Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Hawaiian Telecom SIP Trunk Service with Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3 and Avaya Session Border Controller for Enterprise Rel. 6.2 – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between the service provider Hawaiian Telecom and an Avaya SIP-enabled enterprise solution. The Avaya SIP-enabled enterprise solution consists of Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3, Avaya Session Border Controller for Enterprise Rel. 6.2, and various Avaya endpoints.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

Hawaiian Telecom SIP Trunk Service provides PSTN access via SIP trunks between the enterprise and Hawaiian Telecom's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the service provider Hawaiian Telecom and an Avaya SIP-enabled enterprise solution.

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of an Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3, Avaya Session Border Controller for Enterprise Rel. 6.2, and various Avaya endpoints. This solution does not extend to configurations without the Avaya Session Border Controller for Enterprise or Avaya Aura® Session Manager.

Customers using Avaya SIP-enabled enterprise solution with Hawaiian Telecom SIP Trunk service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional analog trunks and/or PSTN trunks such as ISDN-PRI. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting an Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to the Hawaiian Telecom SIP Trunk service via the public internet, as depicted in **Figure 1.**

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability, the following areas were tested for compliance:

- SIP trunk registration with the service provider
- Incoming calls from the PSTN were routed to the DID numbers assigned by Hawaiian Telecom. Incoming PSTN calls were terminated to the following end points: Avaya 9600 Series IP Telephones (SIP), Avaya 9600 Series IP Telephones (H.323), Avaya 2420 Digital Telephones, Avaya one-X® Communicator (H.323 and SIP modes), analog telephones and Fax machines.
- Outgoing calls to the PSTN were routed via Hawaiian Telecom's network to the various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (with voicemail off).

- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Note: Testing was perfomed with G.711MU, G.711A and G.729A codecs.
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- International calls.
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call transfers.
- Station Conference.
- T.38 fax support (inbound).
- G.711Mu fax pass-through support (outbound).
- EC500 (Extension to Cellular call redirection).
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

Items not supported or not tested included the following:

- Inbound toll-free calls were not tested.
- 0, 0+10, 911.

2.2. Test Results

Interoperability testing of Hawaiian Telecom SIP trunk service with Avaya SIP-enabled enterprise solution was completed successfully with the following observations/limitations.

- **Call Display on Transferred Calls to PSTN** – Caller ID display is not updated on PSTN phones involved with call transfers from Avaya Aura® Communication Manager to the PSTN. After the call transfer is completed, the PSTN phone does not display the actual connected party but instead shows the ID of the host extension that initiated the call transfer. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/Hawaiian Telecom solution. It is listed here simply as an observation.
- **T.38 Fax:** T.38 fax from the enterprise to the PSTN (outbound) is not supported by Hawaiian Telecom; Hawaiian Telecom only supports T.38 fax from the PSTN to the enterprise (inbound). Fax calls from the Enterprise to the PSTN (outbound) defaulted to G.711 pass-through.

- **Calls to Busy Numbers:** Hawaiian Telecom's network is not sending "486 Busy Here" for calls from the enterprise to busy PSTN numbers. Since Busy Tone is heard by the user this observation is considered non critical.
- **Outbound Calling Party Number (CPN) Block (Privacy):** To support outbound privacy calls (calling party number block), Avaya Aura® Communication Manager sends "anonymous" as the calling number in the SIP From header, uses the P-Asserted-Identity (PAI) header to identify the actual calling party number and includes "Privacy: id" in the INVITE message. During the testing Hawaiian Telecom's network was configured not to pass the PAI header, thus on outbound calls (from Communication Manager to the PSTN) with privacy enabled Hawaiian Telecom will respond with "604 Does Not exist anywhere".

2.3. Support

For support on Hawaiian Telecom systems, call Toll Free at 1-808-643-0944 or visit the corporate Web page at: https://www.hawaiiantel.com/business/Business.aspx

3. Reference Configuration

Figure 1 below illustrates the test configuration used. The test configuration simulates an enterprise site with Avaya SIP-enabled enterprise solution connected to the Hawaiian Telecom SIP trunk service through the public internet.

The Avaya components used to create the simulated customer site included:

- Avaya S8300 Server running Avaya Aura® Communication Manager.
- Avaya G450 Media Gateway.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® Session Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® System Manager.
- Dell R210 V2 Server running Avaya Session Border Controller for Enterprise.
- Avaya 9600-Series IP Telephones (H.323).
- Avaya 9600-Series IP Telephones (SIP).
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya 2420 Digital telephones.
- Analog Telephones.
- Fax machines.
- Desktop PC running various administration interfaces.

Located at the edge of the enterprise is the Avaya Session Border Controller for Enterprise. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya Session Border Controller for Enterprise. In this way, the Avaya Session Border Controller for Enterprise can protect the enterprise against any SIP-based attacks. The Avaya Session Border Controller for Enterprise provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya Session Border Controller for Enterprise and Hawaiian Telecom across the public IP network is SIP over UDP. The transport protocol between the Avaya Session Border Controller for Enterprise and Avaya Aura® Session Manager across the

enterprise IP network is SIP over TCP. The transport protocol between Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the enterprise IP network is SIP over TLS. For ease of troubleshooting during testing, the compliance test was conducted with the Transport Method set to **tcp** between Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

For security reasons, any actual public IP addresses used in the configuration have been masked. Similarly, any references to real routable PSTN numbers have also been masked to numbers that cannot be routed by the PSTN.

One SIP trunk group was created between the Avaya Aura® Communication Manager and the Avaya Aura® Session Manager to carry the traffic to and from the service provider (two-way trunk group). To separate the codec settings required by the service provider from the codec used by the telephones, two IP network regions were created, each with a dedicated signaling group. For inbound calls, the calls flowed from the service provider to Avaya Session Border Controller for Enterprise then to Avaya Aura® Session Manager. Avaya Aura® Session Manager used the configured dial patterns and routing policies to determine the recipient (in this case Avaya Aura® Communication Manager) and on which link to send the call. Once the call arrived at Avaya Aura® Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions could be performed.

Outbound calls to the PSTN were first processed by Avaya Aura® Communication Manager for outbound feature treatment such as Automatic Route Selection (ARS) and Class of Service restrictions. Once Avaya Aura® Communication Manager selected the proper SIP trunk; the call is routed to Avaya Aura® Session Manager. The Avaya Aura® Session Manager once again used the configured dial patterns and routing policies to determine the route to the Avaya Session Border Controller for Enterprise for egress to Hawaiian Telecom's network.

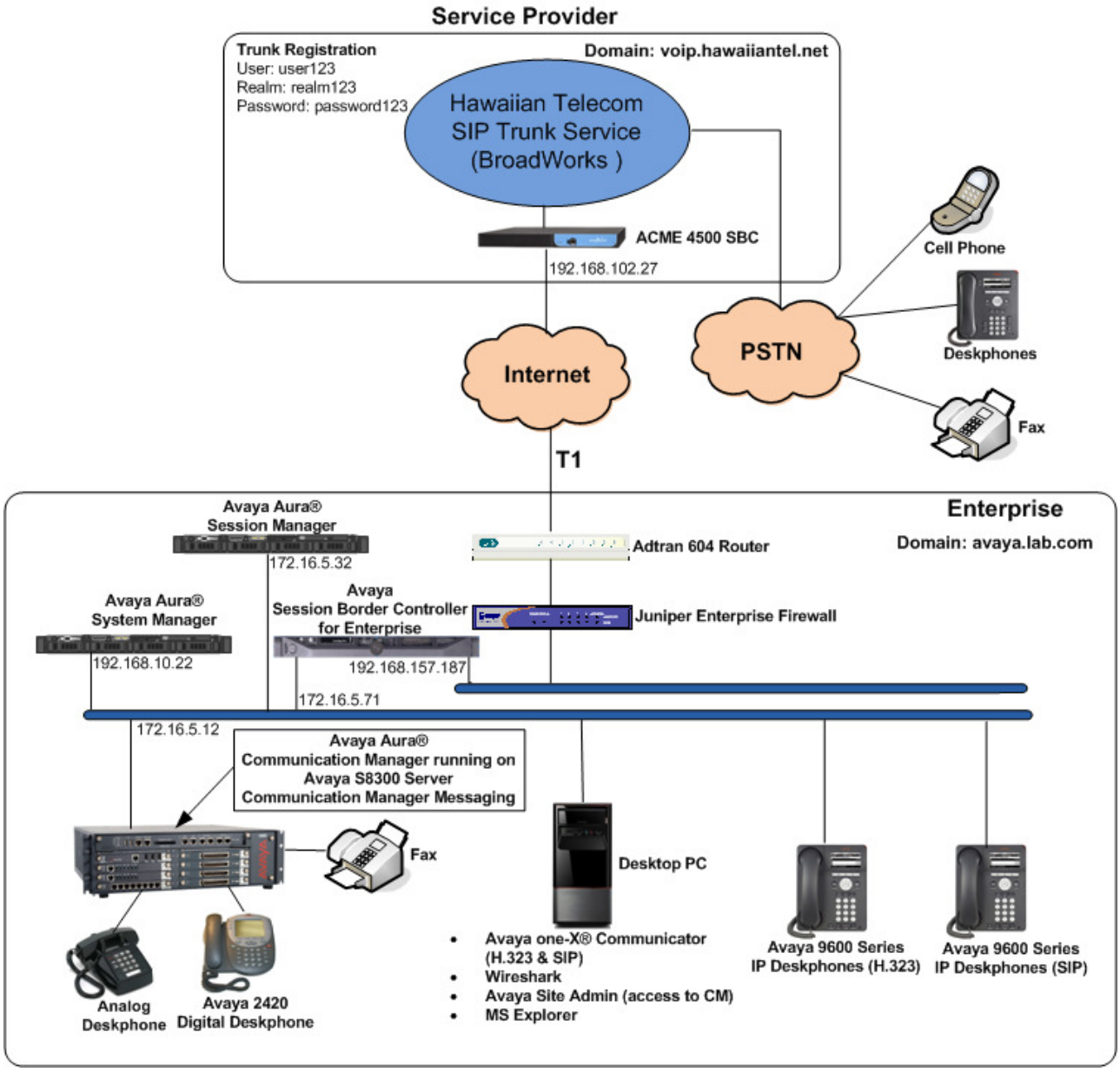


Figure 1: Avaya SIP-enabled Enterprise Solution and Hawaiian Telecom SIP Trunk Service

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on an Avaya S8300Server.	6.3.0 SP0 (03.0.124.0-20553)
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 1 (6.3.1.0.631004)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 1 Build No. 6.3.0.8.5682-6.3.8.859 Software Update Rev. No. 6.3.1.9.1212
G450 Gateway	33.13.0
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.0.Q36
Avaya Aura® Integrated Management Site Administrator	6.0.07
Avaya Aura® Communication Manager Messaging (CMM)	CMM 6.3 SP0
Avaya one-X® Communicator (SIP & H.323)	6.1.8.06-SP8-40314
Avaya 9600 Series IP Telephones (H.323)	Avaya one-X® Desk phone Edition Version S3.2
Avaya 9600 Series IP Telephones (SIP)	Avaya one-X® Deskphone SIP Version 2.6.9.1
Avaya 2420 Series Digital Phone	--
Lucent Analog Phone	--
Fax Machines	--
Hawaiian Telecom	
BroadWorks	17 SP3
ACME Session Border Controller (4500)	SCX 6.2.0 MR11

Table 2 – Hardware and Software Components Tested

The specific configuration above was used for the compliance testing. Note that this solution is compatible with other Avaya Servers and Media Gateway platforms running similar versions of Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Avaya Aura® Communication Manager. A SIP trunk is established between Avaya Aura® Communication Manager and Avaya Aura® Session Manager for use by signaling traffic to and from Hawaiian Telecom. It is assumed the general installation of Avaya Aura® Communication Manager, Avaya G450 Media Gateway and Avaya Aura® Session Manager has been previously completed.

In configuring the Avaya Aura® Communication Manager, various components such as ip-network-regions, signaling groups, trunk groups, etc. need to be selected or created for use with the SIP connection to the service provider. Unless specifically stated otherwise, any unused ip-network-region, signaling group, trunk group, etc. can be used for this purpose.

The Avaya Aura® Communication Manager configuration was performed using Avaya Integrated Management Site Administrator. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the public IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise, including any trunks to the service provider. The example shows one license with a capacity of 4000 trunks are available and 22 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

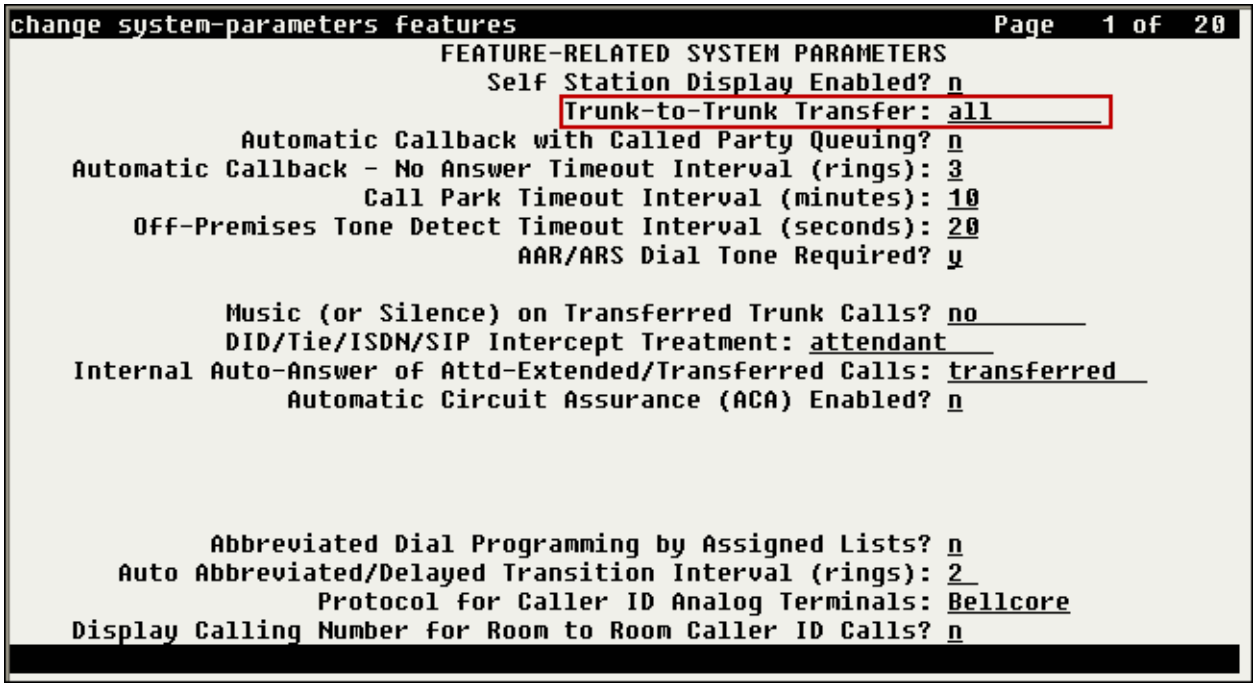
```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                               USED
                     Maximum Administered H.323 Trunks: 4000     10
          Maximum Concurrently Registered IP Stations: 2400     1
            Maximum Administered Remote Office Trunks: 4000     0
Maximum Concurrently Registered Remote Office Stations: 2400     0
              Maximum Concurrently Registered IP eCons: 68       0
  Max Concur Registered Unauthenticated H.323 Stations: 100      0
                       Maximum Video Capable Stations: 2400     0
                   Maximum Video Capable IP Softphones: 2400     2
                      Maximum Administered SIP Trunks: 4000     22
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000     0
   Maximum Number of DS1 Boards with Echo Cancellation: 80       0
                             Maximum TN2501 VAL Boards: 10       0
                     Maximum Media Gateway VAL Sources: 50       1
          Maximum TN2602 Boards with 80 VoIP Channels: 128      0
         Maximum TN2602 Boards with 320 VoIP Channels: 128      0
   Maximum Number of Expanded Meet-me Conference Ports: 300      0

       (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System Features

Use the **change system-parameters feature** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to **none**.



On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both.

```
change system-parameters features                              Page   9 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code: ___
          International Access Code: _____

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

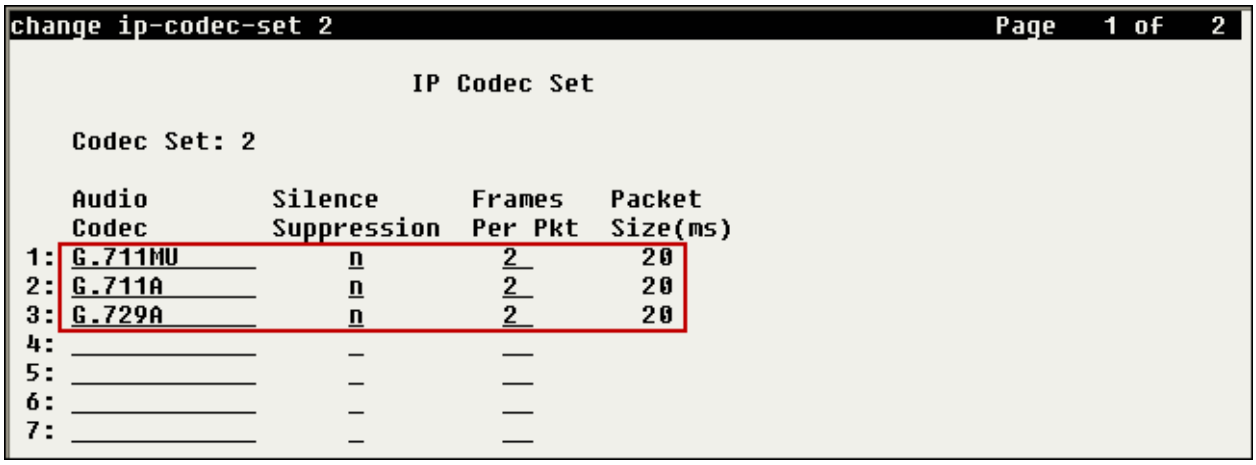
5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8300D Server running Avaya Aura® Communication Manager (**procr**) and for Avaya Aura® Session Manager (**Lab-HG-SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

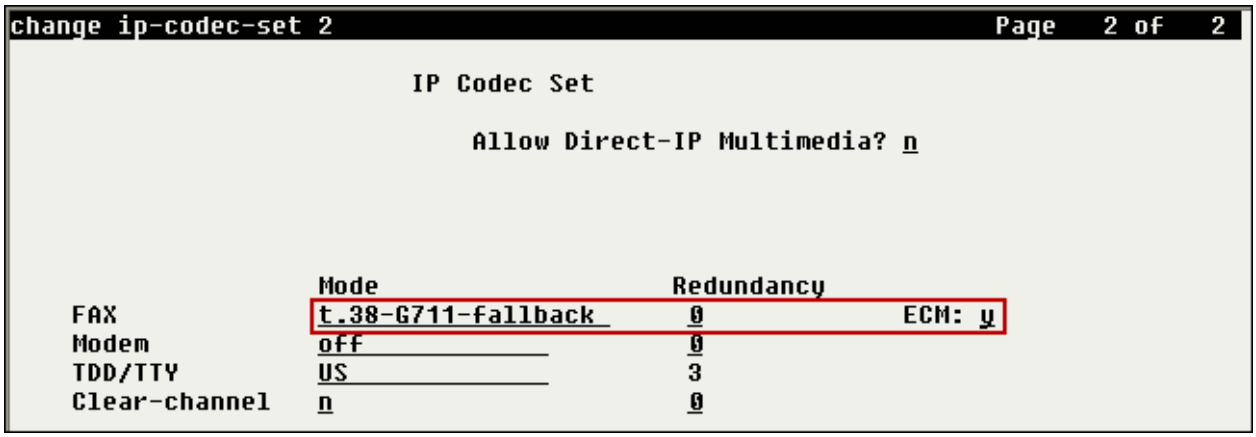
```
change node-names ip                                           Page   1 of   2
                                   IP NODE NAMES
    Name                  IP Address
ASBCE_A1                  172.16.5.71
Lab-HG-SM                 172.16.5.32
MA-CM                     192.168.10.12
default                   0.0.0.0
msgserver                 172.16.5.12
procr                     172.16.5.12
procr6                    ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Hawaiian SIP Trunking supports G.711MU, G.711A and G.729A. Thus, these codecs were included in this set. Enter **G.711MU, G.711A** and **G.729A** in the **Audio Codec** column of the table. Default values can be used for all other fields.



On **Page 2**, set the **Fax Mode** to **t.38-G711-fallback**



Use the **change ip-codec-set** command to define a list of codecs to use for telephones. For the compliance test, ip-codec-set 1 was used for this purpose. Default values can be used for all other fields.

```
change ip-codec-set 1                                          Page   1 of   2

                           IP Codec Set

   Codec Set: 1

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

On **Page 2**, set the **Fax Mode** to **off.**

```
change ip-codec-set 1                                          Page   2 of   2

                           IP Codec Set

                               Allow Direct-IP Multimedia? n



                     Mode                    Redundancy
   FAX               off                     0
   Modem             off                     0
   TDD/TTY           US                      3
   Clear-channel     n                       0
```

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.lab.com**. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                    Page   1 of  20
                                IP NETWORK REGION
  Region: 2
Location: 1___    Authoritative Domain: avaya.lab.com
   Name: SP Region_____________  Stub Network Region: n
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 2               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048_                        IP Audio Hairpinning? n
   UDP Port Max: 3349_
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20__
   Keep-Alive Interval (sec): 5__
            Keep-Alive Count: 5_
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 2                                    Page   4 of  20

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Avaya Aura® Communication Manager and the Avaya Aura® Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Avaya Aura® Communication Manager will serve as an Evolution Server for the Avaya Aura® Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between the Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The transport method used between the Avaya Aura® Session Manager and the Avaya Session Border Controller for Enterprise is specified as TCP in **Sections 6.5**. Lastly, the transport method between the Avaya Session Border Controller for Enterprise and Hawaiian Telecom is UDP. This is defined in **Section 7.2.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the Avaya Aura® Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5070**. (For TCP, the well-known port value is 5060).
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Avaya Aura® Communication Manager detects its peer as an Avaya Aura® Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Avaya S8300D Server running Avaya Aura® Communication Manager as defined in **Section 5.3**.

- Set the **Far-end Node Name** to **Lab-HG-SM**. This node name maps to the IP address of Avaya Aura® Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Avaya Aura® Communication Manager to redirect media traffic directly between the inside IP of the Avaya Session Border Controller for Enterprise and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Avaya Aura® Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```
change signaling-group 2                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 2                      Group Type: sip
  IMS Enabled? n                  Transport Method: tcp
       Q-SIP? n
    IP Video? n                                          Enforce SIPS URI for SRTP? y
 Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

  Near-end Node Name: procr                    Far-end Node Name: Lab-HG-SM
Near-end Listen Port: 5070                   Far-end Listen Port: 5070
                                           Far-end Network Region: 2

Far-end Domain: avaya.lab.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? n                        Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                 Alternate Route Timer(sec): 6
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.

- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
change trunk-group 2                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 2                      Group Type: sip          CDR Reports: y
  Group Name: Service Provider              COR: 1      TN: 1      TAC: 602
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk      Auth Code? n
                                              Member Assignment Method: auto
                                                    Signaling Group: 2
                                                  Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
change trunk-group 2                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                        Redirect On OPTIM Failure: 5000

           SCCAN? n                                  Digital Loss Group: 18
                    Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Avaya Aura® Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with Hawaiian Telecom. Thus, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values were used for all other fields.

```
change trunk-group 2                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                    Maintenance Tests? y

                   Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                  Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

On **Page 4**, set **Network Call Redirection** field to **y** to direct Avaya Aura® Communication Manager to use the SIP REFER message for transferring calls off-net to the PSTN. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to **n**.

Set the **Telephone Event Payload Type** to **101**, the value preferred by Hawaiian Telecom. Set **Convert 180 to 183 for Early Media** to **y**.

```
change trunk-group 2                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                                        Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                    Send Transferring Party Information? n
                               Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                 Send Diversion Header? y
                               Support Request History? n
                          Telephone Event Payload Type: 101

                      Convert 180 to 183 for Early Media? y
                Always Use re-INVITE for Display Updates? n
                      Identity for Calling Party Display: P-Asserted-Identity
           Block Sending Calling Party Location in INVITE? n
                Accept Redirect to Blank User Destination? n
                                          Enable Q-SIP? n
```

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs).

The screen below shows DID numbers assigned for testing. The DID numbers were mapped to the enterprise extensions 3040 - 3047. These 10-digit numbers were used for the outbound calling party information on the service provider trunk when calls were originated from these extensions.

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

Ext  Ext              Trk        Private          Total
Len  Code             Grp(s)     Prefix           Len
 4   3                                           4      Total Administered: 7
4    3040           2          5551231474       10        Maximum Entries: 540
4    3041           2          5551231475       10
4    3042           2          5551231476       10
4    3045           2          5551231479       10
4    3046           2          5551231477       10
4    3047           2          5551231478       10
```

In a real customer environment, normally DID numbers are comprised of local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with 1 will send the calling party number as the **Private Prefix** plus the extension number.

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

Ext  Ext              Trk        Private          Total
Len  Code             Grp(s)     Prefix           Len
 4   3                                           4      Total Administered: 7
4    1              2          555123           10        Maximum Entries: 540
```

5.9. . Inbound Routing

DID numbers received from Hawaiian Telecom were mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 2                    Page   1 of   3
                        INCOMING CALL HANDLING TREATMENT
 Service/       Number   Number       Del Insert
 Feature         Len      Digits
 public-ntwrk    10 5551231474        10  3040
 public-ntwrk    10 5551231475        10  3041
 public-ntwrk    10 5551231476        10  3042
 public-ntwrk    10 5551231477        10  3046
 public-ntwrk    10 5551231478        10  3047
 public-ntwrk    10 5551231479        10  3045
```

In a real customer environment, where DID numbers are usually comprised of local extension plus a prefix, a single entry can be applied for all extensions, like in the example below.

```
change inc-call-handling-trmt trunk-group 2                    Page   1 of   3
                        INCOMING CALL HANDLING TREATMENT
 Service/       Number   Number       Del Insert
 Feature         Len      Digits
 public-ntwrk    10 555123            6
 public-ntwrk
 public-ntwrk
```

5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).

```
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
   0          13   udp
   1          4    dac
   2          4    ext
   3          4    ext
   4          4    udp
   5          4    ext
   6          3    dac
   7          4    ext
   8          4    ext
   9          1    fac
   *          3    dac
   #          2    dac
```

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                  Page   1 of  10
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
                      Announcement Access Code: #7__
                       Answer Back Access Code: ____
                         Attendant Access Code: __
      Auto Alternate Routing (AAR) Access Code: *01_
    Auto Route Selection (ARS) - Access Code 1: 9___  Access Code 2: ____
                  Automatic Callback Activation: ____  Deactivation: ____
Call Forwarding Activation Busy/DA: ____   All: ____  Deactivation: ____
   Call Forwarding Enhanced Status: ____   Act: ____  Deactivation: ____
                        Call Park Access Code: ____
                      Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                  CDR Account Code Access Code: ____
                       Change COR Access Code: ____
                  Change Coverage Access Code: ____
            Conditional Call Extend Activation: ____  Deactivation: ____
                    Contact Closure   Open Code: ____    Close Code: ____
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 which contains the SIP trunk to the service provider (as defined next).

```
change ars analysis 17                                       Page   1 of   2
                           ARS DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 2

      Dialed             Total      Route     Call    Node   ANI
      String            Min  Max   Pattern   Type    Num    Reqd
   170                  11   11    deny      fnpa    ___    n
   1700                 11   11    deny      fnpa    ___    n
   171                  11   11    deny      fnpa    ___    n
   172                  11   11    2         fnpa    ___    n
   173                  11   11    deny      fnpa    ___    n
   174                  11   11    deny      fnpa    ___    n
   175                  11   11    deny      fnpa    ___    n
   176                  11   11    deny      fnpa    ___    n
   177                  11   11    deny      fnpa    ___    n
   178                  11   11    deny      fnpa    ___    n
   1786                 11   11    2         fnpa    ___    n
   179                  11   11    deny      fnpa    ___    n
   180                  11   11    deny      fnpa    ___    n
   1800                 11   11    2         fnpa    ___    n
   1800555              11   11    deny      fnpa    ___    n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 2 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format**: **unk-unk** calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**

```
change route-pattern 2                                    Page   1 of   3
                     Pattern Number: 2      Pattern Name: Windstream
                                  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: 2   0       1                                                  n    user
2:                                                                n    user
3:                                                                n    user
4:                                                                n    user
5:                                                                n    user
6:                                                                n    user

    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W    Request                                Dgts Format
                                                       Subaddress
1: y y y y y n  n            rest                                 unk-unk   next
2: y y y y y n  n            rest                                           none
3: y y y y y n  n            rest                                           none
4: y y y y y n  n            rest                                           none
5: y y y y y n  n            rest                                           none
6: y y y y y n  n            rest                                           none
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include adding the following items:

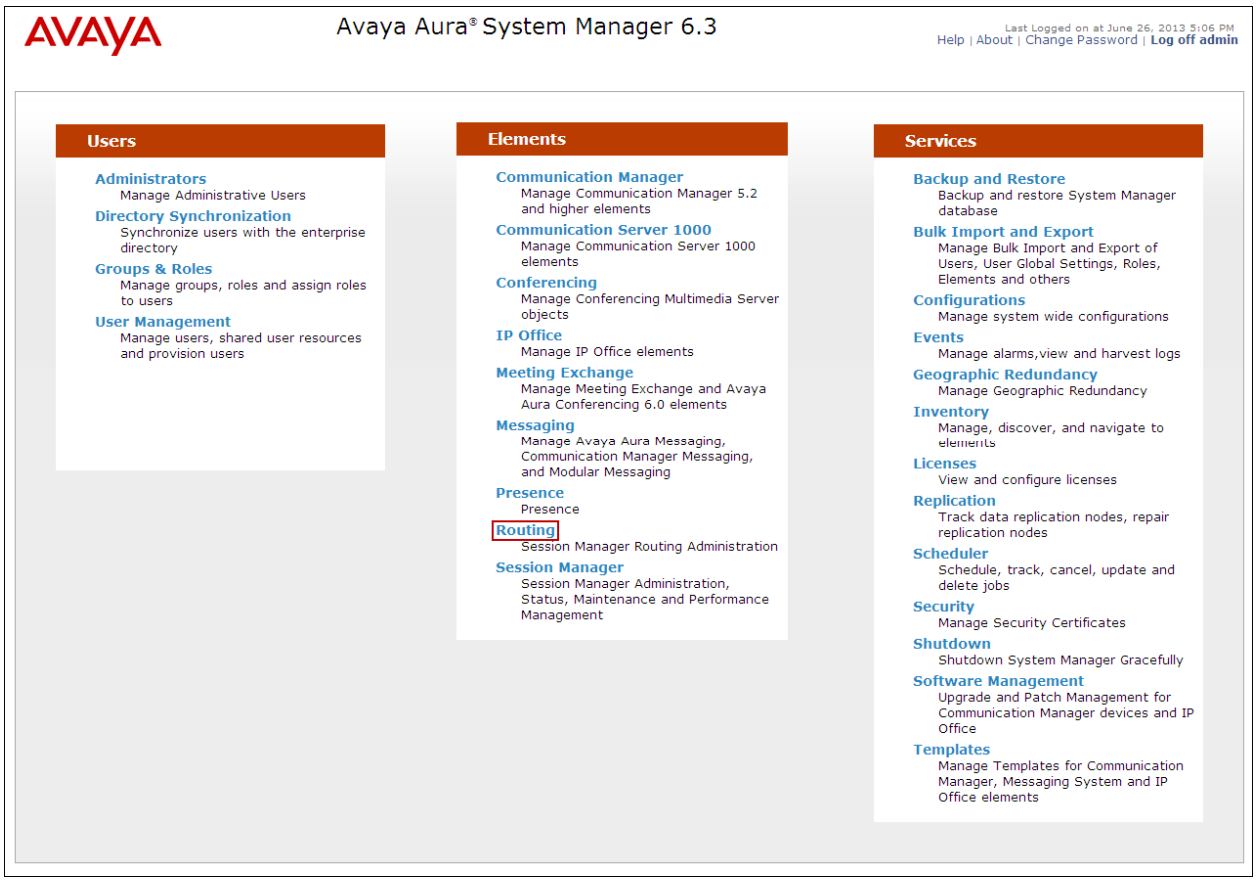
- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to Avaya Aura® Communication Manager, the Avaya Session Border Controller for Enterprise and Avaya Aura® Session Manager
- Entity Links, which define the SIP trunk parameters used by Avaya Aura® Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Regular Expressions, which also can be used to route calls
- Avaya Aura® Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager.

It may not be necessary to create all the items above when configuring a connection to the service provider since some of these items would have already been defined as part of the initial Avaya Aura® Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Avaya Aura® Session Manager itself. However, each item should be reviewed to verify the configuration.

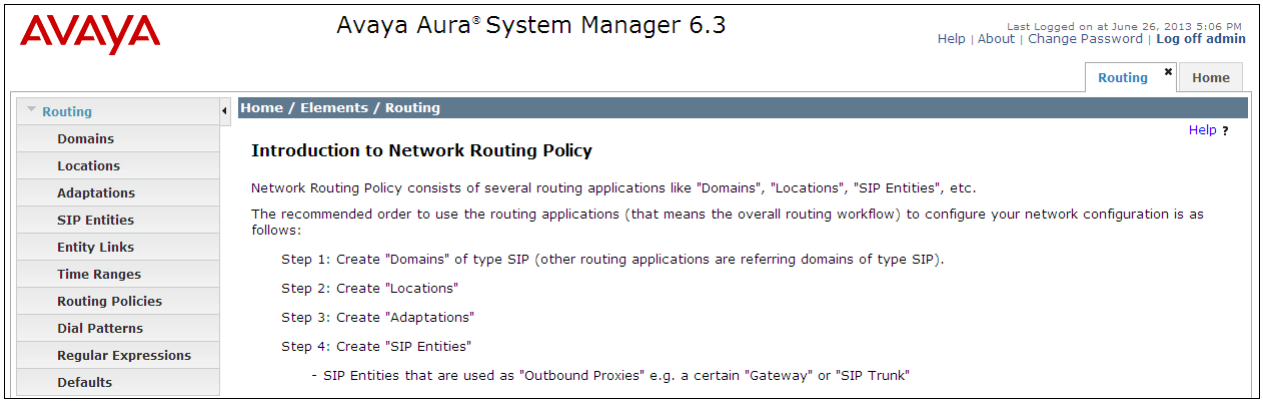
Note that some of the default information in the screenshots may have been cut out (not included) for brevity

6.1. System Manager Login and Navigation

Avaya Aura® Session Manager configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials (not shown). The screen shown below is then displayed, click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Routing** link shown below.



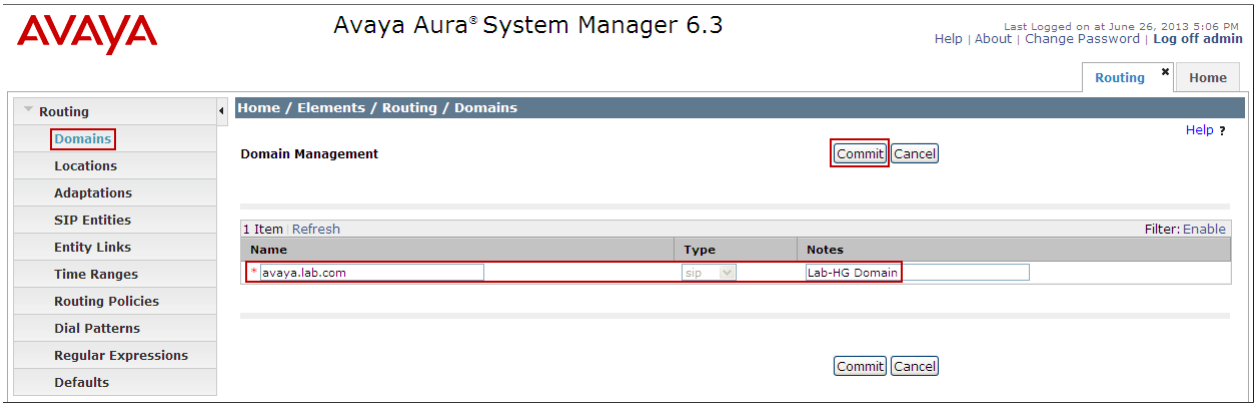
6.2. Specify SIP Domain

Create a SIP domain for each domain of which Avaya Aura® Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avaya.lab.com**).

To add a domain Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the enterprise domain.



6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

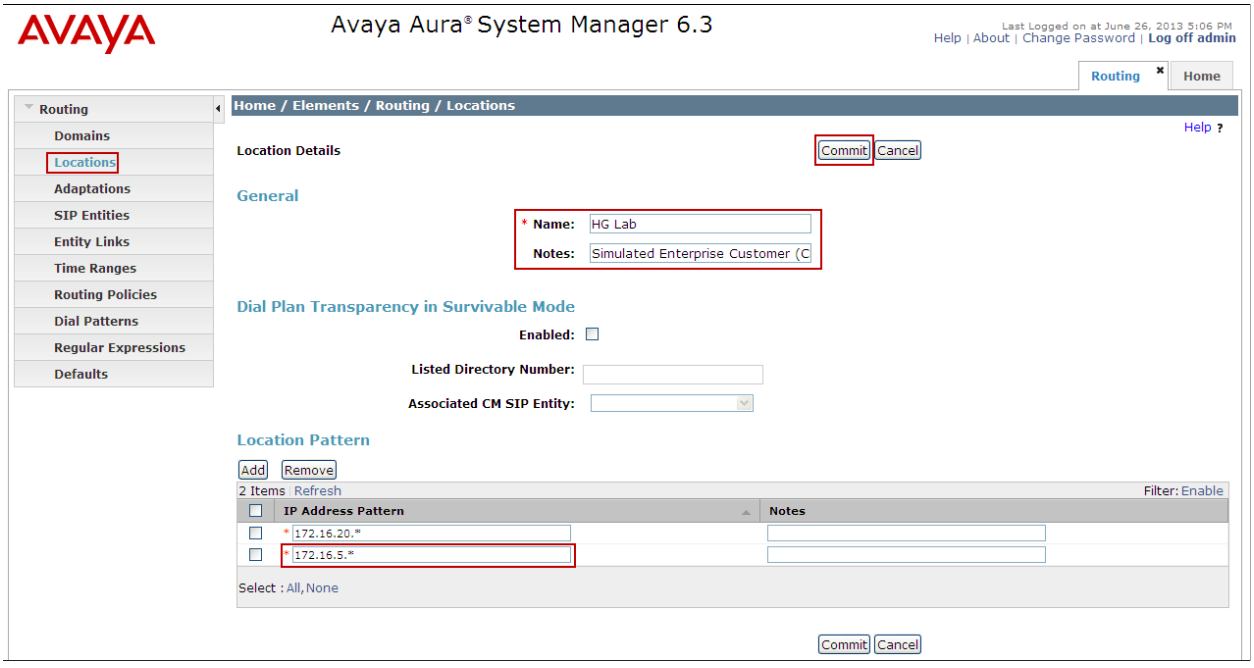
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

In the **Location Pattern**, click **Add** and enter the following values. Use default values for all remaining fields:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

The screen below shows the addition of the **HG Lab**, which includes all equipment on the **172.16.5.x** subnet including Avaya Aura® Communication Manager, and Avaya Aura® Session Manager itself. Click **Commit** to save.



6.4. SIP Entities

A SIP Entity must be added for Avaya Aura® Session Manager and for each SIP telephony system connected to it which includes Avaya Aura® Communication Manager and the Avaya Session Border Controller for Enterprise. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the SBC.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

To define the ports used by Avaya Aura® Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

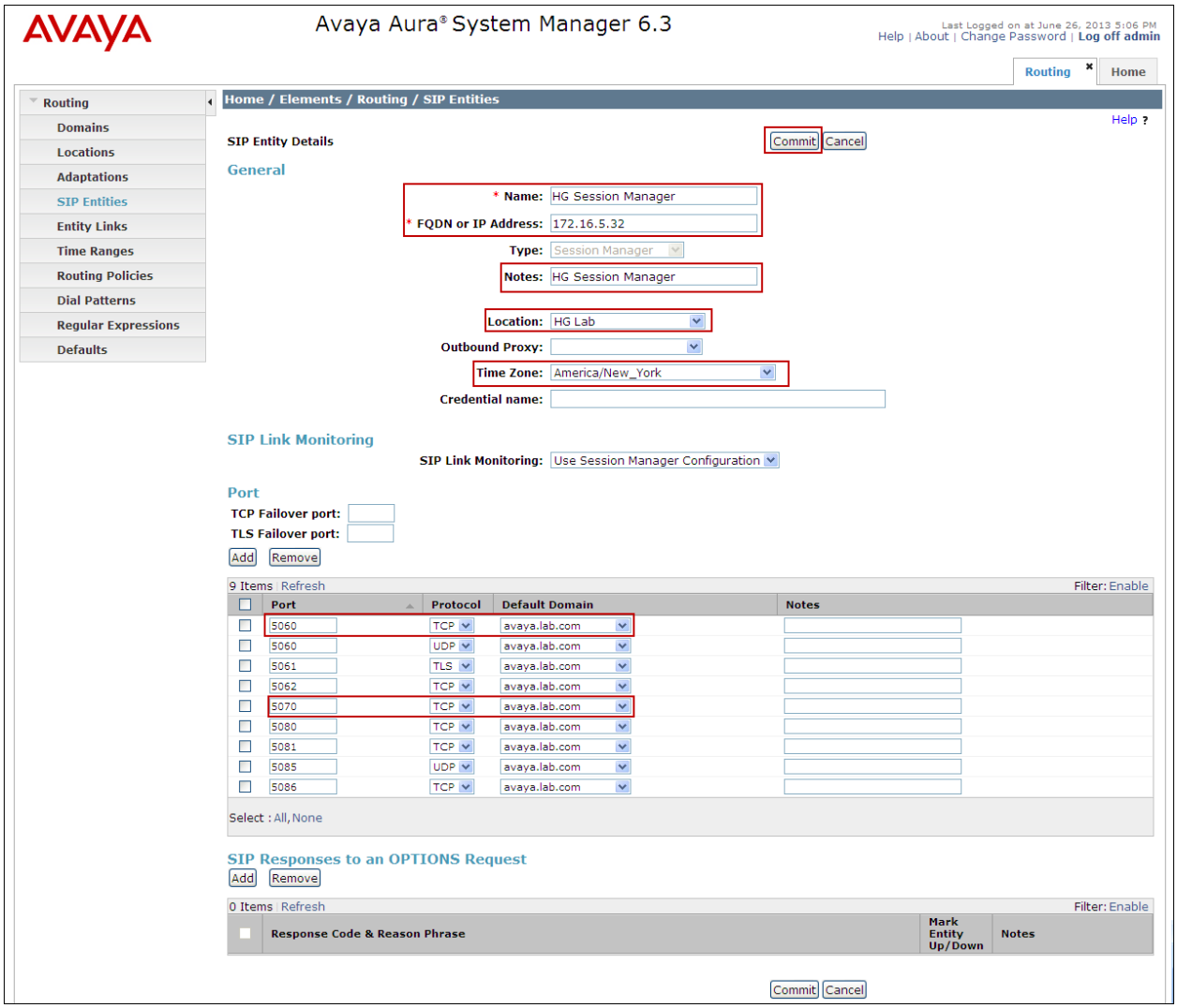
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save.

For the compliance test, only two Ports were used:

- **5060** with **TCP** for connecting to Avaya Session Border Controller for Enterprise.
- **5070** with **TCP** for connecting to Avaya Aura® Communication Manager.

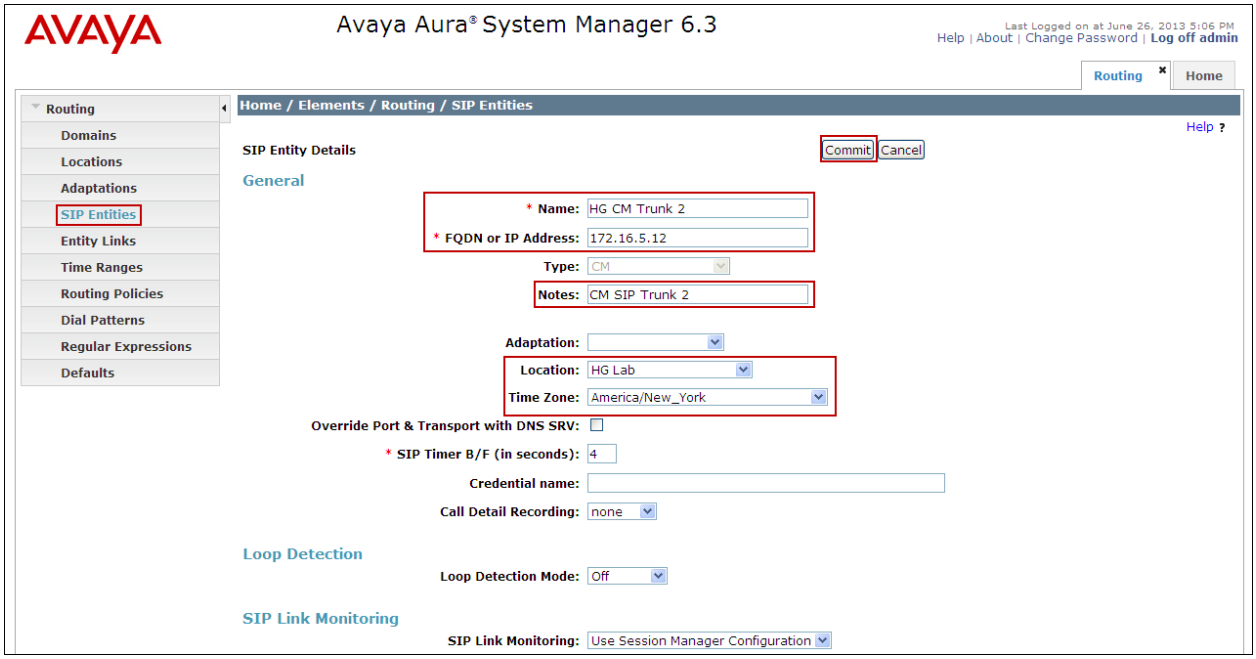
The following screen shows the addition of the Session Manager SIP entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.



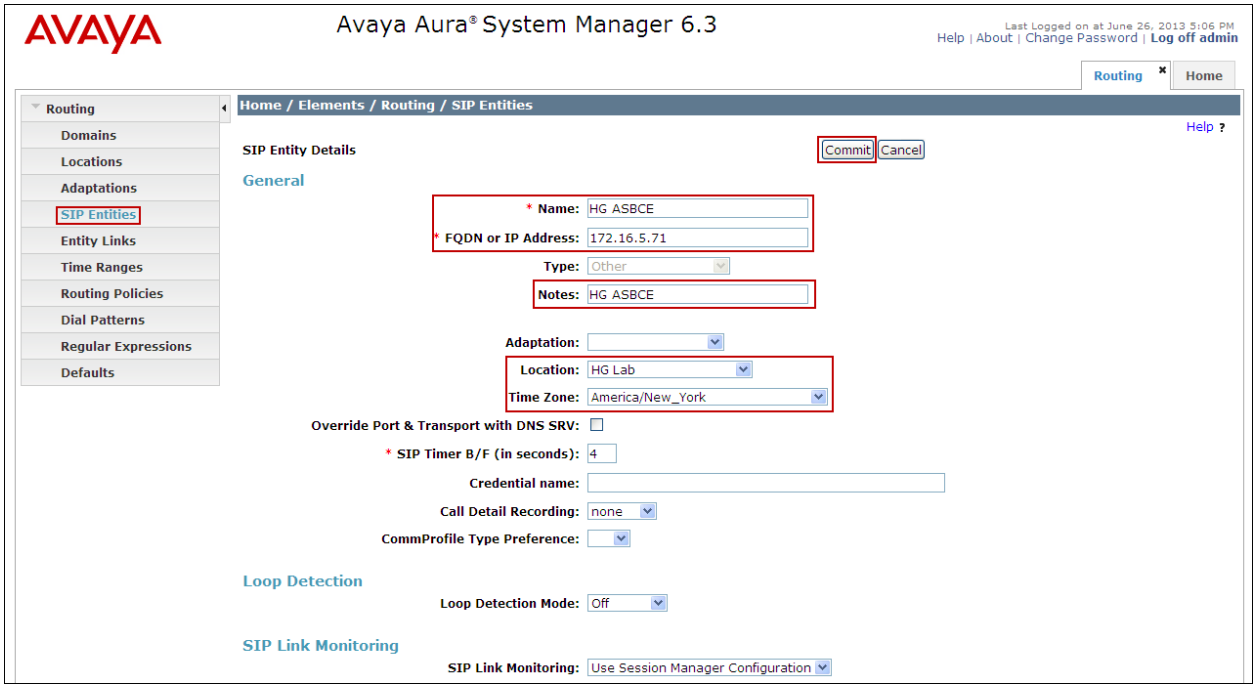
The following screen shows the addition of the Communication Manager SIP entity.

A separate SIP entity for Avaya Aura® Communication Manager, other than the one created at Avaya Aura® Session Manager installation, is required in order to send SIP service provider traffic.

The **FQDN or IP Address** field is set to the IP address of the Avaya S8300D Server running Avaya Aura® Communication Manager



The following screen shows the addition of the SIP entity for the Avaya Session Border Controller for Enterprise. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**).



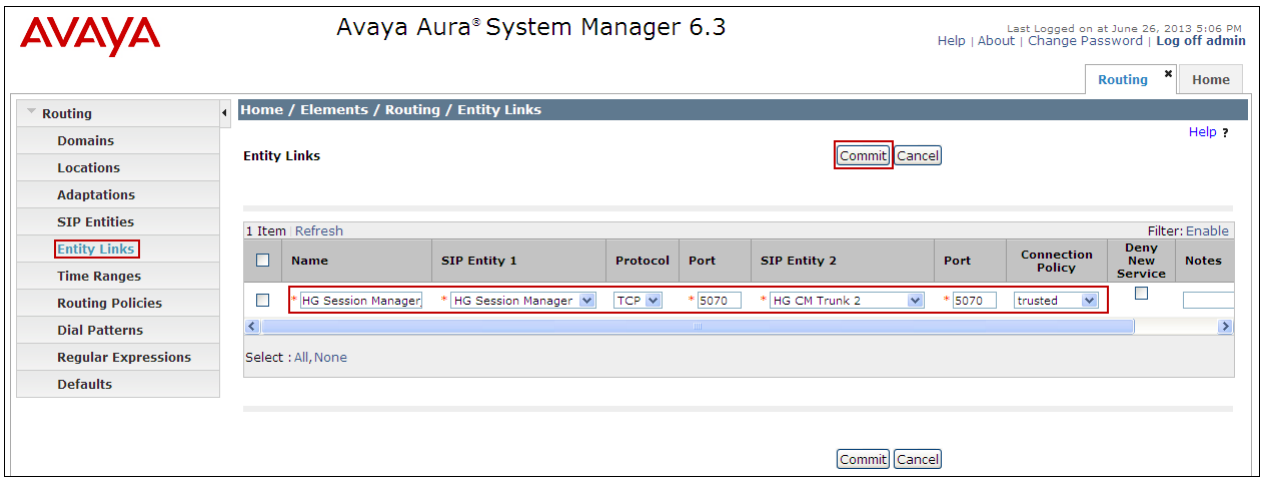
6.5. Entity Links

A SIP trunk between Avaya Aura® Session Manager and a telephony system is described by an Entity Link. Two entity links were created; one to the Avaya Aura® Communication Manager for use only by service provider traffic and one to the Avaya Session Border Controller for Enterprise. To add an entity link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

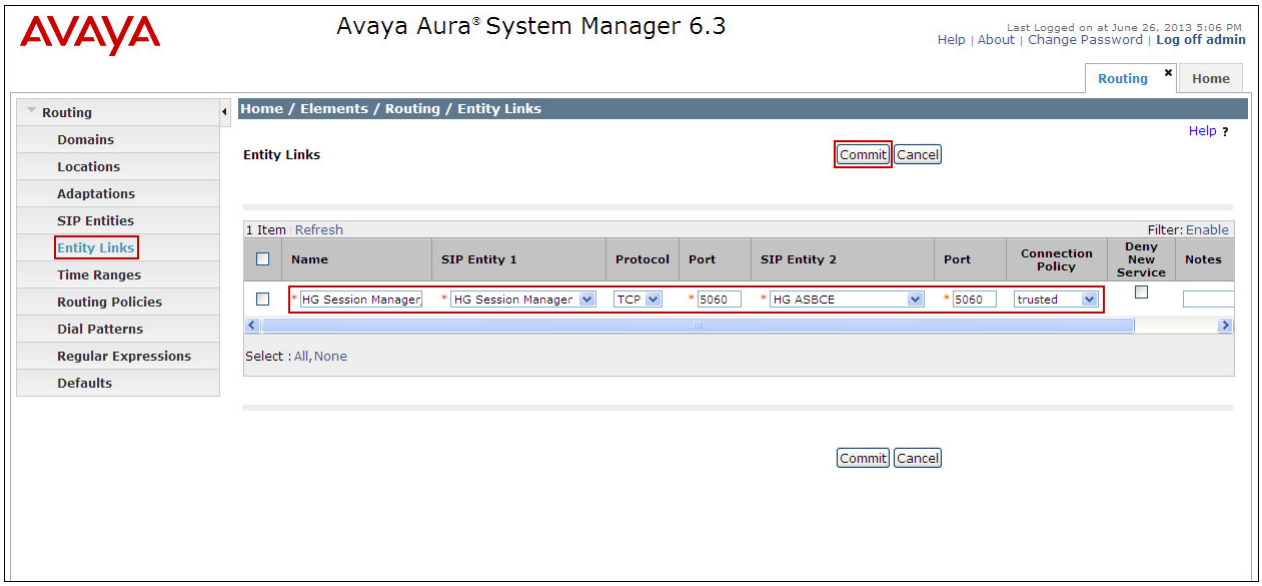
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Avaya Aura® Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select Trusted (not shown).

Click **Commit** to save. The following screens illustrate the entity links to Avaya Aura® Communication Manager and the Avaya Session Border Controller for Enterprise. It should be noted that in a customer environment the entity link to Avaya Aura® Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Avaya Aura® Communication Manager signaling group form in **Section 5.6**.

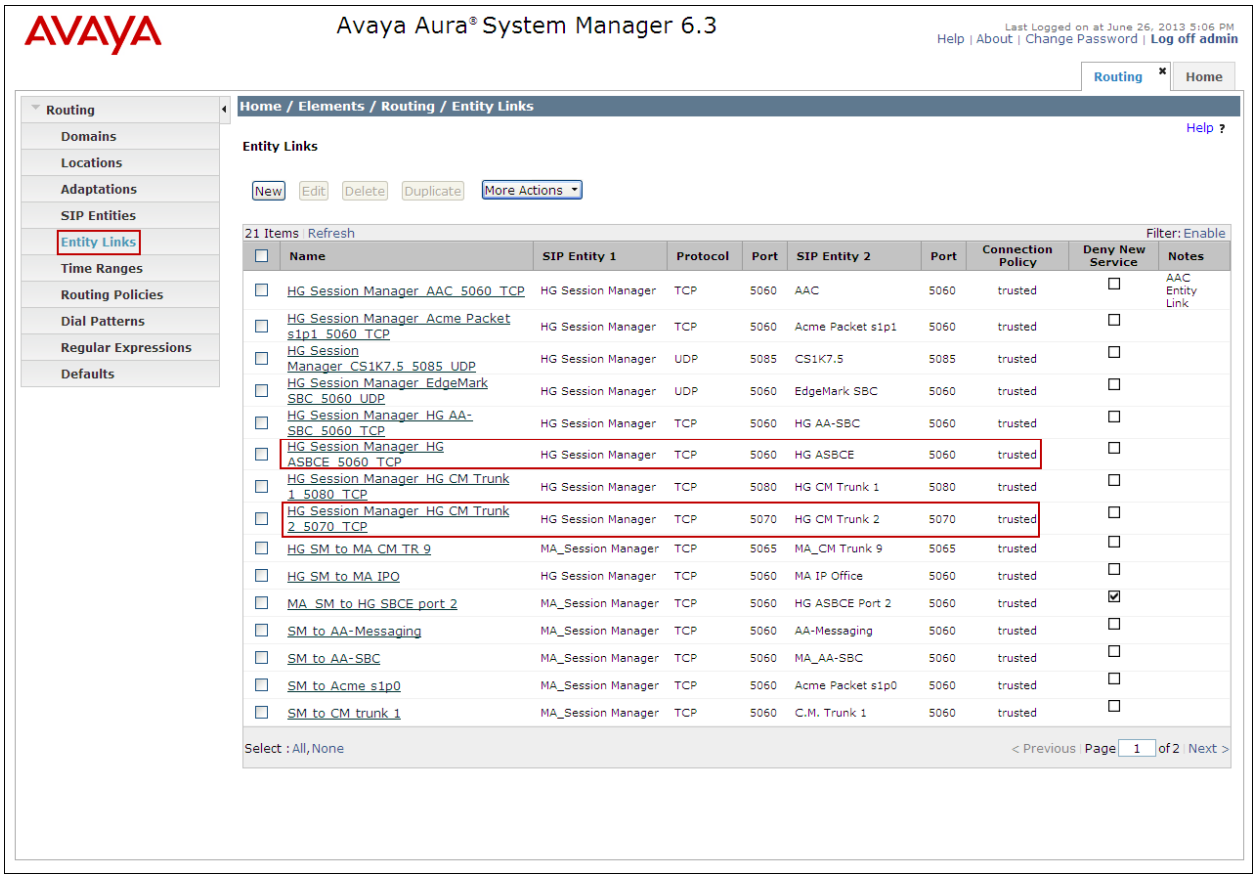
Entity link to Avaya Aura® Communication Manager:



Entity link to the Avaya Session Border Controller for Enterprise:



The following screen shows the list of entity links. Note that only the highlighted links were created for the compliance test, and are the ones relevant to these Application Notes.



6.6. Routing Policies

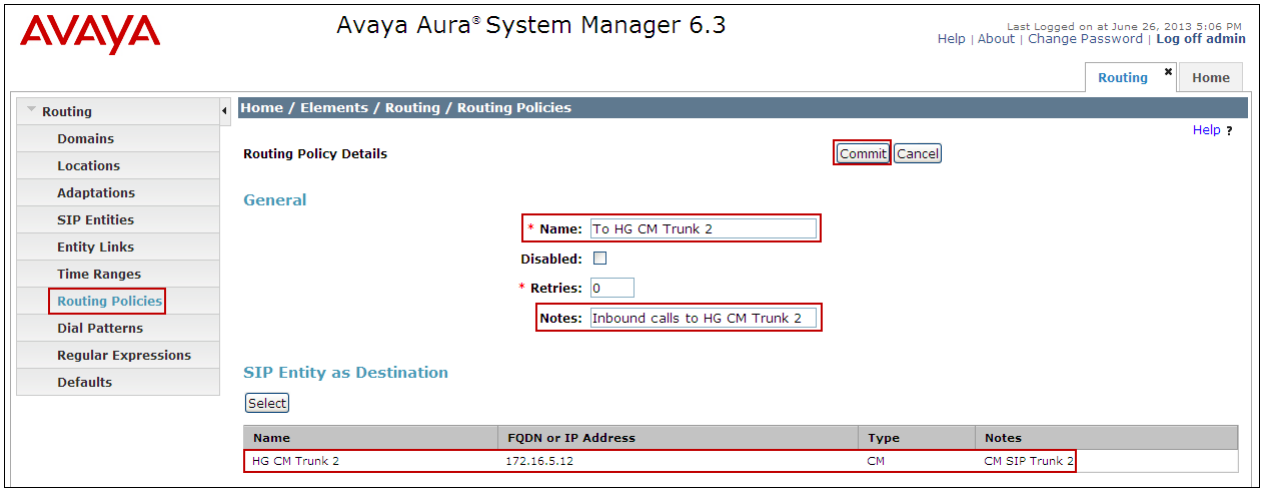
Routing policies describe the conditions under which calls are routed to the SIP entities specified in **Section 6.5**. Two routing policies must be added: one for Avaya Aura® Communication Manager and one for the Avaya Session Border Controller for Enterprise. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields:

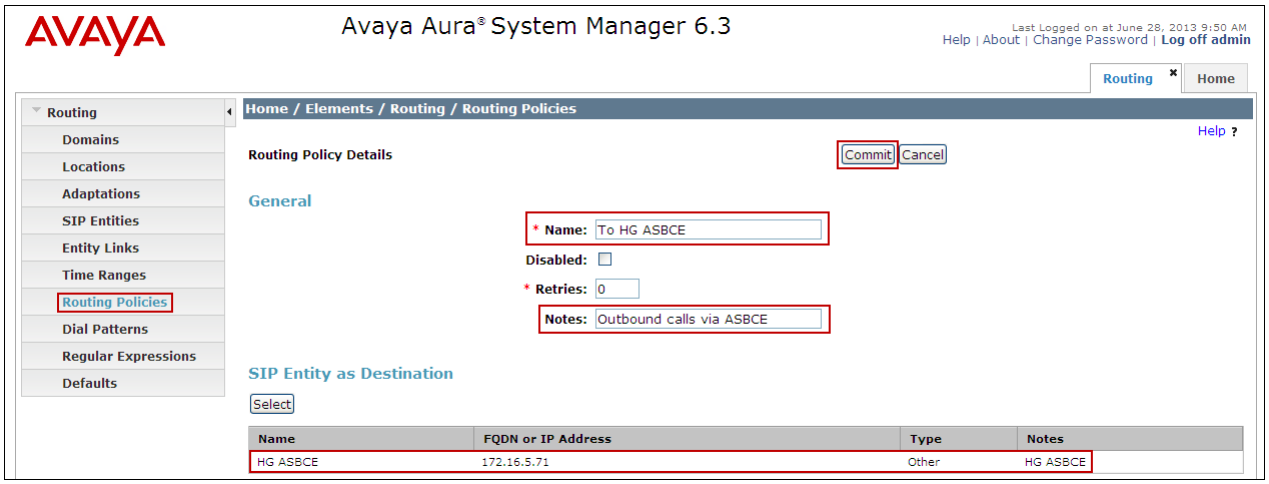
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select.** The selected SIP entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the routing policy for Avaya Aura® Communication Manager.



The following screens show the routing policy for the Avaya Session Border Controller for Enterprise.



6.7. Dial Patterns

Dial patterns are needed to route calls through Avaya Aura® Session Manager. For the compliance test, dial patterns were needed to route calls from Avaya Aura® Communication Manager to Hawaiian Telecom and vice versa. Dial patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values. Use default values for all remaining fields:

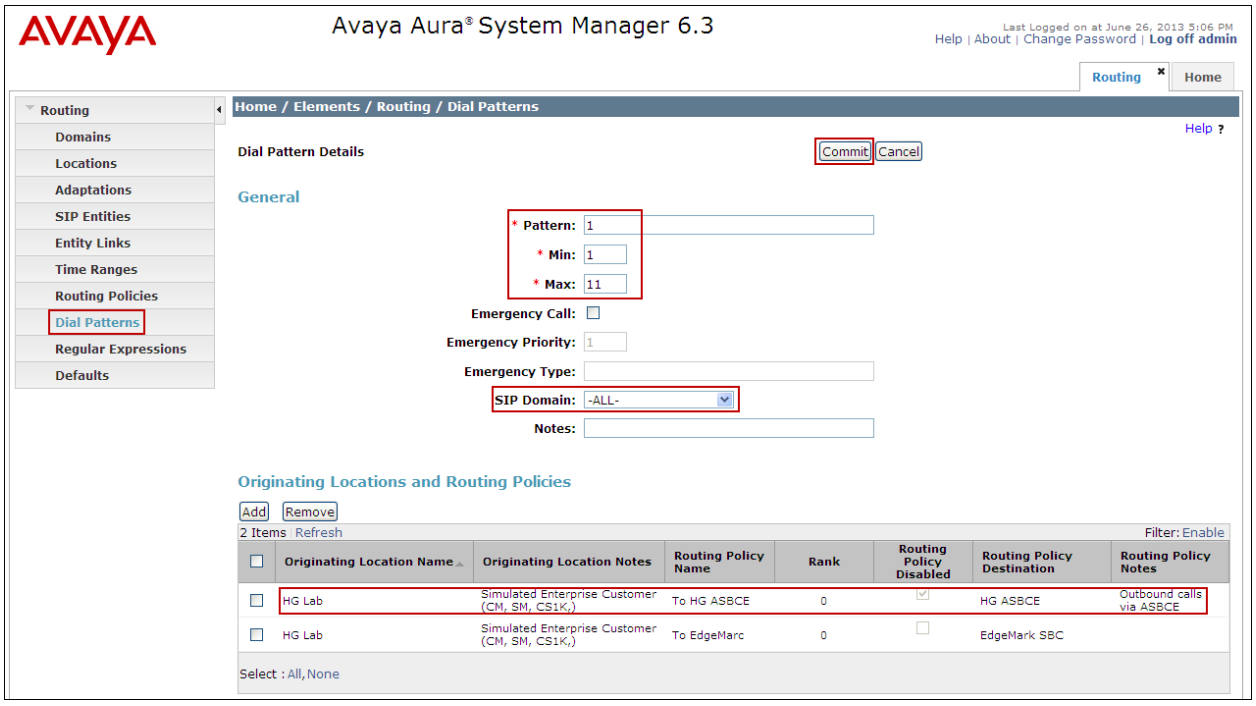
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

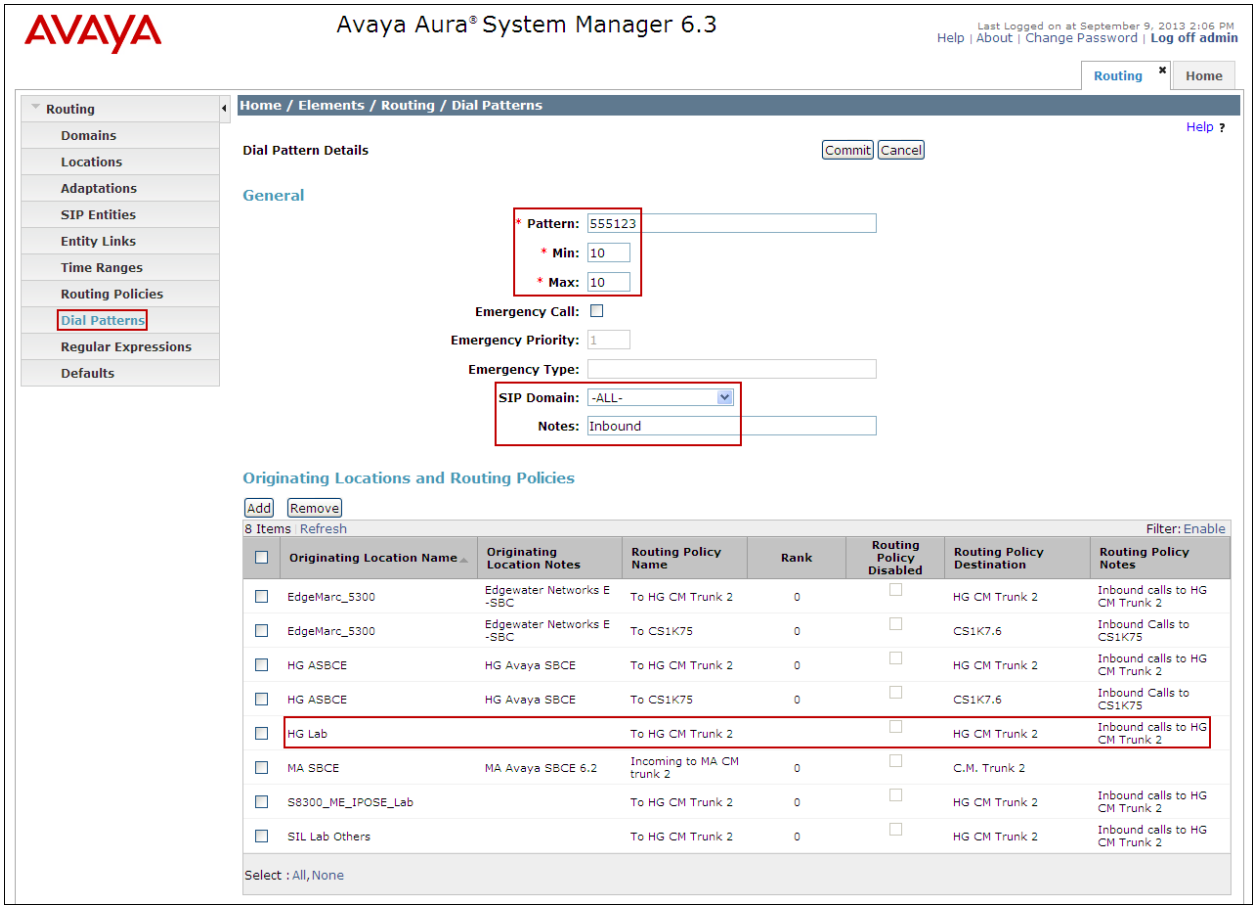
Default values can be used for the remaining fields. Click **Commit** to save.

Examples of the dial patterns used for the compliance testing are shown below.

The first example shows dial pattern **1**, with destination SIP Domain of **–ALL-**, Originating Location Name **HG Lab,** and Route Policy Name **To HG ASBCE.** This dial pattern was used for outbound calls to the PSTN.



The following dial pattern example used for the compliance testing was for inbound calls to the enterprise. It uses dial pattern **555123** matching the DID numbers assigned to the enterprise by Hawaiian Telecom. This dial pattern was configured with the destination SIP Domain of **–ALL-** , Originating Location Name **HG Lab,** and Routing Policy Name **HG CM Trunk 2.**



6.8. Add/View Avaya Aura® Session Manager

The creation of an Avaya Aura® Session Manager element provides the linkage between Avaya Aura® System Manager and Avaya Aura® Session Manager. This was most likely done as part of the initial Avaya Aura® Session Manager installation. To add an Avaya Aura® Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If the Avaya Aura® Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **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 **Save** (not shown) to add this Avaya Aura® Session Manager.

The screen below shows the Avaya Aura® Session Manager values used for the compliance test.

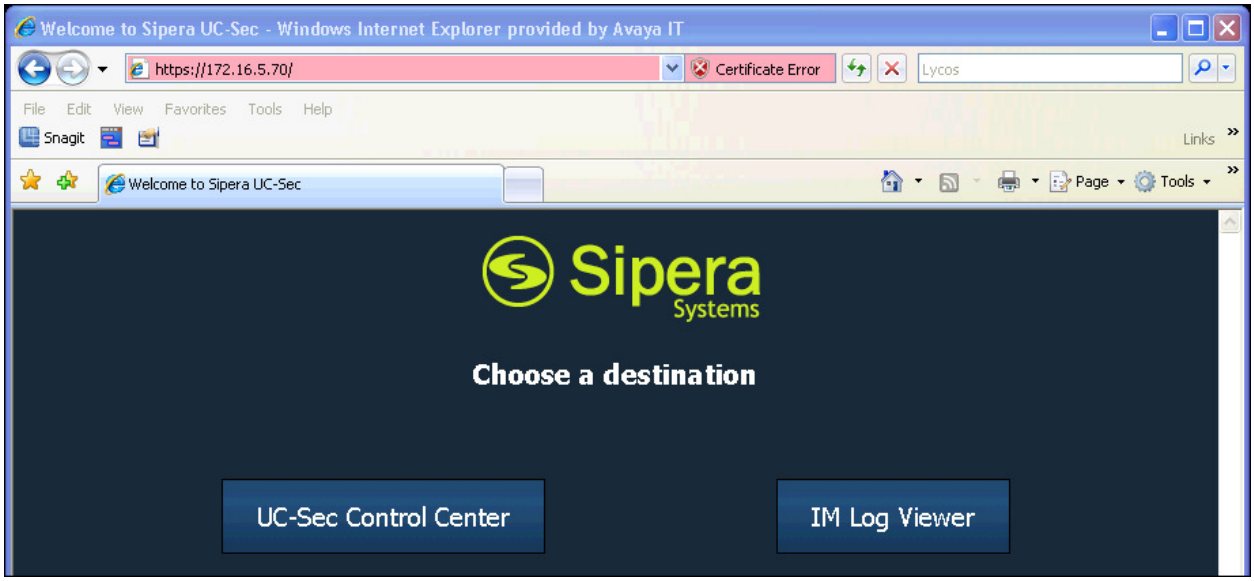
7. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).

This section describes the required configuration of the Avaya SBCE to connect to Hawaiian Telecom's SIP Trunk service.

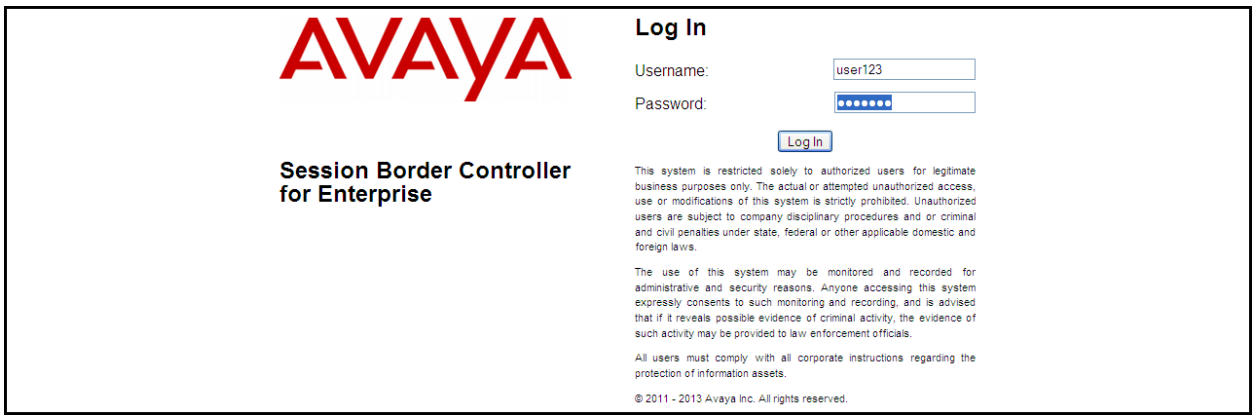
It is assumed that the Avaya SBCE is provisioned and ready to be used on the IP network; the configuration shown here is accomplished using the Avaya SBCE web interface.

7.1. Log in Avaya SBCE

Access the web interface by typing "https://x.x.x.x" (where x.x.x.x is the management IP of the Avaya SBCE)



Select **UC-Sec Control Center** and enter the **Username** and **password** to log in.



7.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices in the UC-Sec control Center.

7.2.1. Server Interworking Avaya-SM

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned", and then modified to meet specific requirements for the enterprise SIP-enabled solution.

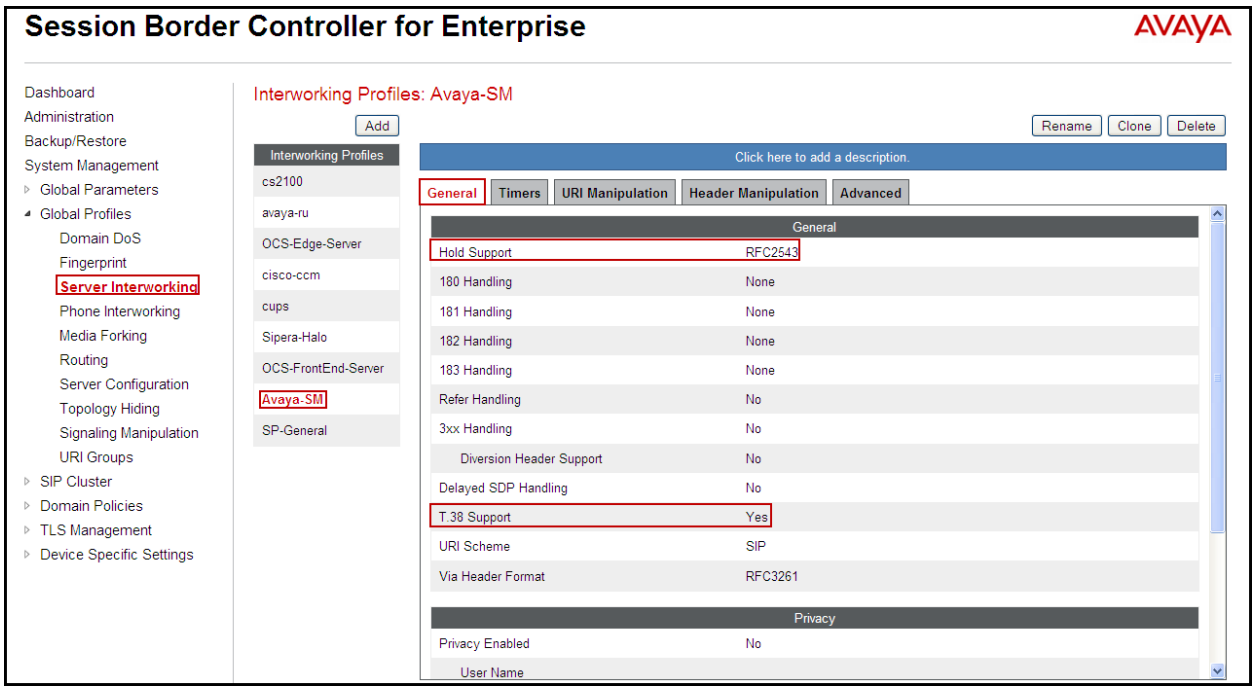
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone** on top right of the screen**.**

Enter the new profile name in the **Clone Name** field, the name of **Avaya-SM** was chosen in this example. Click **Finish.**

For the newly created **Avaya-SM** profile, click **Edit** (not shown) at the bottom of the General tab

- Verify that for **Hold Support**, **RFC2543** is selected.
- Verify that for **T.38 Support** is selected.
- Click **Next**.
- Leave other fields with their default values.
- Click **Finish** on the **Privacy and DTMF** tab.

The following screen capture shows the newly added **Avaya-SM** Profile.



7.2.2. Server Interworking SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

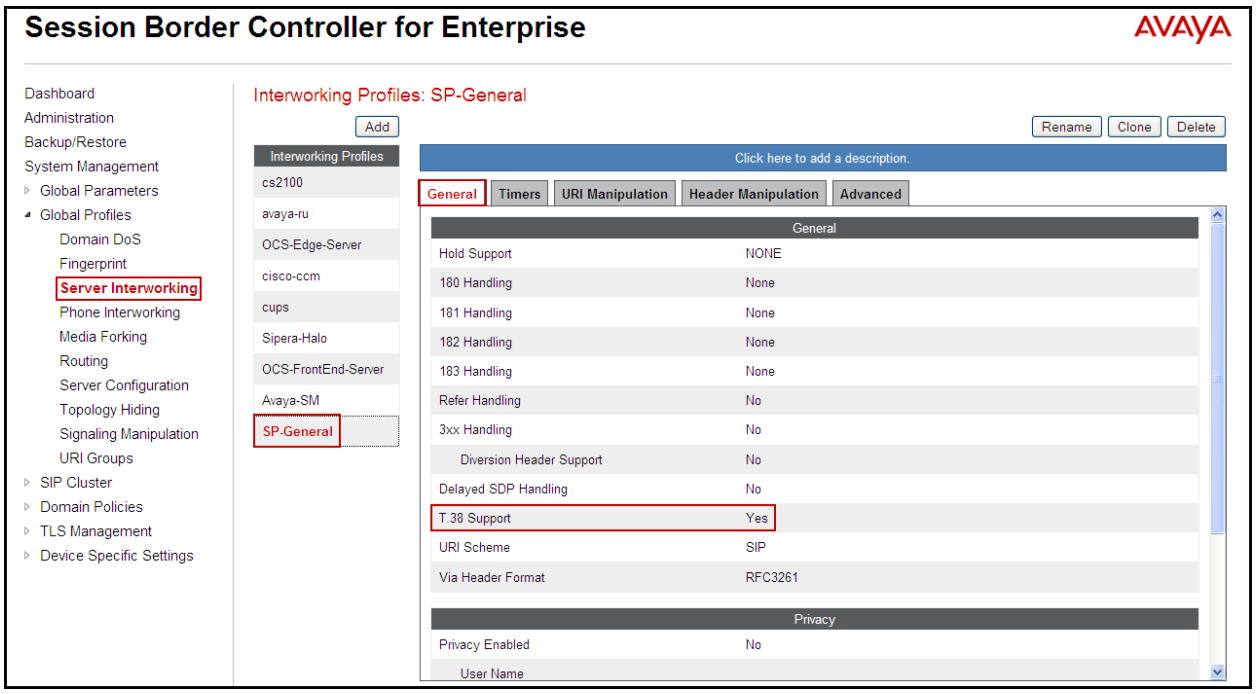
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add.**

Enter the new profile name (not shown), the name of **SP-General** was chosen in this example. Accept the default values for all fields by clicking **Next** and then Click **Finish.**

For the newly created **SP-General** profile, click **Edit** (not shown) at the bottom of the General tab.

- Select **T.38 Support**
- Click **Next**.
- Leave other fields with their default values.
- Click **Finish** on the **Privacy** tab.

The following screen capture shows the newly added **SP-General** profile.



7.2.3. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

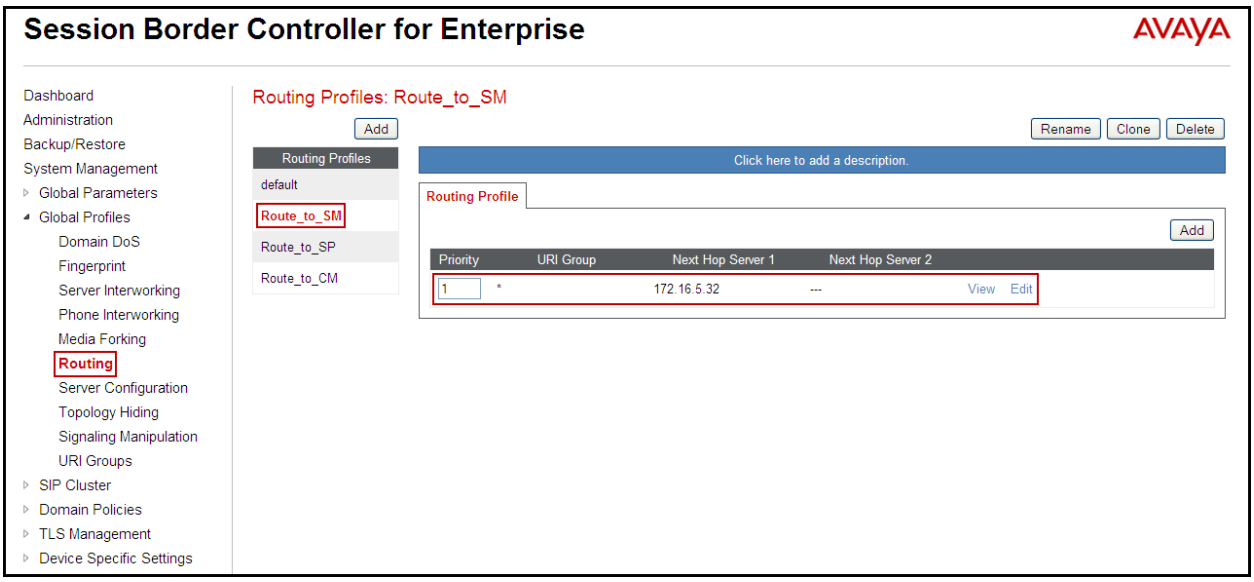
To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section**.**
- Enter Profile Name: **Route_to_SM.**
- Click **Next.**

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.32** (Session Manager IP address).
- Check **Routing Priority Based on Next Hop Server.**
- **Outgoing Transport:** select **TCP.**
- Click **Finish.**

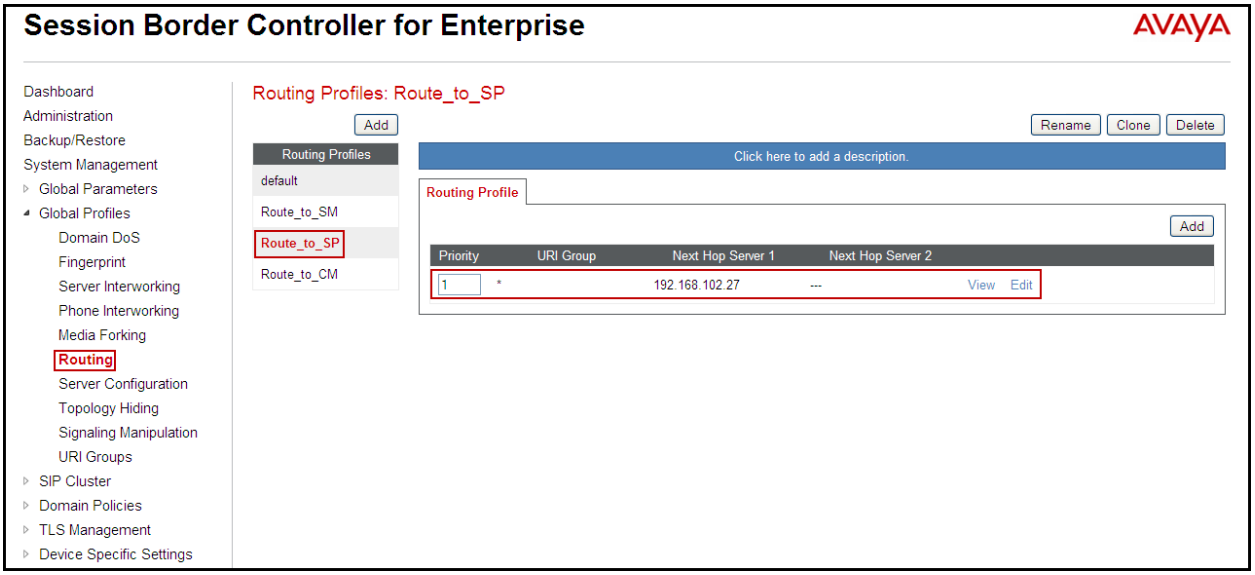
The following screen shows the newly added **Route_to_SM** Profile.



Similarly, for the outbound route:

- Click **Add** in the **Routing Profiles** section**.**
- Enter Profile Name: **Route_to_SP**
- Click **Next.**
- **Next Hop Server 1: 192.168.102.27** (Service Provider IP address)
- Check **Routing Priority Based on Next Hop Server.**
- **Outgoing Transport:** select **UDP.**
- Click **Finish.**

The following screen capture shows the newly added **Route_to_SP** Profile.



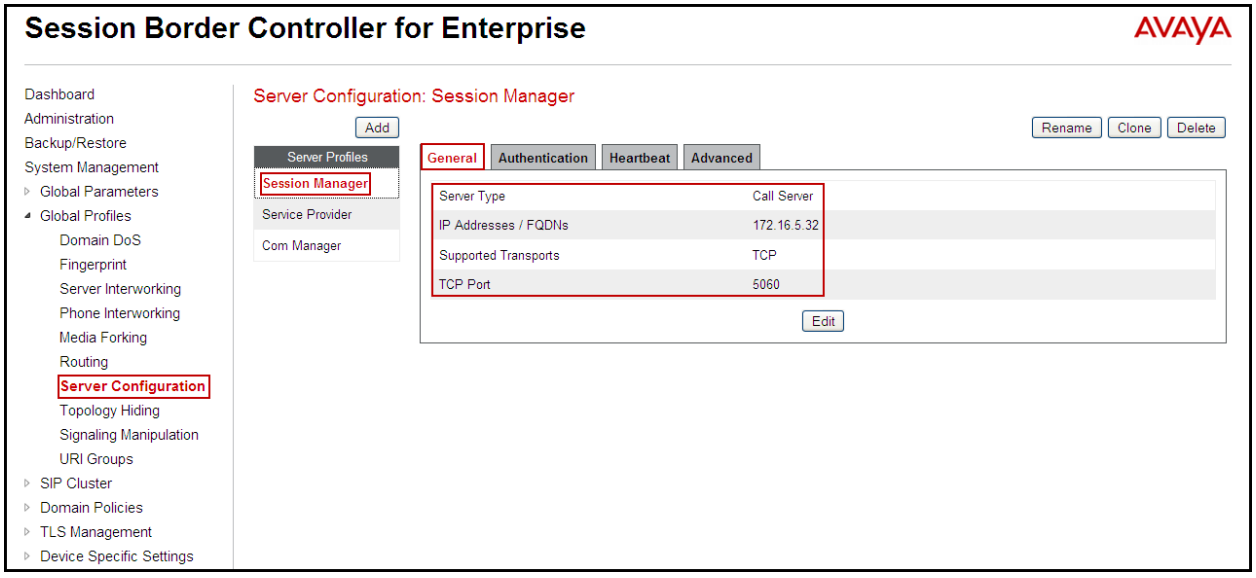
7.2.4. Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server or SIP Proxy at the service provider's network.

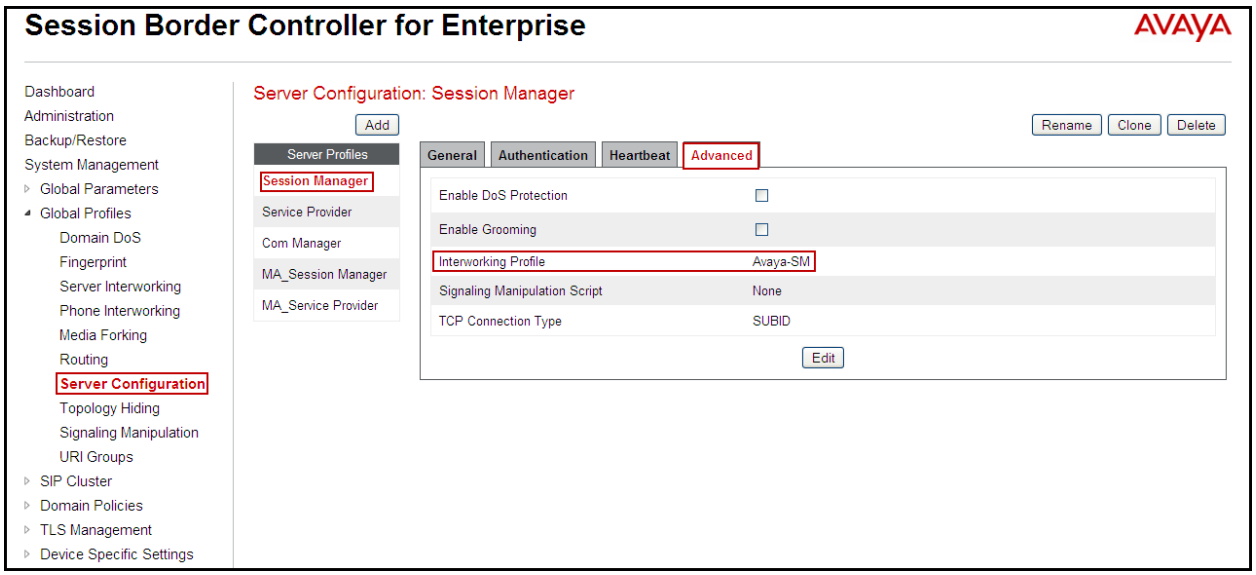
To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add** in the **Server Profiles** section and enter the profile name: **Session Manager**.

- In the **Add Server Configuration Profile - General** window
  - **Server Type**: select **Call Server.**
  - **IP Address: 172.16.5.32** (IP Address of Session Manager).
  - **Supported Transports**: check **TCP.**
  - **TCP Port:** enter **5060.**
  - Click **Next.**
- Click **Next** in the **Authentication** window.
- Click **Next** in the **Heartbeat** window.
- In the **Advanced** window
  - Select **Avaya-SM** from the **Interworking Profile** drop down menu.
  - Leave the **Signaling Manipulation Script** at the default **None**.
  - Click **Finish.**

The following screen capture shows the **General** tab of the newly added **Session Manager** profile.



The following screen capture shows the **Advanced** tab of the added **Session Manager** profile.

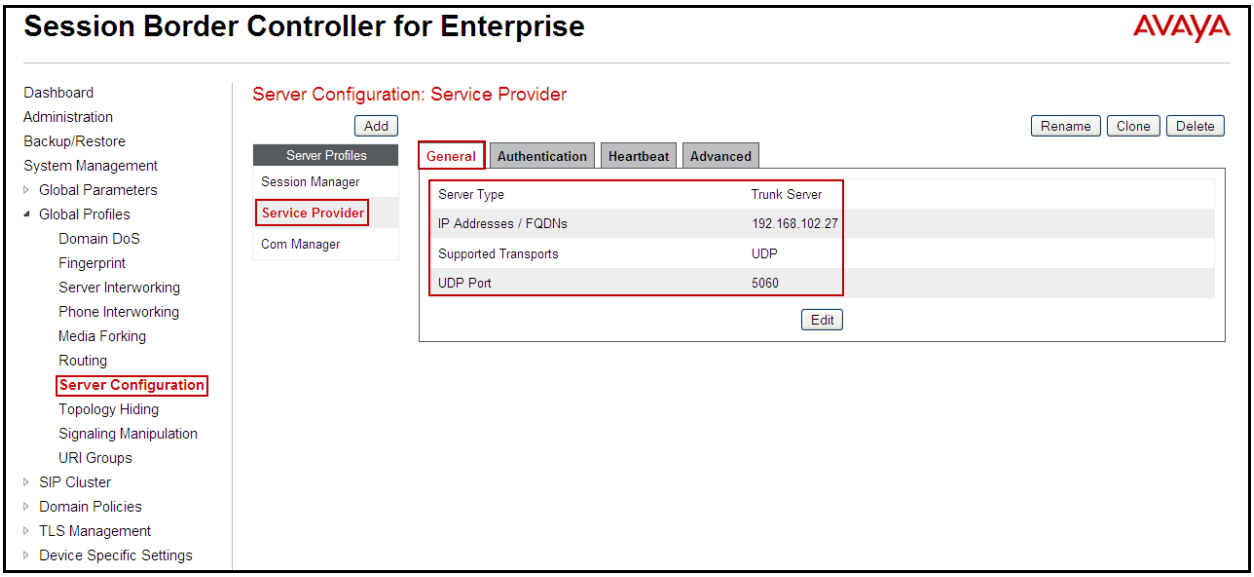


To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** section and enter the profile name: **Service Provider.**

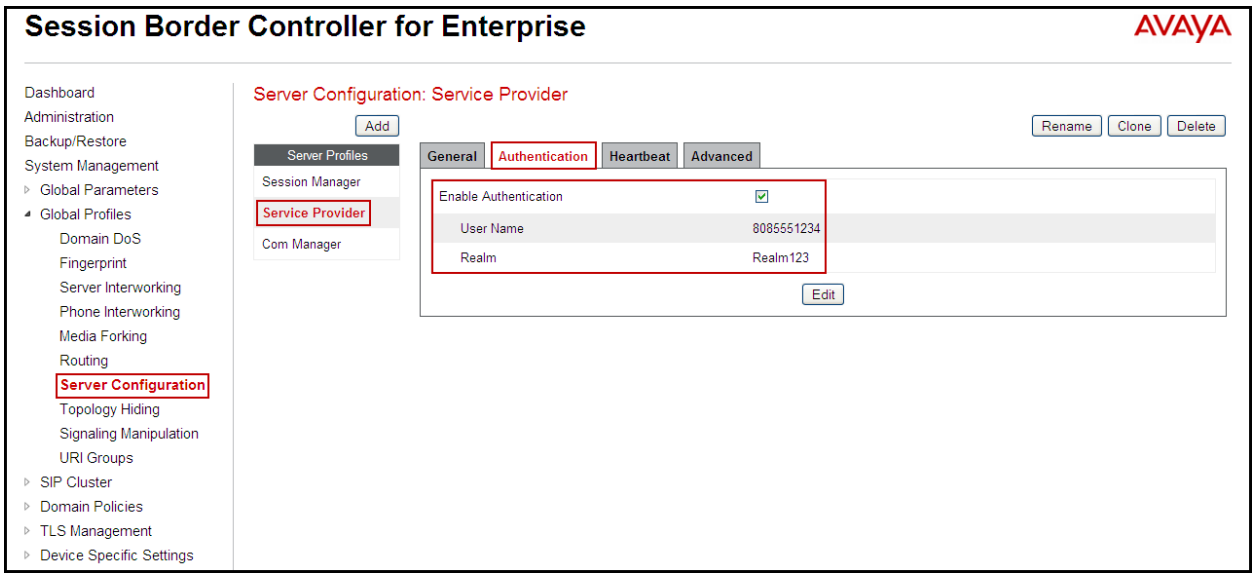
- In the **Add Server Configuration Profile - General** window
  - **Server Type:** select **Trunk Server.**
  - **IP Address: 192.168.102.27** (service provider's SIP Proxy IP address).
  - **Supported Transports**: check **UDP**.
  - **UDP Port:** enter **5060**.
  - Click **Next**.
- In the **Authentication** window
  - Select **Enable Authentication**.
  - Enter the **user name** provided by Hawaiian Telecom in the **User Name** field.
  - Enter the **Realm** provided by Hawaiian Telecom in the **Realm** field.
  - Enter the **password** provided by Hawaiian Telecom in the **Password** field.
  - Re-enter the password provided by Hawaiian Telecom in the **Confirm Password** field
  - Click **Next** to continue.
- In the **Heartbeat** window
  - Select **Enable Heartbeat**.
  - Select **Register** for **Method.**
  - Enter **frequency** for registration challenges (Value of **60** seconds was used in the compliance testing).
  - Enter the **From URI** information (e.g., **8085551234@192.168.157.187**)
    - **8085551234** is the pilot user provided by Hawaiian Telecom for registration purpose.

    - **192.168.157.187** is the outside IP address assigned to the Avaya SBCE.
  - Enter the **To URI** information (i.e., **8085551234@hawaiiantel.net**).
    - **8085551234** is the pilot user provided by Hawaiian Telecom for registration purpose.
    - **Hawaiiantel.net** is the domain name provided by Hawaiian Telecom.
  - Click **Next** to continue.
- In the **Advanced** window
  - Select **SP General** from the **Interworking Profile** drop down menu.
  - Leave other fields with their default values for now, a **Signaling Manipulation** Script will be assigned later.
  - Click **Finish.**

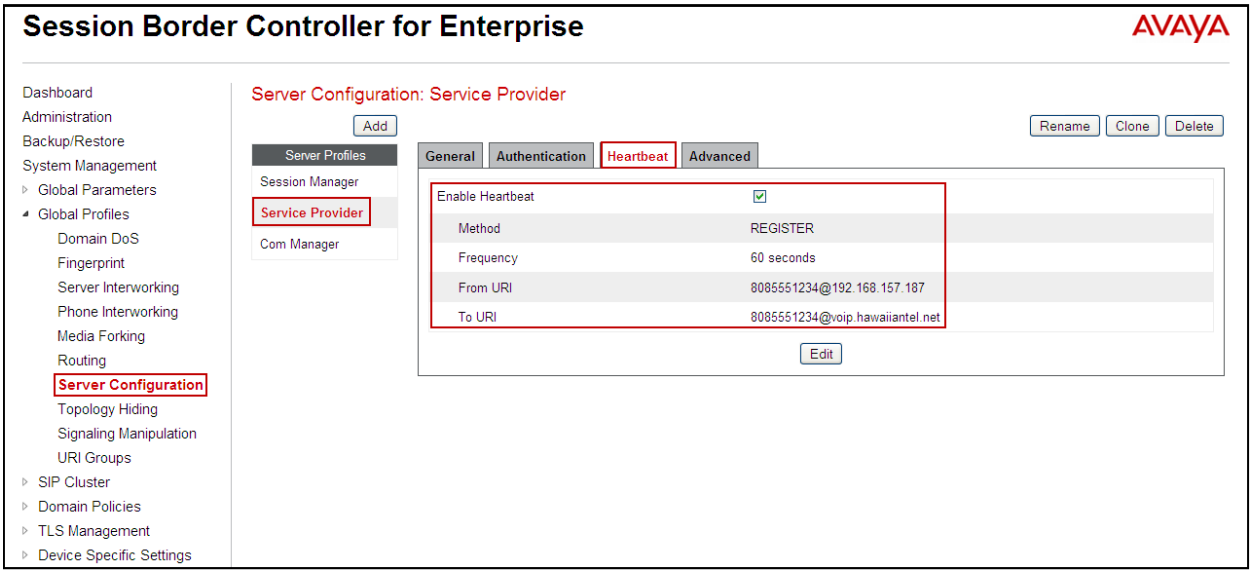
The following screen capture shows the **General** tab of the **Service Provider** Profile.



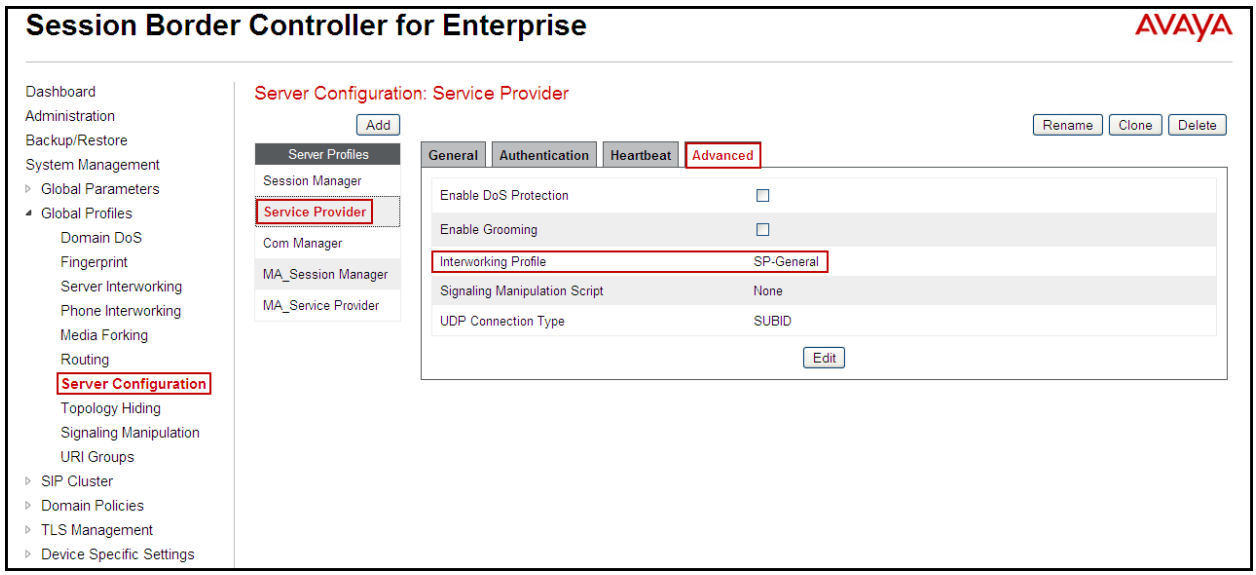
The following screen capture shows the **Authentication** tab of the **Service Provider** Profile.



The following screen capture shows the **Heartbeat** tab of the **Service Provider** Profile.



The following screen capture shows the **Advanced** tab of the **Service Provider** Profile.



7.2.5. Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

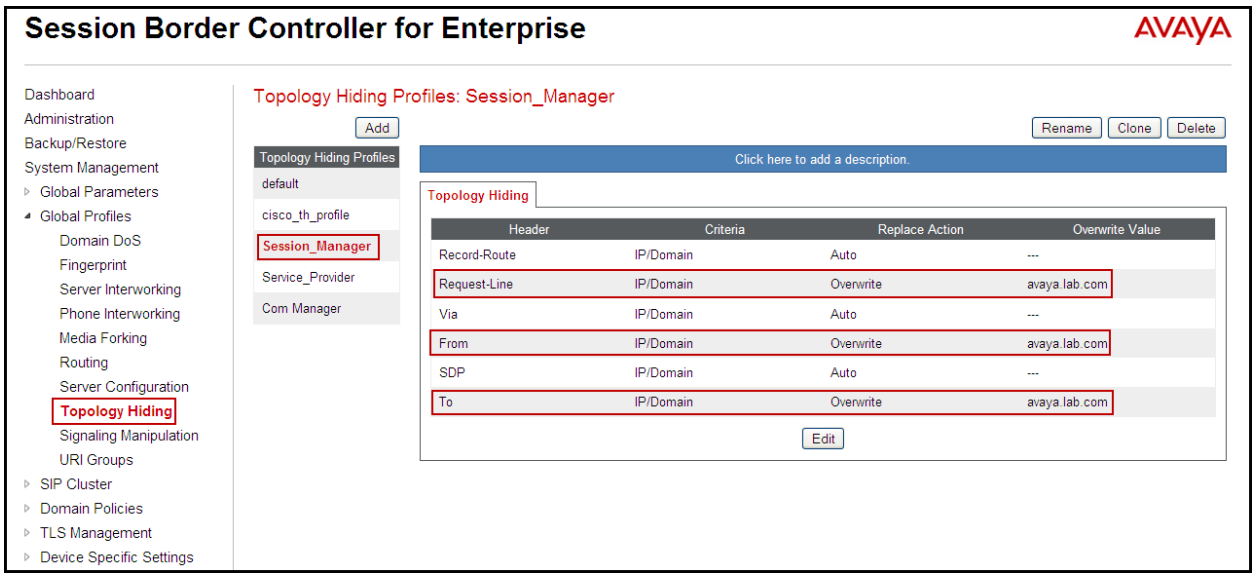
For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name**: **Session_Manager**.
- Click **Finish**.
- Click **Edit** on the newly added **Session_Manager** Topology Hiding profile.
- In the **From** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the enterprise **(avaya.lab.com)** under **Overwrite Value**.
- In the **To** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Enterprise **(avaya.lab.com)** under **Overwrite Value**.

- In the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Enterprise **(avaya.lab.com)** under **Overwrite Value**.

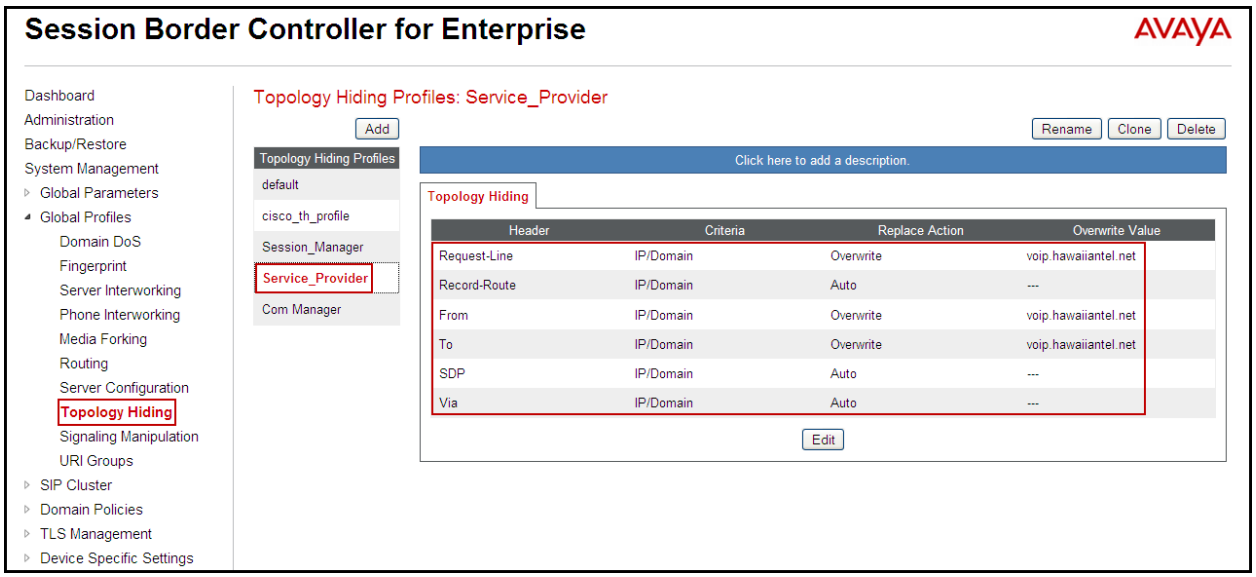
The following screen capture shows the newly added **Session_Manager** profile.



To add the Topology Hiding profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name**: **Service_Provider.**
- Click **Finish**.
- Click **Edit** on the newly added **Service_Provider** Topology Hiding profile.
- In the **From** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider **(voip.hawaiiantel.net)** under **Overwrite Value**.
- In the **To** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider **(voip.hawaiiantel.net)** under **Overwrite Value**.
- In the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider **(voip.hawaiiantel.net)** under **Overwrite Value**.
- Click **Finish**.

The following screen capture shows the newly added **Service_Provider** profile.



7.3. Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

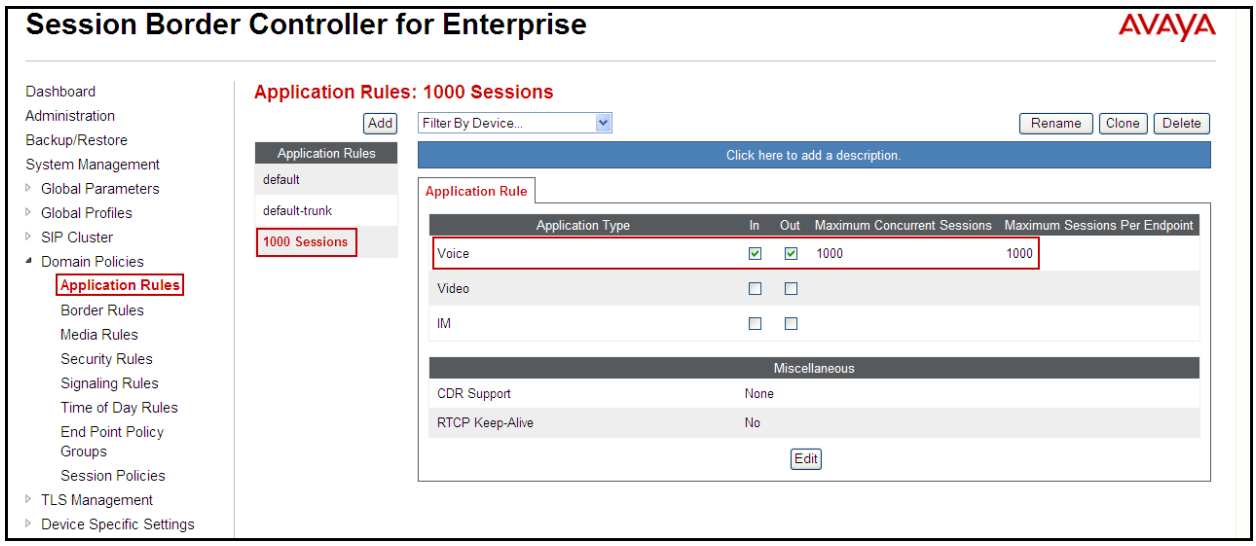
7.3.1. Create Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

From the navigation menu on the left-hand side, select **Domain Policies → Application Rules**

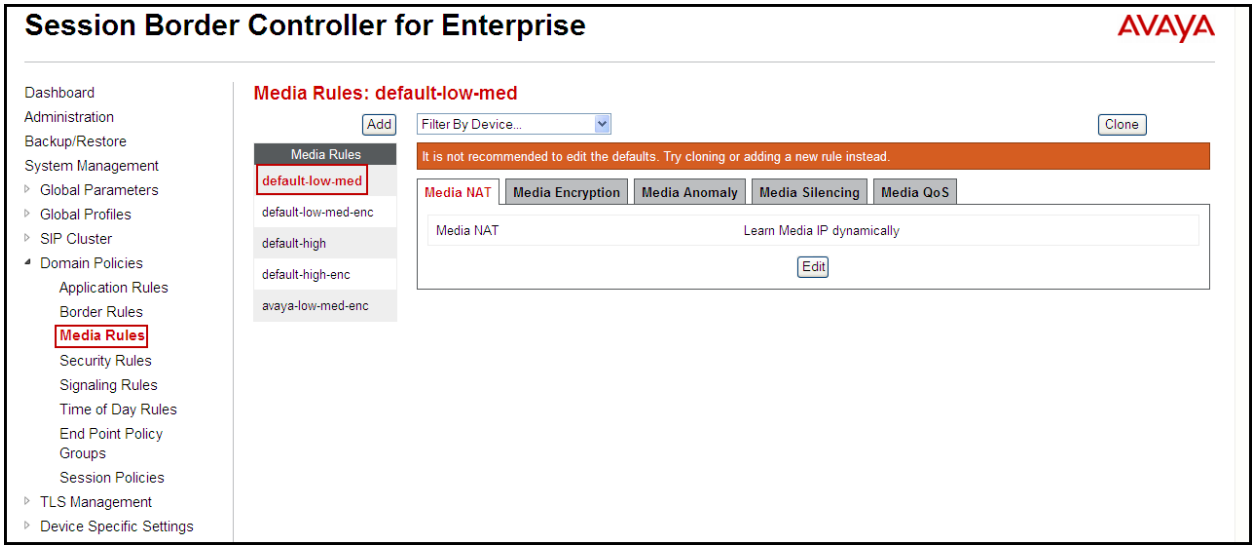
- Select **default** in the **Application Rules** list (not shown).
- Click the **Clone** button on top right of the screen (not shown).
- Name**:** enter the name of the profile, e.g., **1000 Sessions**
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Enpoint** to recommended values: **1000** was used in the sample configuration.
- Click **Finish** (not shown).

The following screen capture shows the newly created application rule.



7.3.2. Media Rules

For the compliance test, the **default-low-med** Media Rule was used.



7.3.3. Signaling Rules

Signaling Rules define the actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

Headers such as Alert-Info, P-Location, P-Charging-Vector and others are sent in SIP messages from Session Manager to the Avaya SBCE for egress to the Service Provider's network. These headers should not be exposed external to the enterprise. For simplicity, these headers were

simply removed (blocked) from both requests and responses for both inbound and outbound calls.

A Signaling Rules was created, to later be applied in the direction of the Enterprise or the Service Provider. To create a rule to block these headers coming from Session Manager from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** in the **Signaling Rules** list.
- Click on **Clone** on top right of the screen.
- Enter a name: **SessMgr_SigRule**. Click **Finish**.

Select the **Request Headers** tab of the newly created Signaling rule.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: AV-Global-Session-ID.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the **Alert-Info** header:

- Select **Add in Header Control.**
- **Header Name: Alert-Info.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the **P-AV-Message-Id** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-AV-Message-Id.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the **P-Charging-Vector** header:

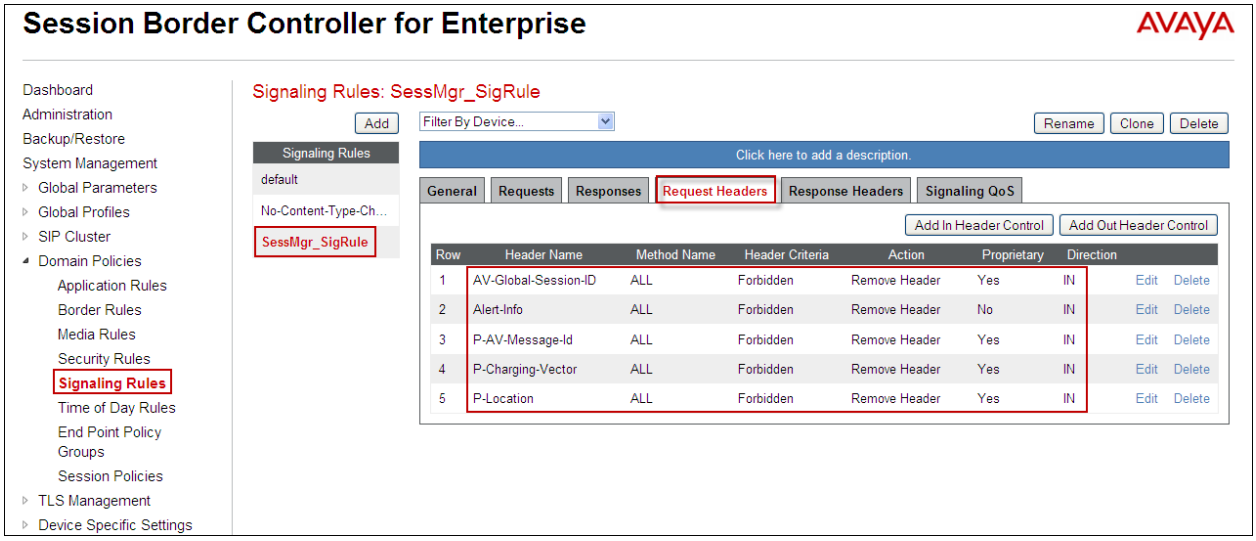
- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-Charging-Vector.**

- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the **P-Location** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-Location.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

The following screen capture shows the **Request Headers** tab of the **SessMgr_SigRule** signaling rule.



Select the **Response Headers** tab.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: AV-Global-Session-ID.**
- **Response Code: 200.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**

- Click **Finish.**

To add the **Alert-Info** header:

- Select **Add in Header Control.**
- **Header Name: Alert-Info.**
- **Response Code: 200.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the **P-AV-Message-Id** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-AV-Message-Id.**
- **Response Code: 200.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

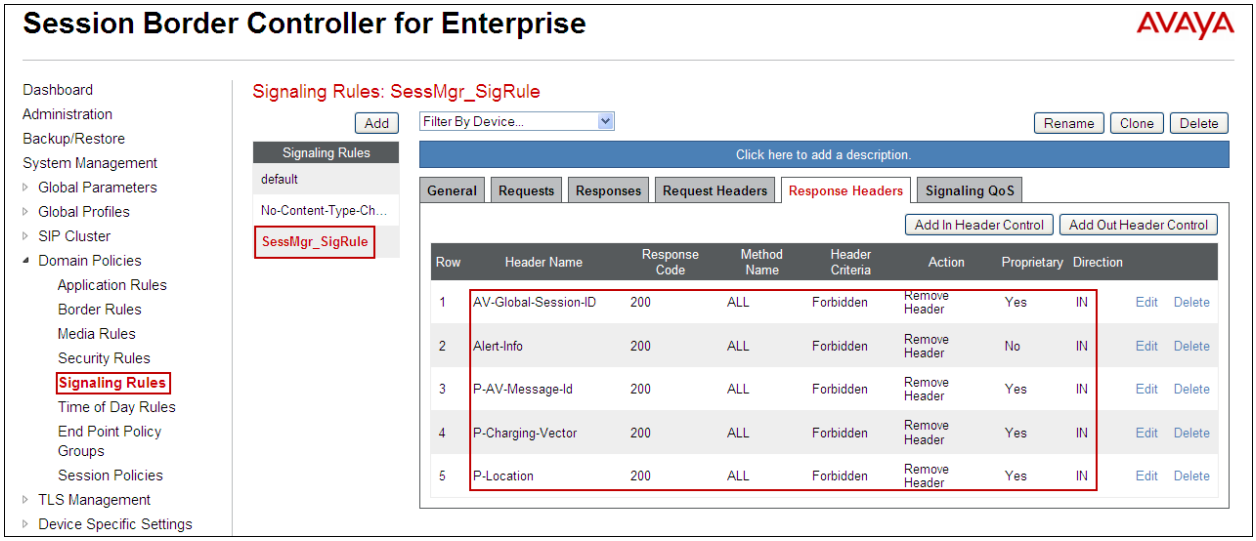
To add the **P-Charging-Vector** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-Charging-Vector.**
- **Response Code: 200.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the **P-Location** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-Location.**
- **Response Code: 200.**
- **Method Name: ALL.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

The following screen capture shows the **Response Headers** tab of the **SessMgr_SigRule** signaling rule.



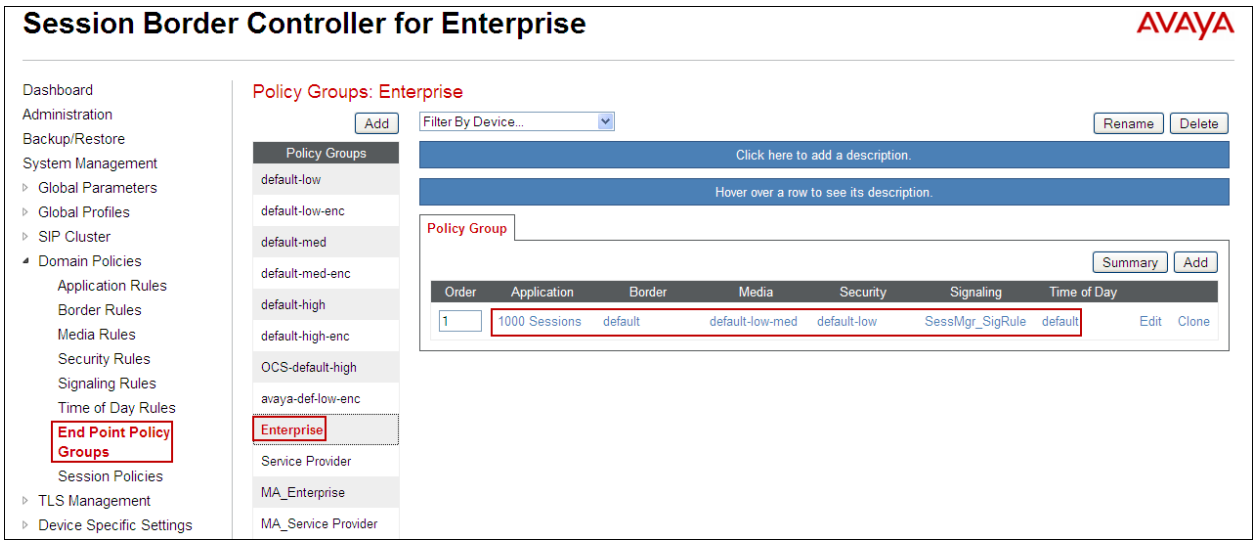
7.3.4. End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add** in the **Policy Groups** section.

- **Group Name: Enterprise**.
- **Application Rule: 1000 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: SessMgr_SigRule.**
- **Time of Day: default.**
- Click **Finish**.

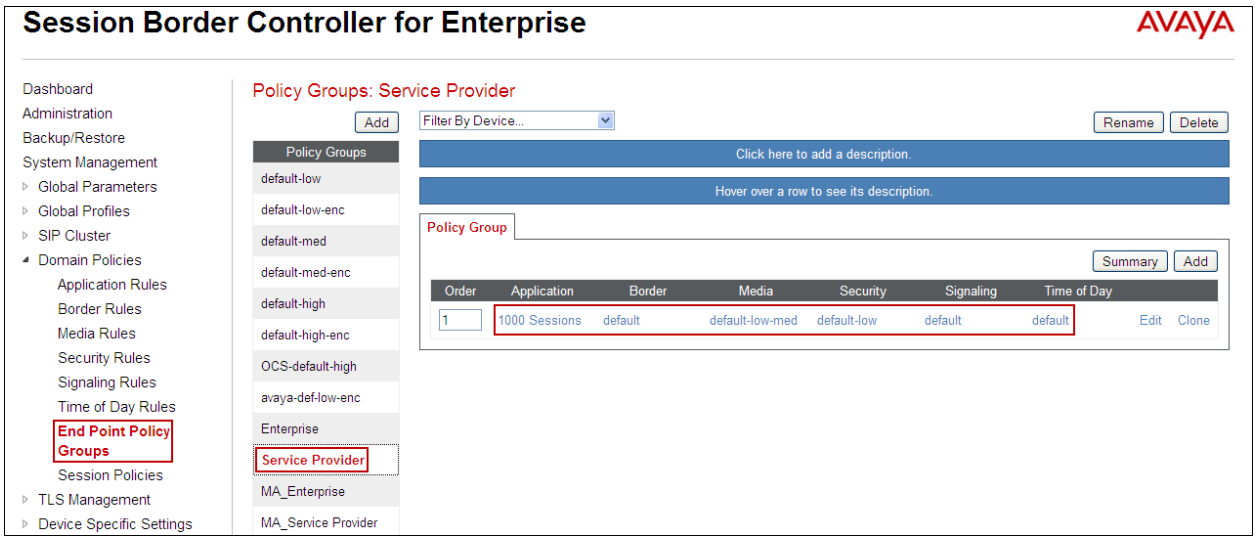
The following screen capture shows the newly added **Enterprise** End Point Policy Group.



Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add** in the **Policy Groups** section.

- **Group Name: Service Provider**.
- **Application Rule: 1000 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- Click **Finish**.

The following screen capture shows the newly added **Service Provider** End Point Policy Group.

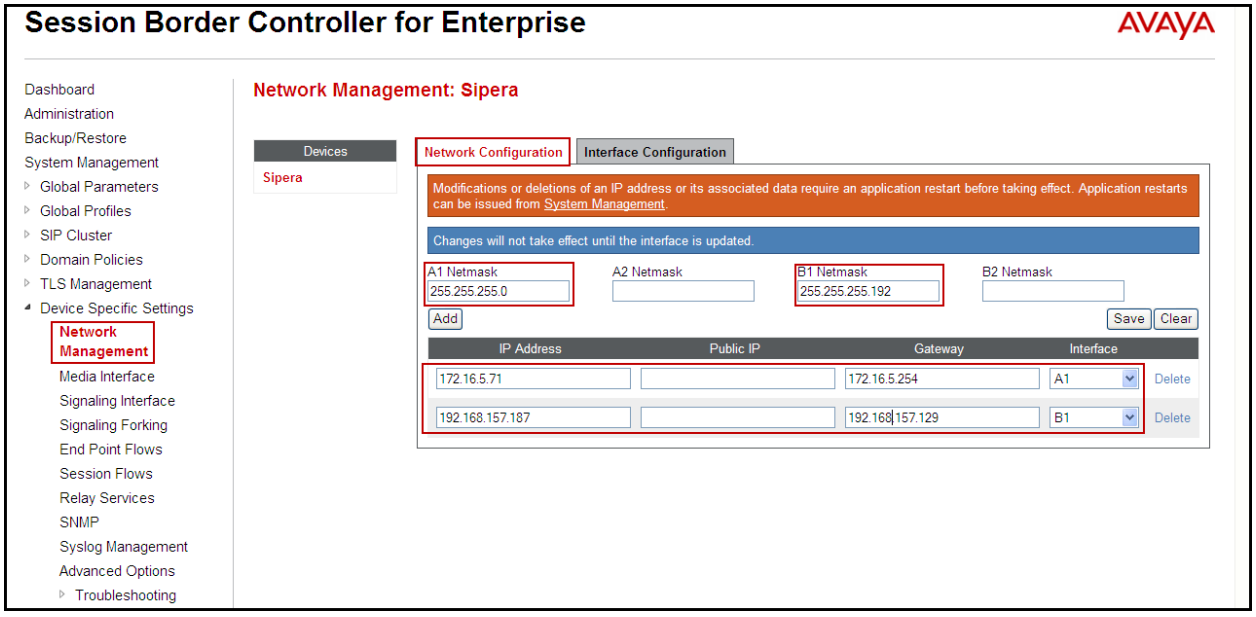


7.4. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

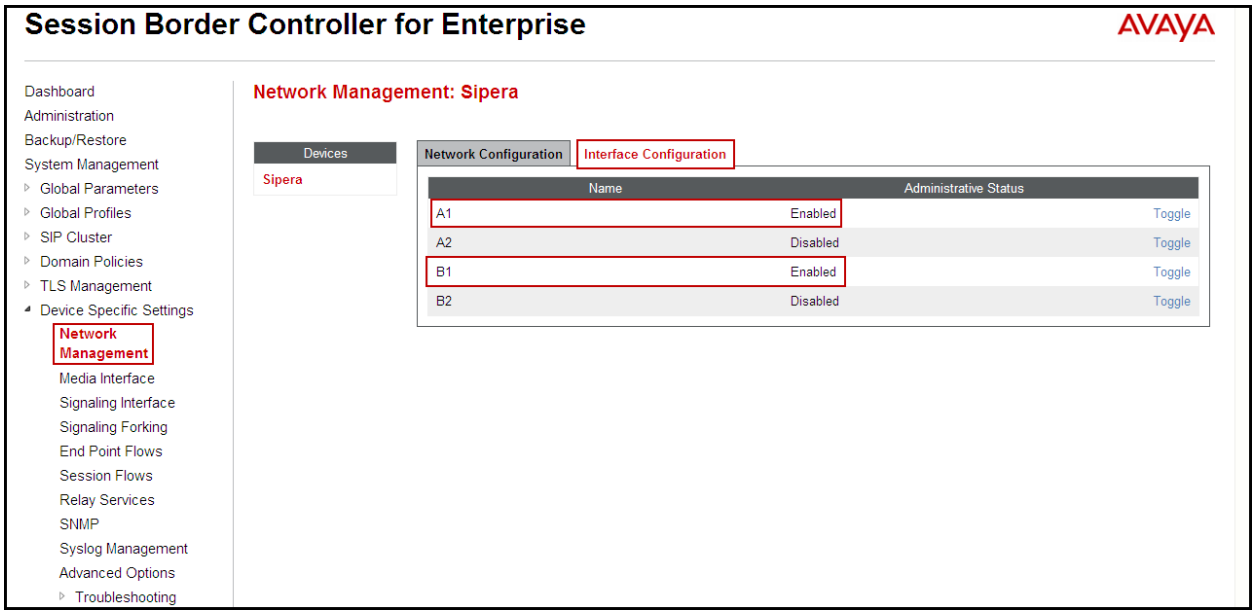
7.4.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.



In the event that changes need to be made to the network configuration information, they could be entered here.

On the Interface Configuration tab, click the **Toggle** control for interfaces **A1** and **B1 to** change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled**, so it is important to perform this step, or the Avaya SBCE will not be able to communicate on any of its interfaces.



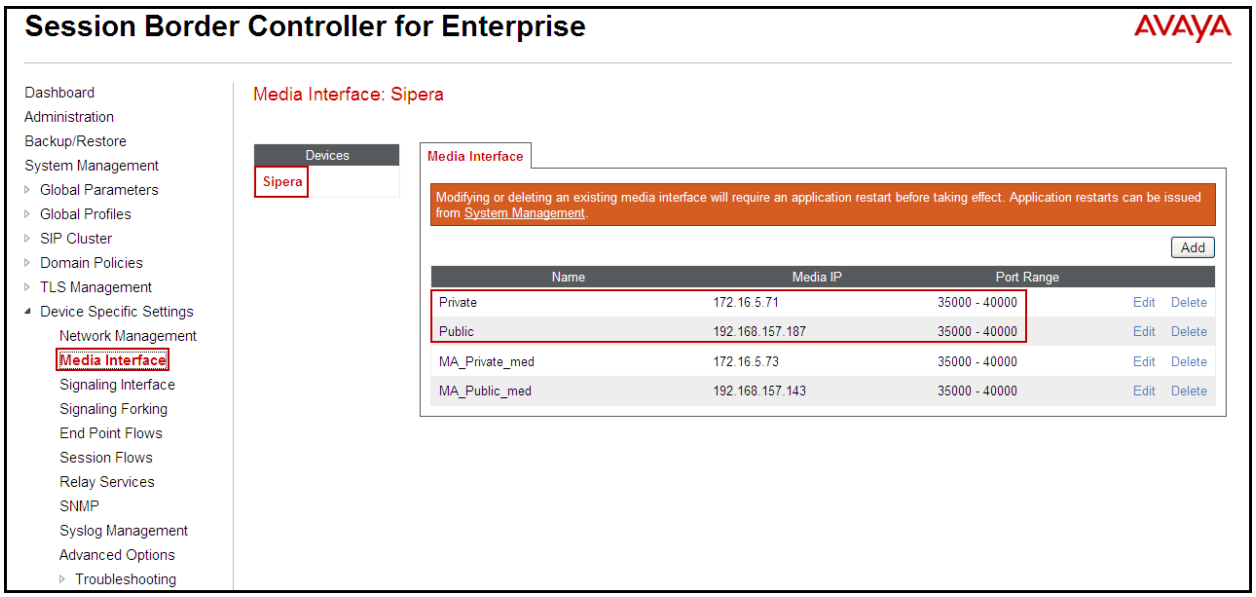
7.4.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE ports range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**.

- Select **Add** in the **Media Interface** area**.**
- **Name: Private.**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range: 35000-40000.**
- Click **Finish.**
- Select **Add** in the **Media Interface** area**.**
- **Name: Public.**
- Select **IP Address: 192.168.157.187** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish.**

The following screen capture shows the added media interfaces.

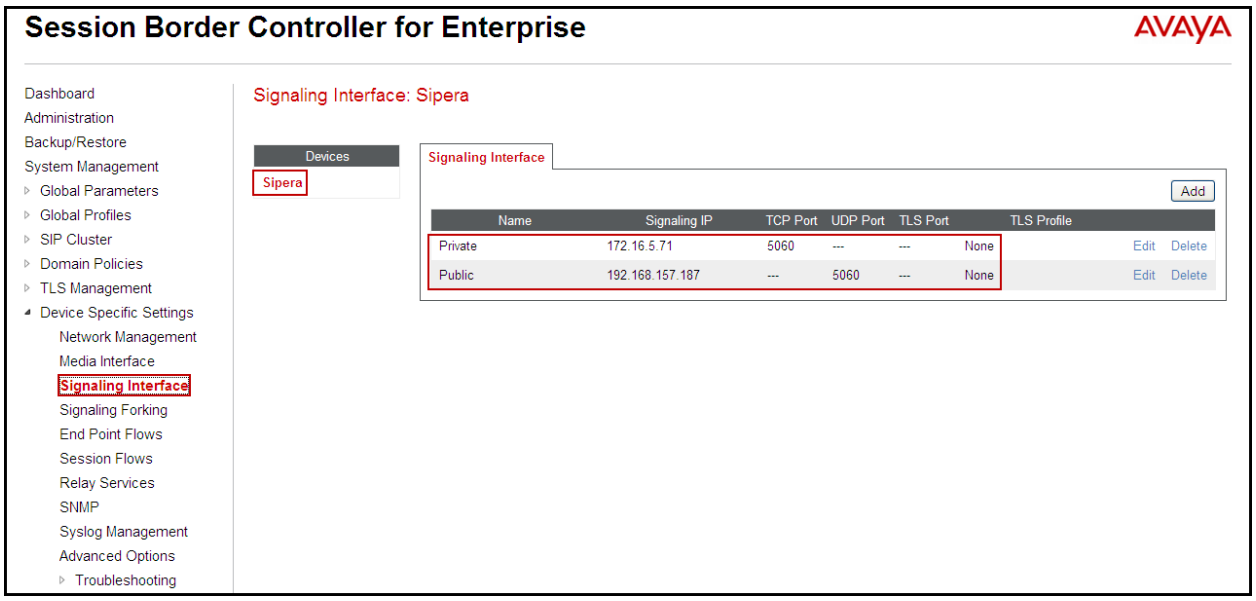


7.4.3. Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**.

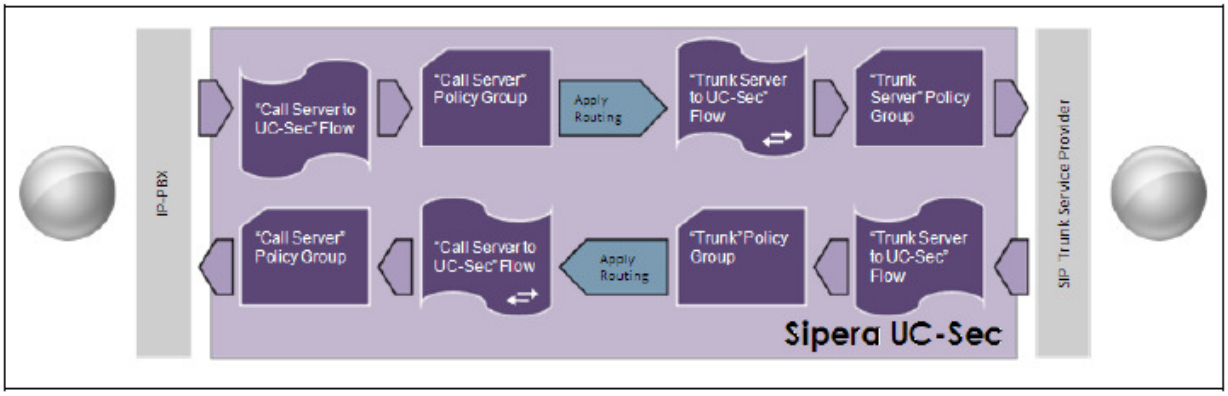
- Select **Add** in the **Signaling Interface** area.
- **Name: Private.**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **TCP Port: 5060.**
- **UDP Port: 5060.**
- Click **Finish.**
- Select **Add** in the **Signaling Interface** area.
- **Name: Public**
- Select **IP Address: 192.168.157.187** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **TCP Port: 5060.**
- **UDP Port: 5060.**
- Click **Finish.**

The following screen capture shows the newly added signaling interfaces.



7.4.4. End Point Flows

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

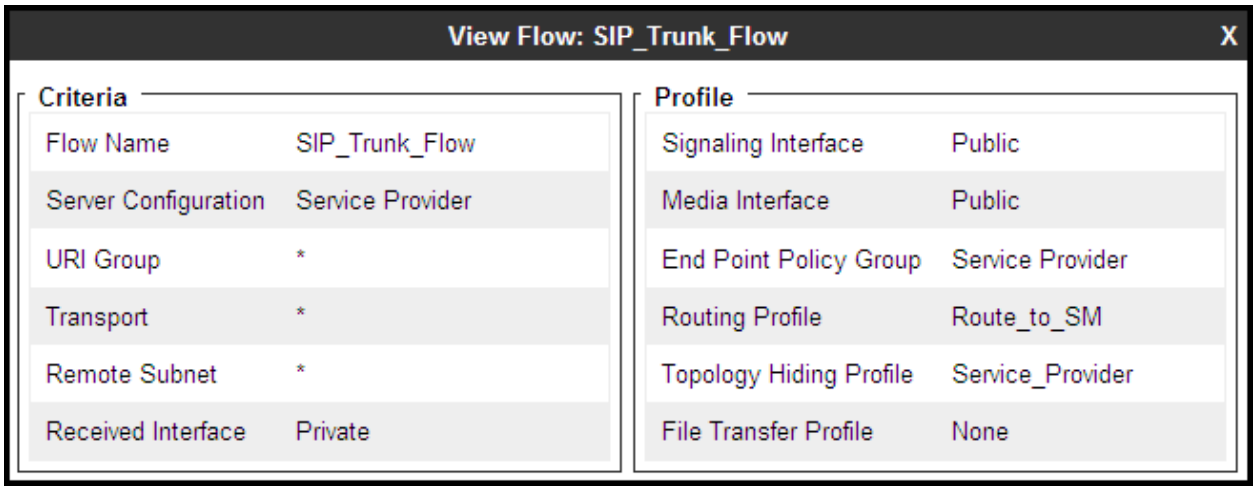


The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, then **Server Flows** tab. Click **Add**.

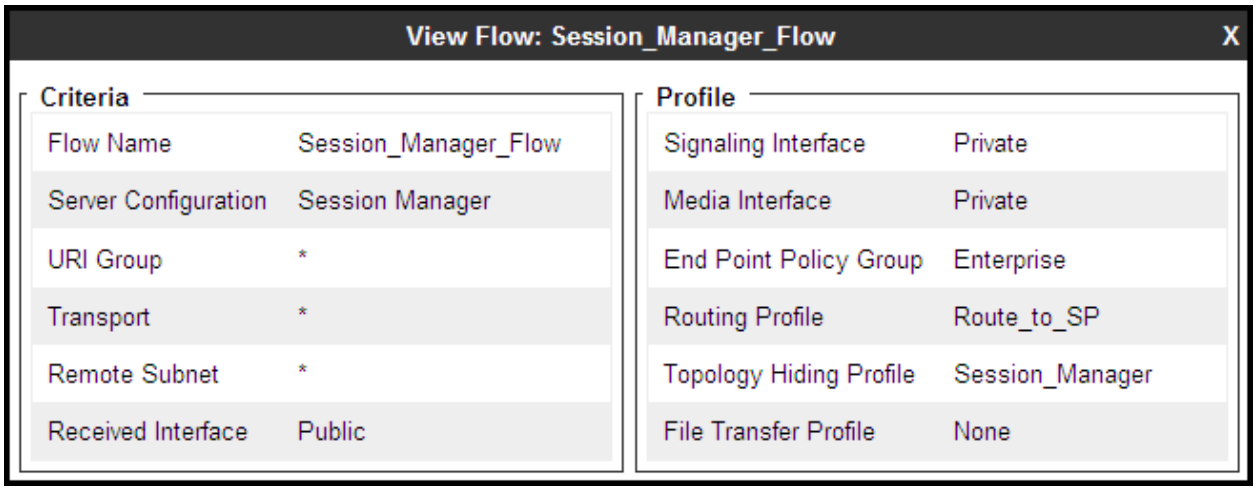
- **Name: SIP_Trunk_Flow.**

- **Server Configuration**: **Service Provider.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private.**
- **Signaling Interface: Public.**
- **Media Interface**: **Public.**
- **End Point Policy Group: Service Provider.**
- **Routing Profile: Route_to_SM** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service_Provider.**
- **File Transfer Profile: None.**
- Click **Finish.**

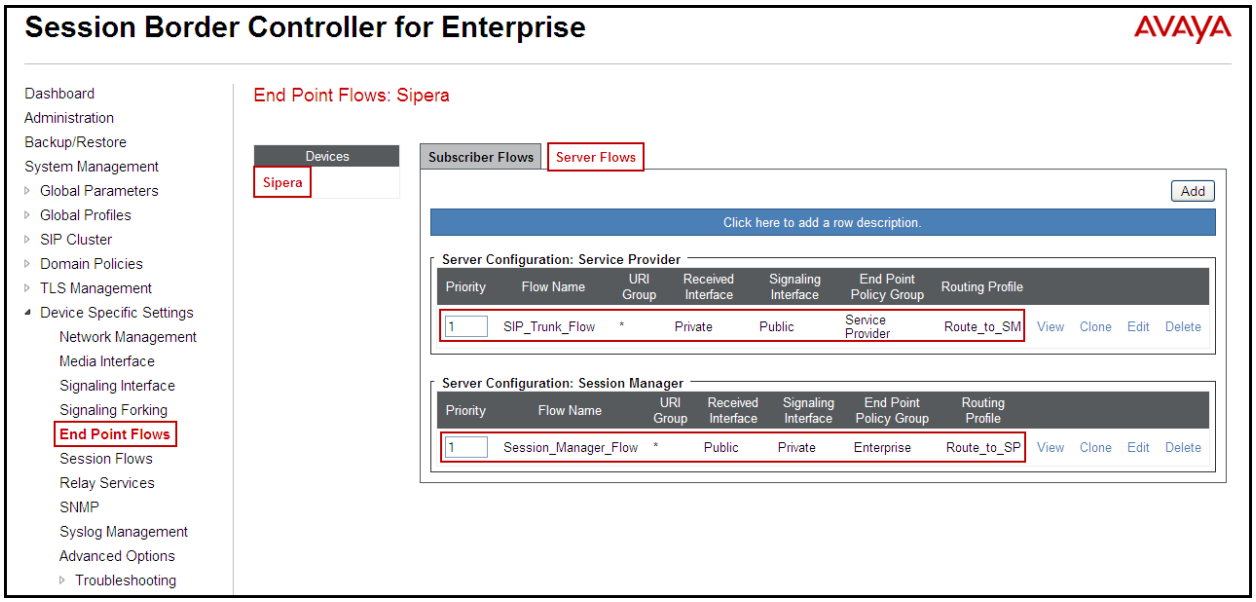


To create the call flow toward Session Manager, click **Add**.

- **Name: Session_Manager_Flow.**
- **Server Configuration**: **Session Manager.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Public**
- **Signaling Interface: Private.**
- **Media Interface**: **Private.**
- **End Point Policy Group: Enterprise.**
- **Routing Profile: Route_to_SP** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Session_Manager.**
- **File Transfer Profile: None.**
- Click **Finish.**



The following screen capture shows the added **End Point Flows.**



8. Hawaiian Telecom SIP Trunk Service Configuration

To use Hawaiian Telecom SIP Trunk service, a customer must request the service from Hawaiian Telecom using the established sales processes. The process can be started by contacting Hawaiian Telecom via the corporate web site at: https://www.hawaiiantel.com/business/Business.aspx or by calling: 1-808-643-0944 and requesting information.

During the signup process, Hawaiian Telecom will require that the customer provide the public IP address used to reach Avaya SBCE at the edge of the enterprise. Hawaiian Telecom will provide the IP address of the SIP proxy/SBC, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, SIP Trunk Registration information, etc. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya SBCE configuration discussed in the previous sections.

9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

1. Communication Manager:

- **list trace station** <extension number>
  Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
  Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
  Displays signaling group service state.
- **status trunk** <trunk group number>
  Displays trunk group service state.
- **status station** <extension number>
  Displays signaling and media information for an active call on a specific station.

2. Session Manager:
    - **traceSM -x** – Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.
    - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Home →Elements → Session Manager →System Tools → Call Routing Test**. Enter the requested data to run the test.

3. Session Border Controller:
   There are several links and menus located on the taskbar in the UC-Sec Control Center that can provide useful diagnostic or troubleshooting information:
    - **Alarms**. Provides information about the health of the SBC.
    - **Incidents.** Provides detailed reports of anomalies, errors, policies violations, etc.
    - **Diagnostics.** This screen provides a variety of tools to aid in troubleshooting the SBC network connectivity and its operation.

   Other useful tools can also be found on the **Troubleshooting Menu,** on the left hand side of the UC-Sec Control Center page.
    - **Packet Capture**. Allows capturing the packets in any of the SBC interfaces, and save them as *pcap* files. From the menu on the left hand side, click **Troubleshooting → Trace → Packet Capture** tab.

10. Conclusion

These Application Notes describe the procedures necessary for configuring Hawaiian Telecom SIP Trunk service with Aura® Communication Manager Release 6.3, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 as shown in **Figure 1**.

Hawaiian Telecom SIP Trunk service passed compliance testing with the observation/limitations noted in **Section 2.2**.

11. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Installing and Configuring Avaya Aura® System Platform*, *Release 6.3, Issue 1, May 2013.*
[2] *Administering Avaya Aura® Communication Manager*, Release 6.3 03-300509, Issue 8, May 2013
[3] *Administering Avaya Aura® Session Manager*, *Release 6.3, Issue 2, June 2013.*
[4] *Administering Avaya Aura® System Manager,* Release 6.3, Issue 1.0, December, 2012.
[5] *Administering Avaya one-X® Communicator, December 2012.*
[6] *Using Avaya one-X® Communicator, Release 6.1, October 2011.*
[7] *RFC 3261 SIP: Session Initiation Protocol,* http://www.ietf.org/.
[8] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, *http://www.ietf.org/*

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 DevConnect Program at devconnect@avaya.com.