conference with another station on either the same switch or remote switch.
- Verify calls from different types of stations on Avaya Aura® Communication Manager to a station on Cisco Unified Communications Manager can be forwarded to another station on the same switch or back across the SIP trunk to a station on the remote switch.
- Repeat the hold, transfer, conference and forward scenarios with calls originating from a station on Cisco Unified Communications Manager.

9. Conclusion

These Application Notes describe how to configure a network that provides SIP trunks between Avaya Aura® Session Manager Release 6.2, Cisco Unified Communications Manager Release 8.6.2 and Avaya Aura® Communication Manager Release 5.2.1. Avaya Aura® Communication Manager serves as a Element Server within the Avaya Aura® architecture and supports Avaya 9600 Series and 96x1 Series IP Deskphones (H.323) and 2410 Digital Telephones are supported by Avaya Aura® Communication Manager.

10. Additional References

Avaya Product documentation relevant to these Application Notes is available at

Avaya Aura® Session Manager

1) Avaya Aura® Session Manager Overview, Doc ID 03-603323.
2) Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473. http://support.avaya.com.
3) Avaya Aura® Session Manager Case Studies, Doc ID 03-603478.
4) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325.
5) Administering Avaya Aura® Session Manager, Doc ID 03-603324.

Avaya Aura® Communication Manager

6) Administering Avaya Aura® Communication Manager, Doc ID 03-300509.
7) Avaya Aura® Communication Manager Screen Reference, Doc ID 03-602878.
8) Avaya Toll Fraud and Security Handbook, Doc ID 555-025-600.

Avaya 9600 Series and 9601 Series IP Deskphones

9) Avaya one-X® Deskphone SIP Administrator Guide. December 6, 2010.
10) Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6.
11) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.2 for 9601 IP Deskphone.
12) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.0 for 9608, 9611G, 9621G and 9641G IP Deskphones.
13) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 2.6.

Avaya Application Notes

14) Configuring SIP trunks among Avaya Aura® Session Manager Release 6.1, Avaya Aura® Communication Manager Release 6.0.1 and Cisco Unified Communications Manager Release 8.0.3
15) Configuring SIP trunks among Avaya Aura® Session Manager Release 6.1, Avaya Aura® Communication Manager Release 6.0.1 and Cisco Unified Communications Manager Release 8.0.3.
16) Configuring SIP Trunks between Avaya Aura® Session Manager Release 6.2, Avaya Aura® Communication Manager Release 6.2 and Cisco Unified Communications Manager Release 8.6.2 – Issue 1.0
17) Integrating Avaya Aura® Session Manager Release 6.2, Avaya Modular Messaging Release 5.2 and Cisco Unified Communications Manager Release 8.6.2 – Issue 1.0

Cisco Unified Communications Manager

Cisco Product documentation relevant to these Application Notes is available at http://www.cisco.com .

18) Cisco Unified Communications Manager Administration Guide, Release 8.6(1), Part Number: OL-24919-01.
19) Cisco Unified Communications Manager Features and Services Guide, Part Number: OL-24921-01.
20) Cisco Unified Real-Time Monitoring Tool Administration Guide, Part Number: OL-24544-01.

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