Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SaskTel 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 service between the service provider SaskTel 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.

SaskTel SIP Trunk Service provides PSTN access via SIP trunks between the enterprise and SaskTel'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 required to configure Session Initiation Protocol (SIP) trunk service between the service provider SaskTel 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 an Avaya SIP-enabled enterprise solution with SaskTel 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 Communication Manager, Session Manager and the Avaya SBCE to SaskTel 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 for 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:

- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to the DID numbers assigned by SaskTel. Incoming PSTN calls were terminated to the following endpoints: Avaya 9600 Series IP Telephones (H.323 and SIP), Avaya 96x1 Series IP Telephones (H.323 and SIP), Avaya 2420 Digital Telephones, Avaya one-X® Communicator (H.323 and SIP), analog telephones and Fax machines.
- Outgoing calls to the PSTN were routed via SaskTel's network to the various PSTN destinations.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 deskphones (SIP), Avaya one-X® Communicator (SIP) and Avaya Flare® Experience for Windows (SIP).
- 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 endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. (Testing was performed with codecs: G.711MU, G.711A and G.729A, SakTel's preferred codec order).
- 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).
- 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.
- 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 and emergency calls are supported but were not tested as part of the compliance test
- Station initiated Network Call Redirection (NCR) using the REFER method was not tested.
- Vector based Network Call Redirection (NCR) using REFER or 302 methods was not tested.
- SIP User-to-User Information (UUI) was not tested.
- T.38 fax is not supported by SaskTel; therefore T.38 fax was not tested.
- G.711 fax pass-through is available with Communication Manager on a "best effort" basis, it's not guaranteed that it will work; therefore G.711 fax pass-through is not recommended with this solution and was not tested.

2.2. Test Results

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

- **Station initiated Network Call Redirection (NCR) using the REFER method and Vector based NCR using the REFER and 302 methods** – A bug was found in Communication Manager software release SP 2.1 and SP3 that prevents the use of the REFER or 302 Network Call Redirection (NCR) methods. In release SP 2.1 and SP3, Communication Manager is incorrectly blocking the use of REFER and 302 NCR methods, this includes station initiated call transfers using the REFER method and Vector based NCR using the REFER and 302 methods. For this reason, testing was done with **Network Call Redirection** set to "**n**" under the Trunk Group configuration described in **Section 5.7**. This issue is under investigation by Avaya.

- **Fax** – T.38 fax is not supported by SaskTel; SaskTel only supports G.711 fax pass-through. G.711 fax pass-through is available with Communication Manager on a "best effort" basis, it's not guaranteed that it will work; therefore G.711 fax pass-through is not recommended with this solution and was not tested.
- **Call Display on Transferred Calls to PSTN** – Caller ID display is not updated on PSTN phones involved with call transfers from 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/SaskTel solution. It is listed here simply as an observation.

2.3. Support

For support on SaskTel systems, call Toll Free at 1-888-773-2122 or visit the corporate Web page at: https://www.sasktel.com/support

3. Reference Configuration

Figure 1 below illustrates the test configuration used. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the SaskTel 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 and SIP).
- Avaya 96x1-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya Flare® Experience for Windows (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 flow through the Avaya Session Border Controller for Enterprise. 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 SaskTel 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 the Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the enterprise IP network is SIP over TLS. Note that for ease of troubleshooting during the 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 either masked or digits have been blurred out.

One SIP trunk group was created between Avaya Aura® Communication Manager and 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 the 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 are 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 SaskTel's network.

Note: Remote worker was tested as part of this solution; the configuration necessary to support remote workers is beyond the scope of these Application Notes and is not discussed in this document.

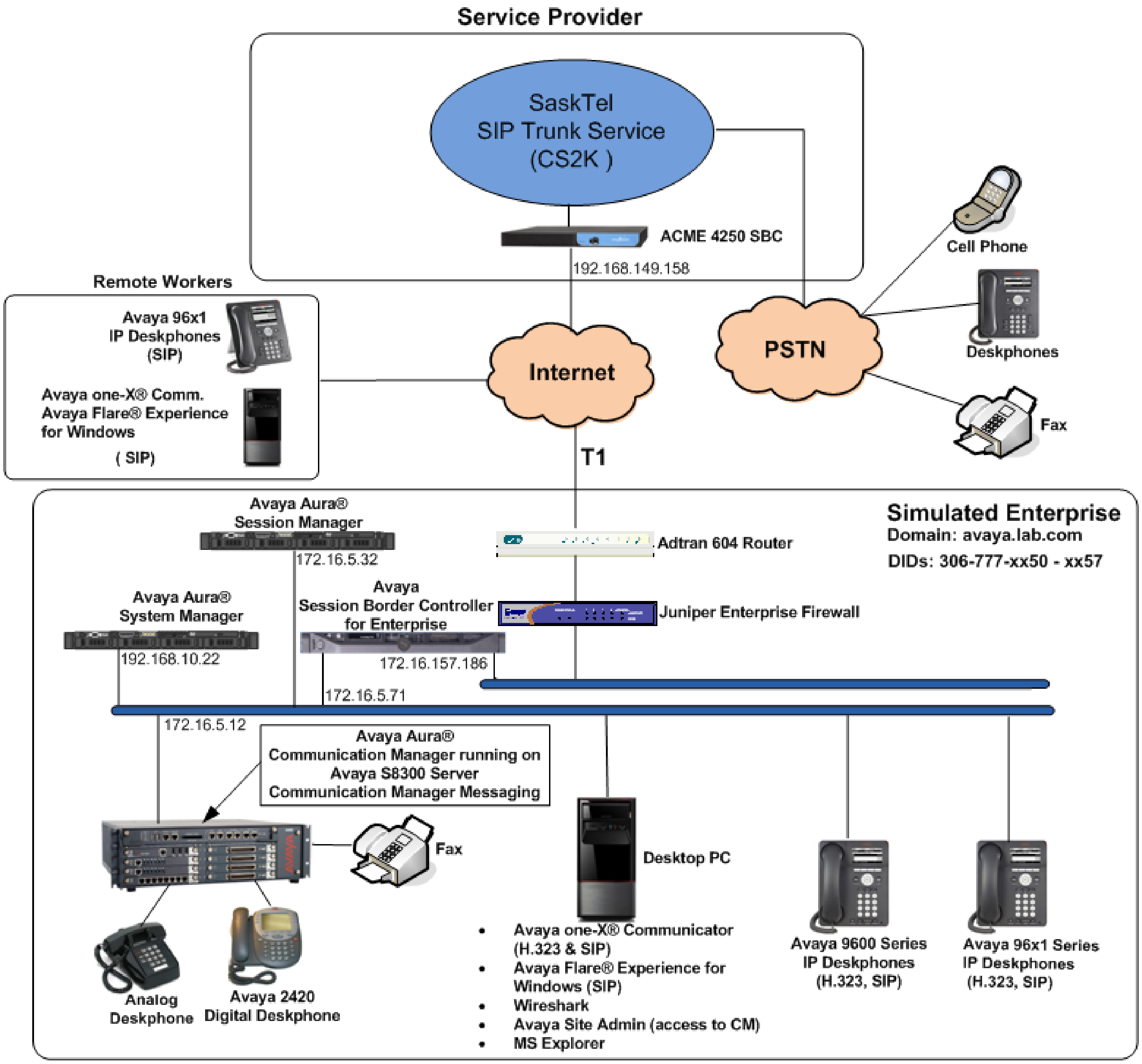


Figure 1: Avaya SIP-enabled Enterprise Solution and SaskTel SIP Trunk Service

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.	6.3.3 (Service Pack 3) (03.0.124.0-21172)
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3.5 (Service Pack 5) (6.3.5.0.635005)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.5 (Feature Pack 3) Build No. 6.3.0.8.5682-6.3.8.2826 Software Update Rev. No. 6.3.5.5.2017
G450 Gateway	34.5.1
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.1.Q07
Avaya Aura® Integrated Management Site Administrator	6.0.07
Avaya Aura® Communication Manager Messaging (CMM)	CMM 6.3 (Service Pack 1)
Avaya one-X® Communicator (SIP & H.323)	6.2.0.04-GA
Avaya Flare® Experience for Windows (SIP)	1.1.4.23
Avaya 9600 Series IP Telephones (H.323)	Avaya one-X® Desk phone Edition Version S3.212A
Avaya 9600 Series IP Telephones (SIP)	Avaya one-X® Deskphone SIP Version 2.6.11.4
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X® Deskphone H.323 Version 6.3037
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X® Deskphone SIP Version 6.3.0.73
Avaya 2420 Series Digital Telephone	--
Lucent Analog Phone	--
Fax Machines	--
SaskTel	
CS2K	CVM16
ACME Session Border Controller (4250)	SC6.2.0 MR-5 GA (Build 777)

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 Communication Manager. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from SaskTel. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and Session Manager has been previously completed.

In configuring 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 Communication Manager configuration was performed using the 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 SIP trunks to the service provider. The example below 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  2
            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 this field set to ***none***.

```
change system-parameters features                               Page   1 of  20
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                     Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

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 Communication Manager **(procr**), and for 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. SaskTel 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; this is SaskTel's preferred codec order. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 2

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

On **Page 2**, set the **Fax Mode** to ***off*** (T.38 fax is not supported by SaskTel).

```
change ip-codec-set 2                                          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
```

Use the **change ip-codec-set** command to define a list of codecs to use for telephones within the enterprise. 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 Communication Manager and Session Manager for use by the service provider SIP 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 Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). Note that 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 Communication Manager and Session Manager. The transport method used between Session Manager and the Avaya SBCE is specified as TCP in **Sections 6.5**. Lastly, the transport method between the Avaya SBCE and SaskTel 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 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 for SIP 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 Communication Manager detects its peer as Session Manager.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Avaya S8300D Server running 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 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 Communication Manager to redirect media traffic directly between the inside IP of the Avaya SBCE 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 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 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 SaskTel. 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 ***n*** to direct Communication Manager not to use the SIP REFER message for transferring calls off-net to the PSTN (Refer to **Section 2.2)**. 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 SaskTel. 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? 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 numbers are 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 enterprise extensions 3040 – 3042, 3045 – 3047, 3049 and 5016. These 10-digit numbers were used for the outbound calling party information on the service provider trunk when calls were originated from these extensions. Note that two digits of the DID numbers have been blurred out for security reasons.

```
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: 10
 4  5                                               4        Maximum Entries: 540
 4  3040             2           306777  50         10
 4  3041             2           306777  51         10
 4  3042             2           306777  57         10
 4  3045             2           306777  55         10
 4  3046             2           306777  56         10
 4  3047             2           306777  52         10
 4  3049             2           306777  54         10
 4  5016             2           306777  53         10
```

In a real customer environment, normally DID numbers are comprised of the 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. The example shown in the screenshot below is assuming that the local extensions in the DID numbers begin with a 1 (e.g., 306777**1**xxx).

```
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: 10
 4  5                                               4        Maximum Entries: 540
 4  1                2           306777             10
```

5.9. . Inbound Routing

DID numbers received from SaskTel were mapped to extensions 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 number. Note that two digits of the DID numbers have been blurred out for security reasons.

```
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 306777  50         10  3040
 public-ntwrk   10 306777  51         10  3041
 public-ntwrk   10 306777  52         10  3047
 public-ntwrk   10 306777  53         10  5016
 public-ntwrk   10 306777  54         10  3049
 public-ntwrk   10 306777  55         10  3045
 public-ntwrk   10 306777  56         10  3046
 public-ntwrk   10 306777  57         10  3042
 public-ntwrk
```

In a real customer environment, where DID numbers are usually comprised of a local extension plus a prefix, a single entry can be applied for all extensions, like in the example shown 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 306777             6
 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: Serv. Provider
                             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
```

Note: To save all Communication Manager provisioning changes, enter the command **save translations**.

6. Configure Avaya Aura® Session Manager

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

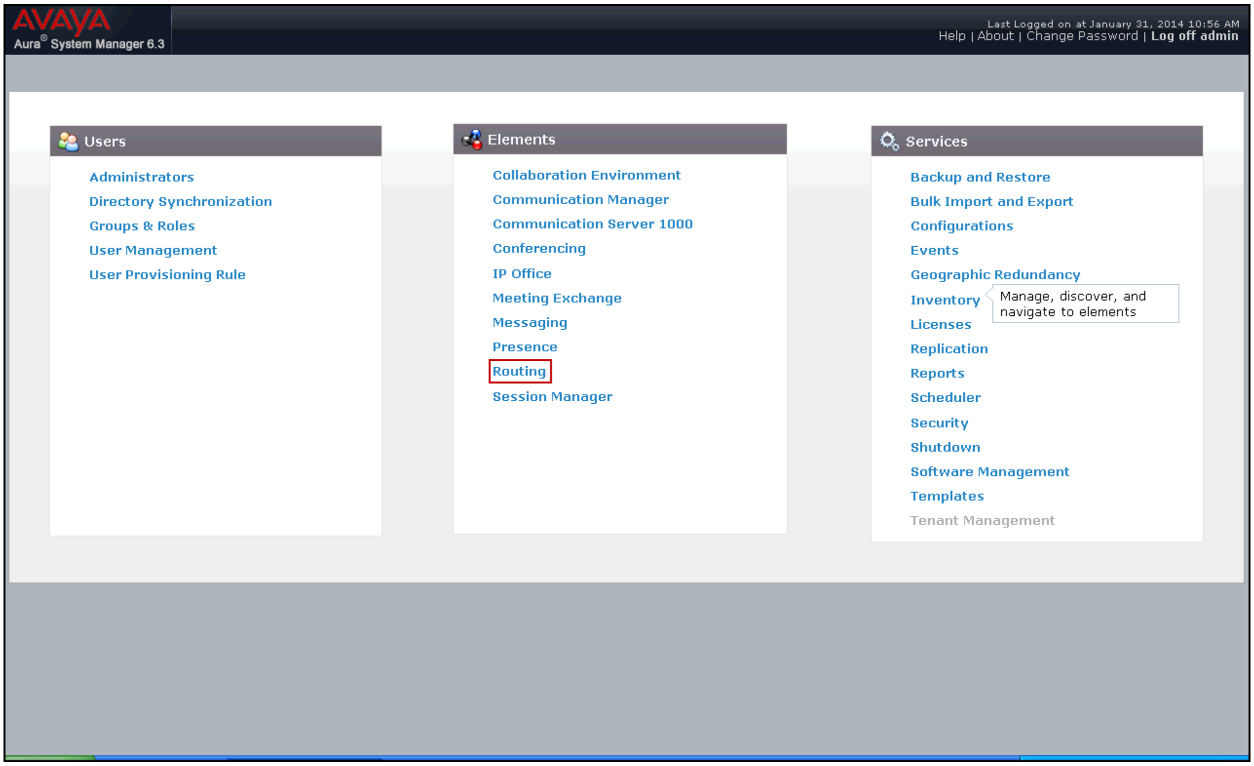
- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager 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
- Session Manager, corresponding to the Session Manager server to be managed by 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 Session Manager installation or may not be required. This includes items such as certain SIP domains, Locations, Adaptations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

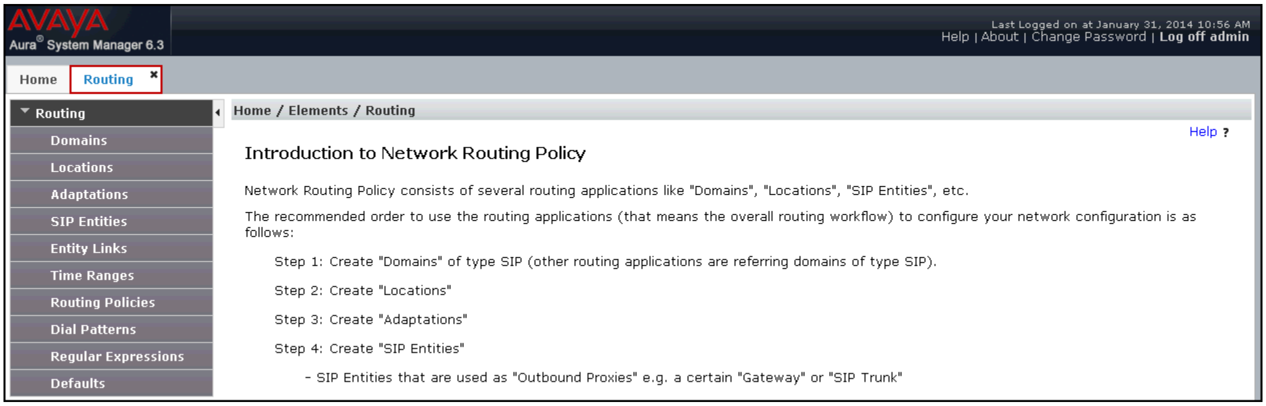
Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of 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.



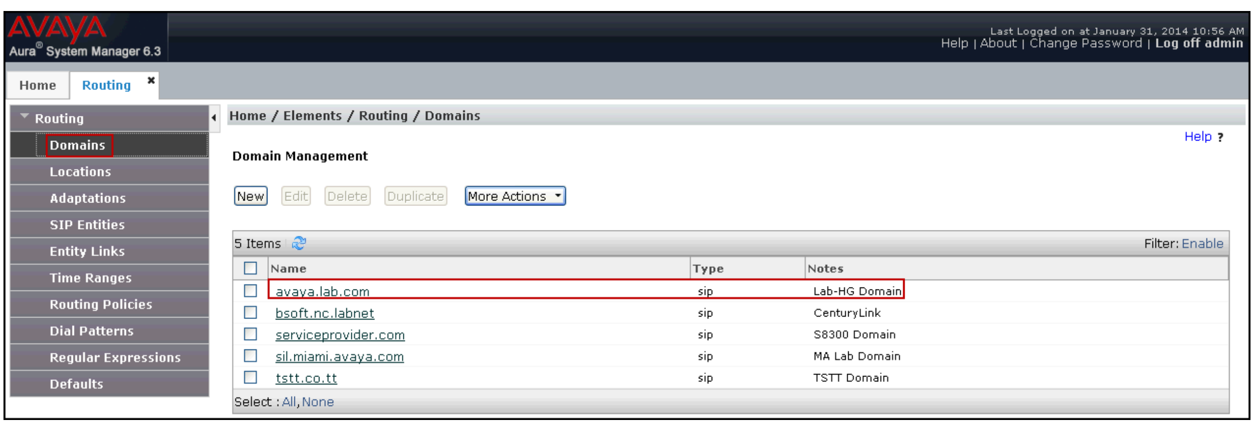
6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test the enterprise domain **avaya.lab.com** was used.

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** to save (not show).

The screen below shows the entry for the enterprise domain **avaya.lab.com**.



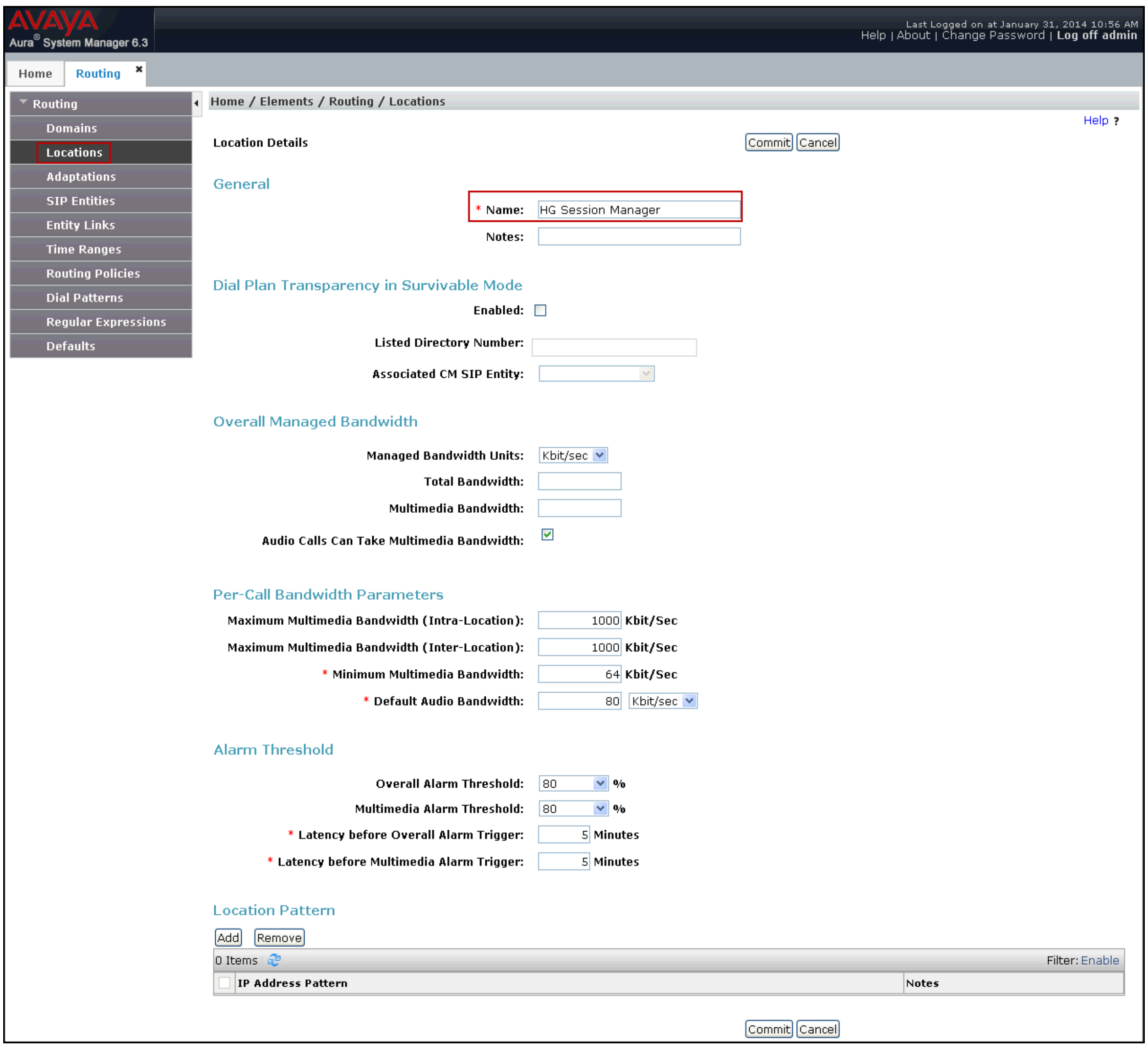
6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the 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).

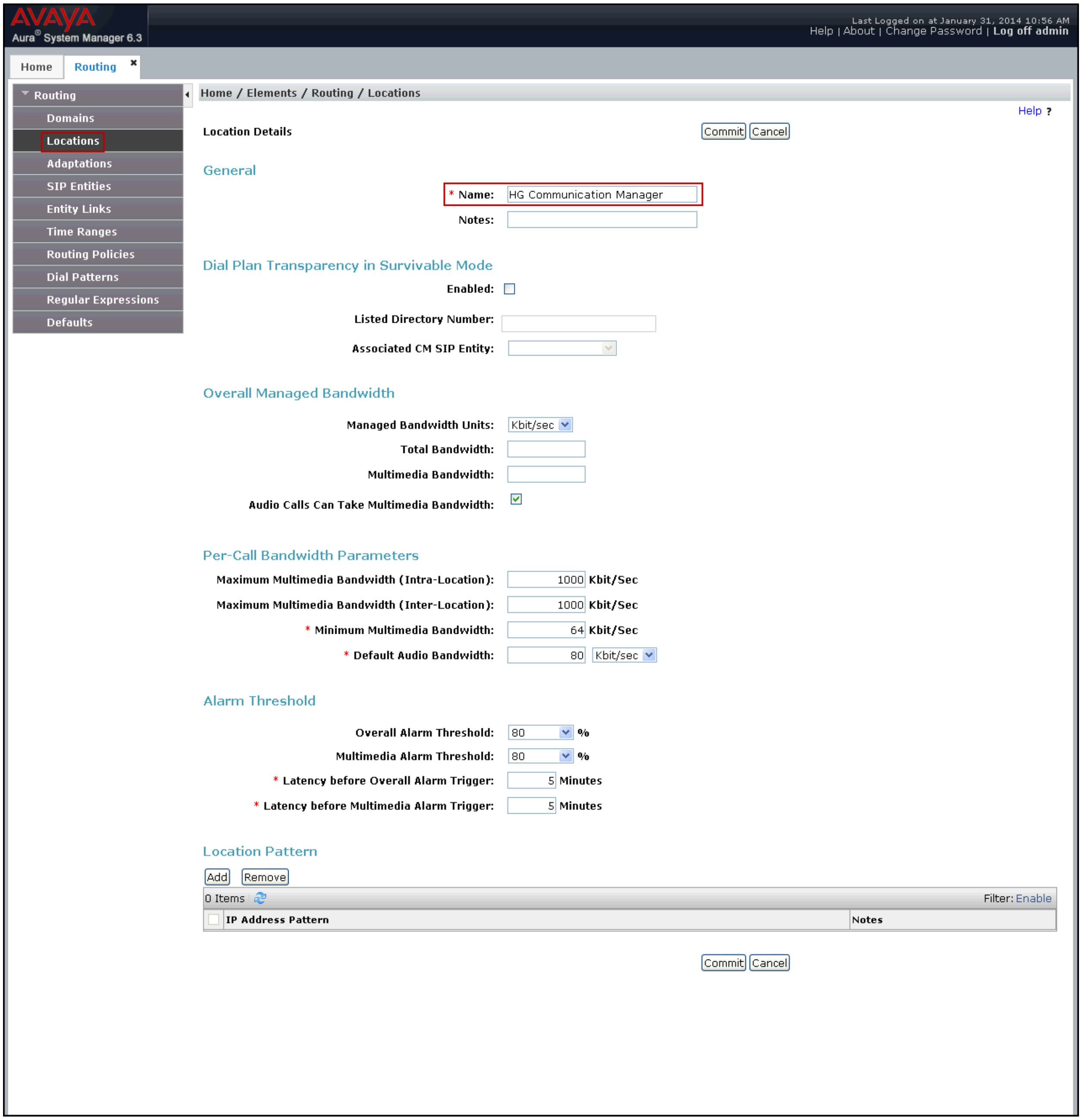
In the **General** section, enter the following values. Use default values for all remaining fields:

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

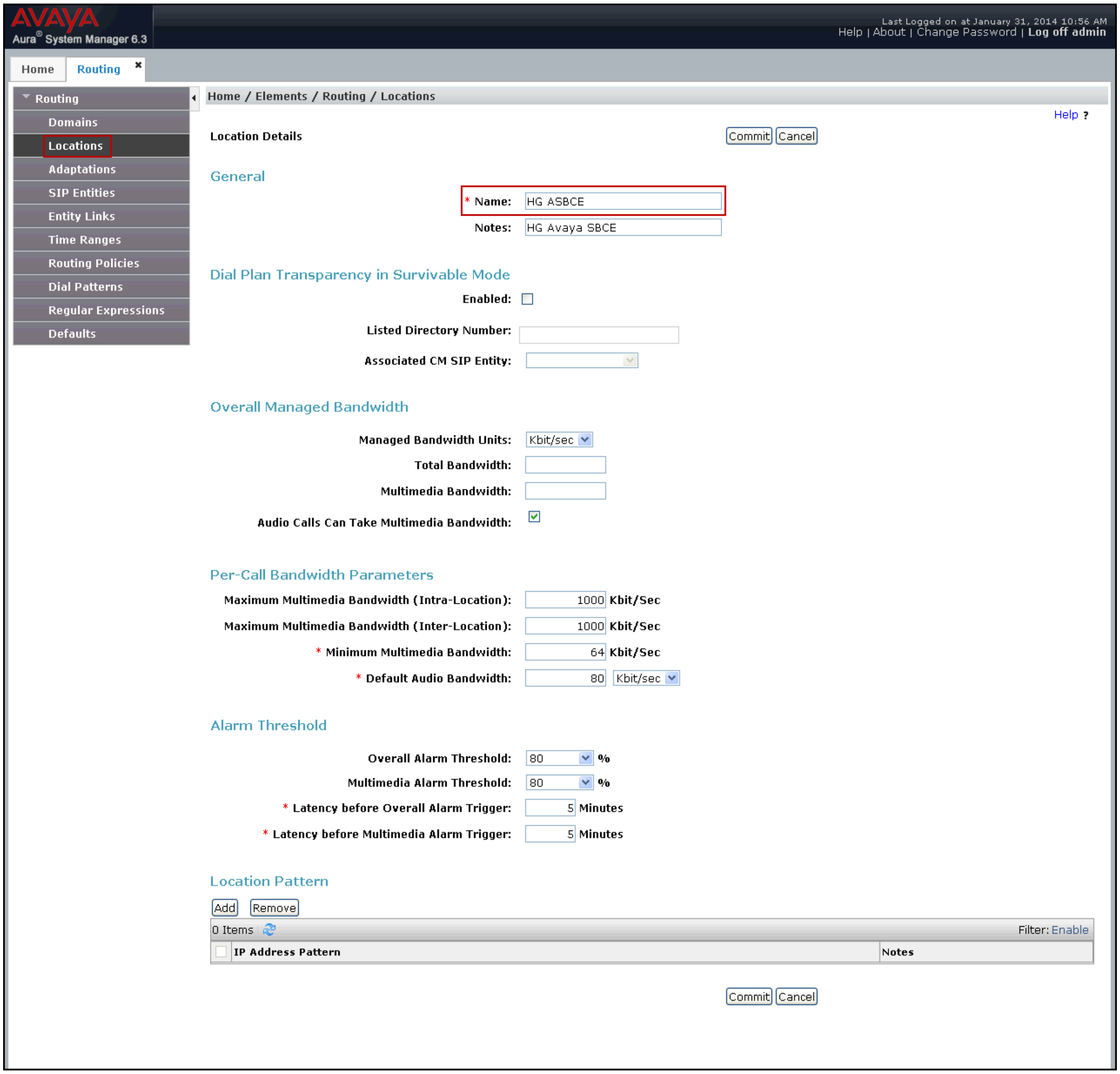
The screen below shows the **HG Session Manager** location. This location will be assigned later to the SIP Entity corresponding to Session Manager.



The following screen shows the **HG Communication Manager** location. This location will be assigned later to the SIP Entity corresponding to Communication Manager.



The following screen shows the **HG ASBCE** location. This location will be assigned later to the SIP Entity corresponding to the Avaya SBCE.



6.4. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. 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 interface that is used for SIP signaling.
- **Type:** Enter ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***Other*** for the Avaya SBCE.
- **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 Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

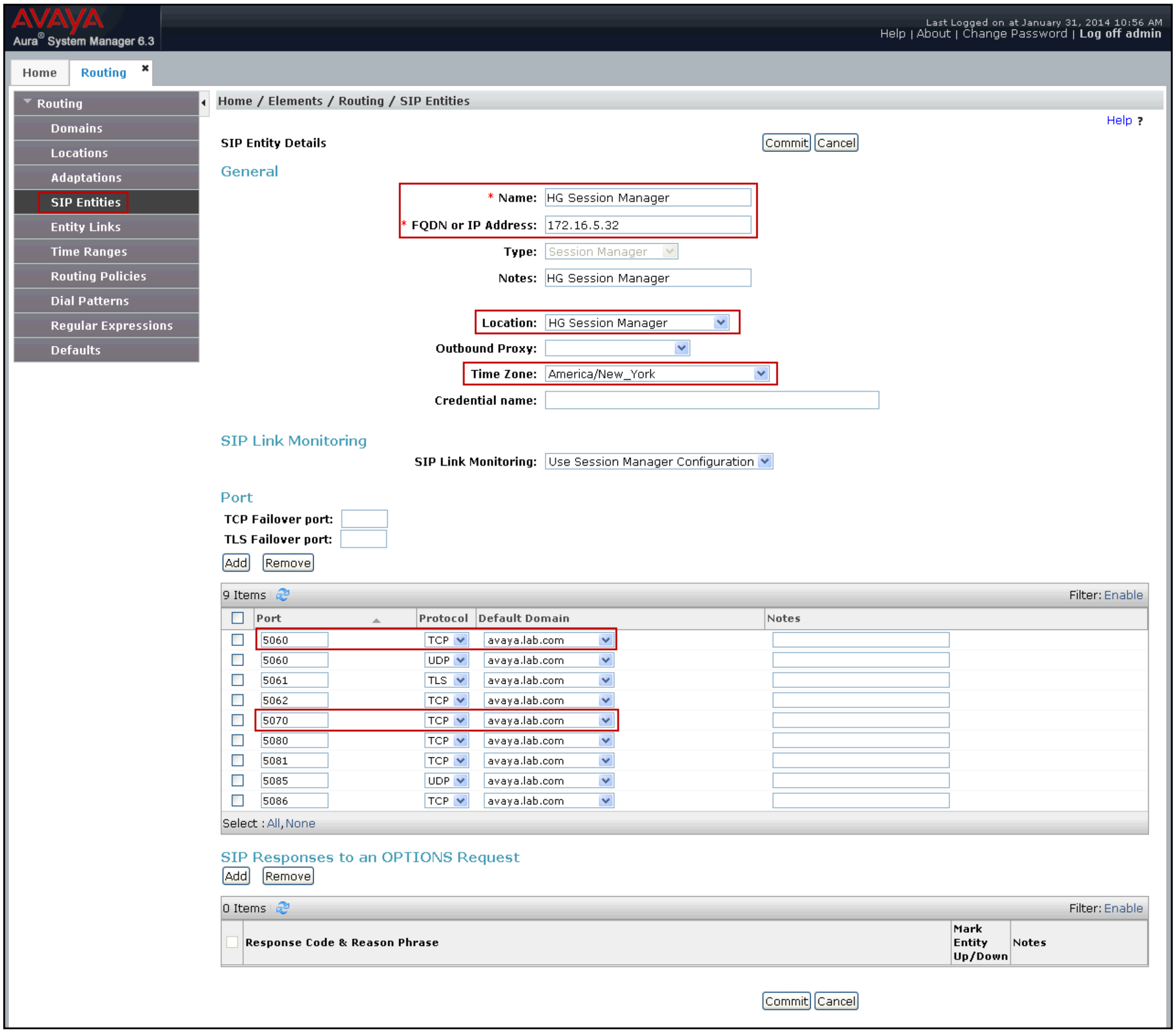
In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

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

For the compliance test, only two Ports were used:

- **5060** with **TCP** for connecting to the Avaya SBCE.
- **5070** with **TCP** for connecting to Communication Manager.

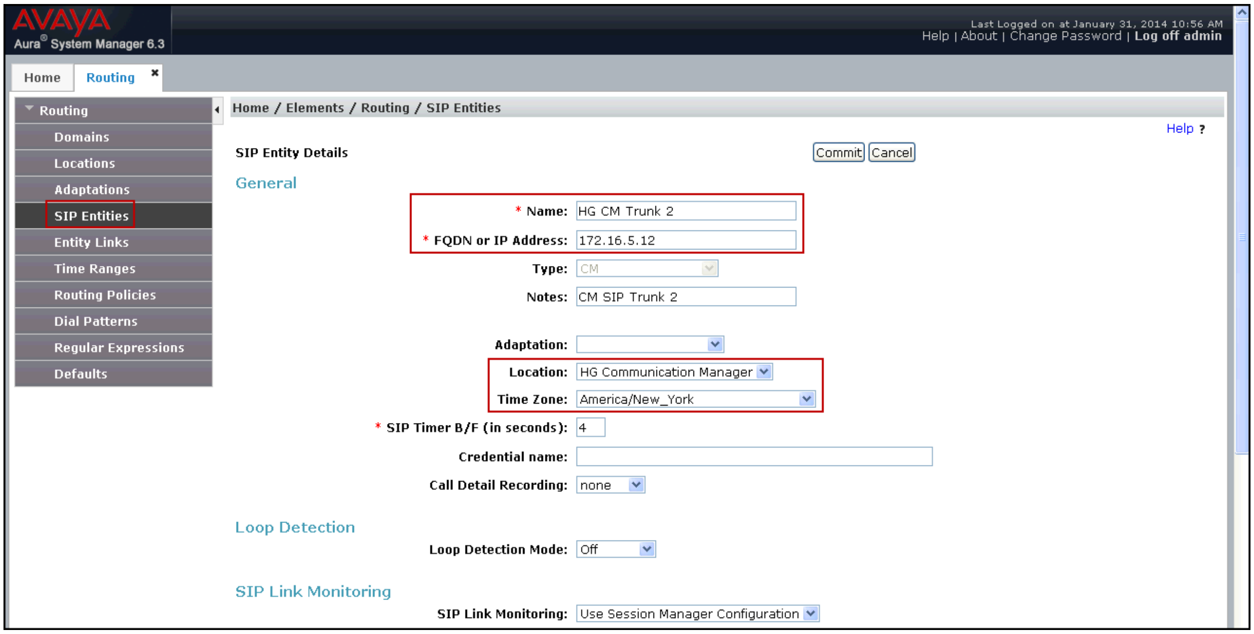
The following screen shows the addition of the Session Manager SIP entity. The name ***HG Session Manager***, the IP address of the Session Manager signaling interface and the Location ***HG Session Manager*** created in **Section 6.3** was used.



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

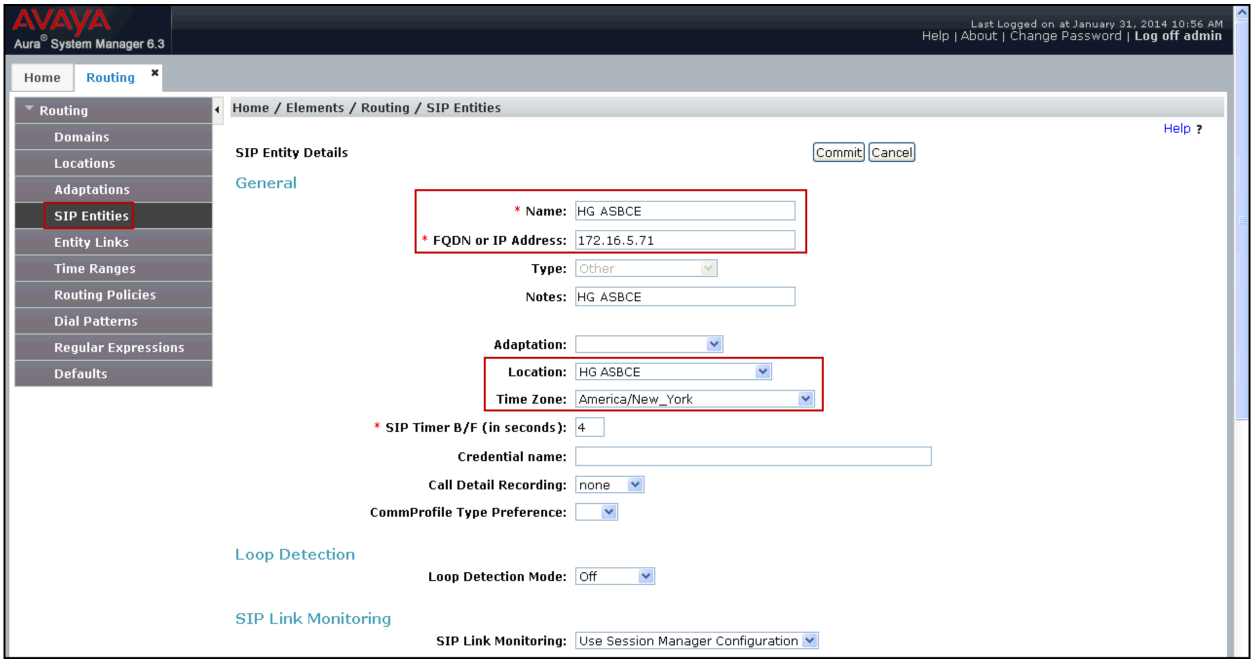
A separate SIP entity for Communication Manager is required in order to route traffic from Communication Manager to the Service Provider.

The name ***HG CM Trunk 2***, the IP of the Avaya S8300D Server running Communication Manager and the location ***HG Communication Manager*** created in **Section 6.3** was used.



The following screen shows the addition of the SIP entity for the Avaya SBCE.

The name ***HG ASBCE***, the inside IP address of the Avaya SBCE and the location ***HG ASBCE*** created in **Section 6.3** was used.



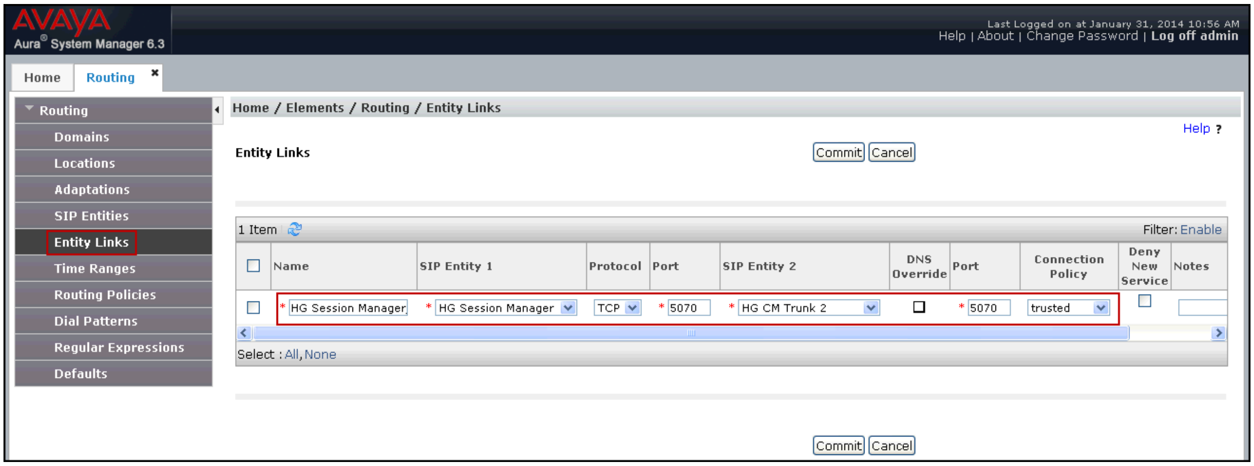
6.5. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two entity links were created; one to Communication Manager and one to the Avaya SBCE, to be used only for service provider traffic. 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:

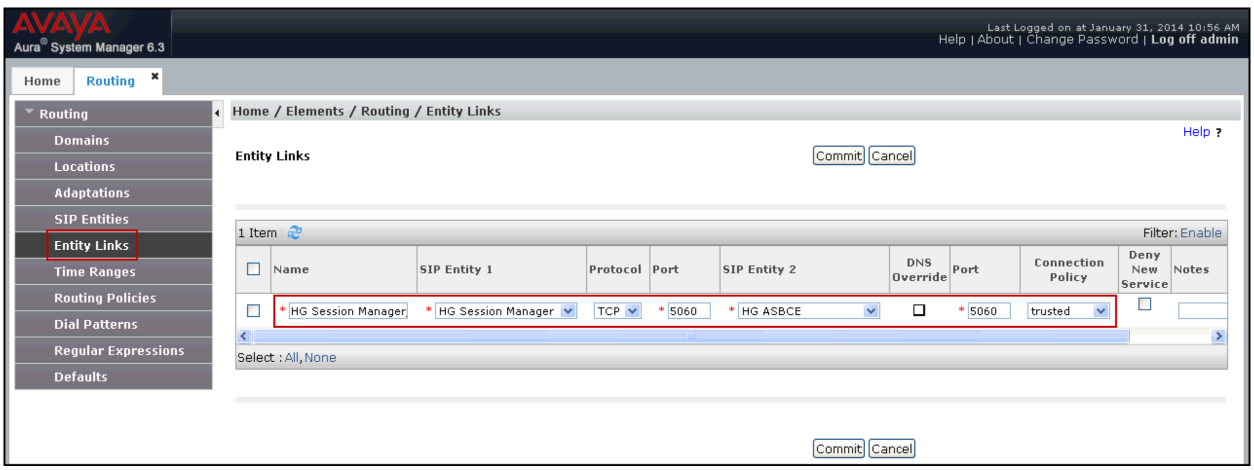
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end 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 will receive 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 Communication Manager and to the Avaya SBCE. It should be noted that in a customer environment the entity link to Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic is not encrypted.

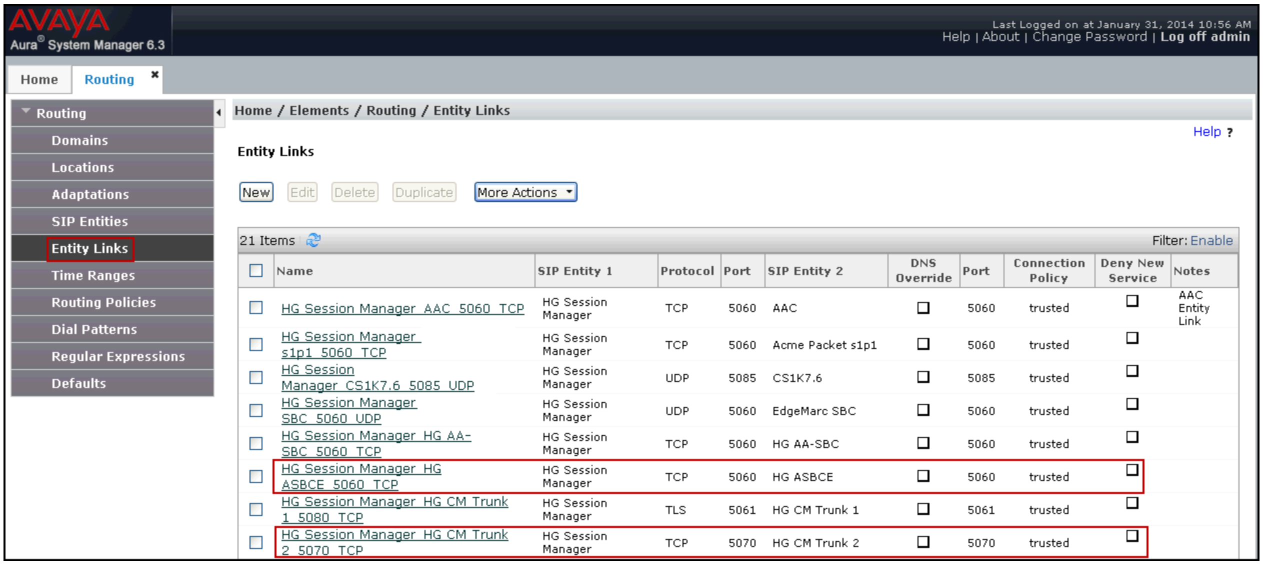
The following screen shows the entity link to Communication Manager:



The following screen shows the entity link to the Avaya SBCE:



The following screen shows the list of the newly added entity links. Note that only the highlighted entity 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 6.4**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. 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:

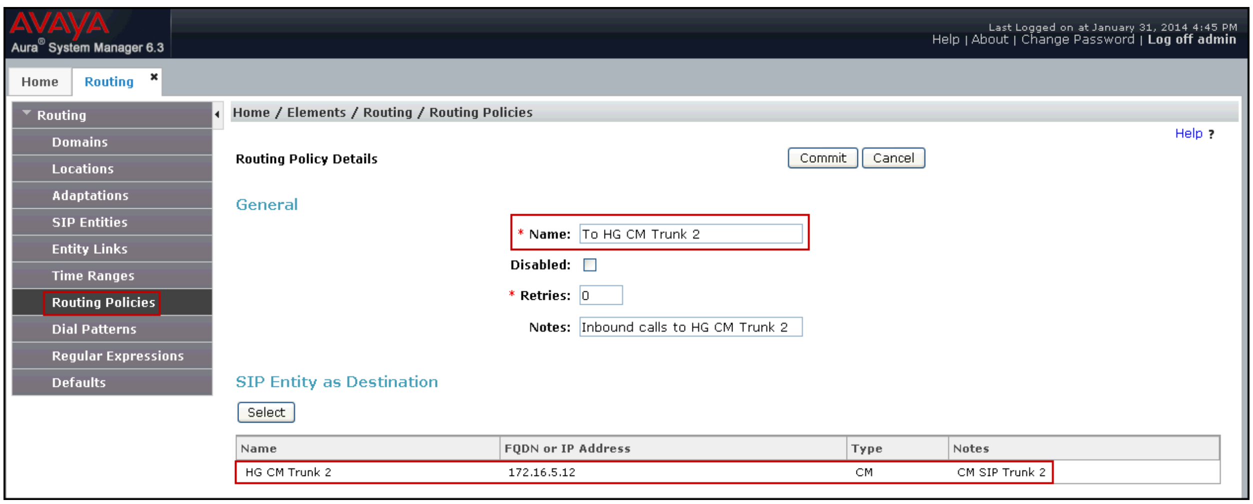
In the **General** section, enter the following values. Use default values for all remaining fields:

- **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 screen shows the routing policy for Communication Manager:



The following screen shows the routing policy for the Avaya SBCE:

6.7. Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to SaskTel 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).

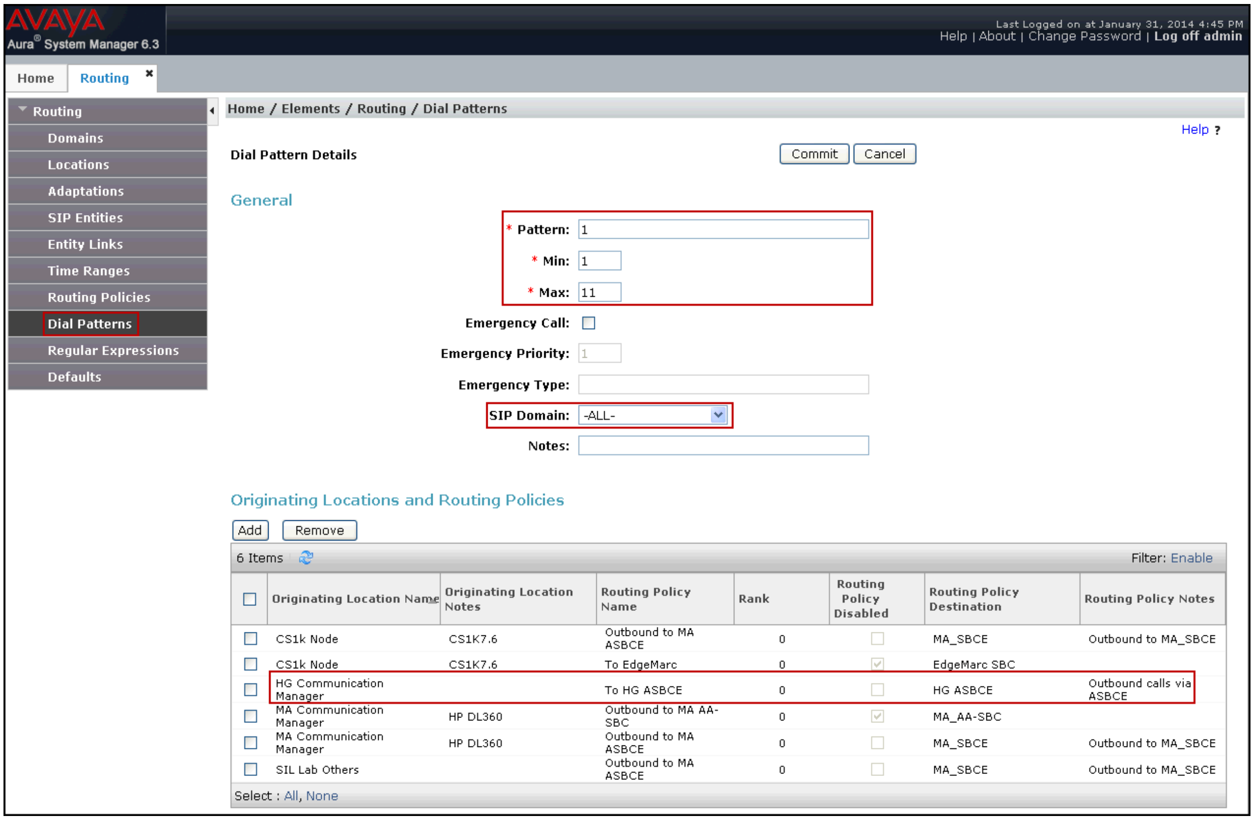
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

- Click **Commit** to save.

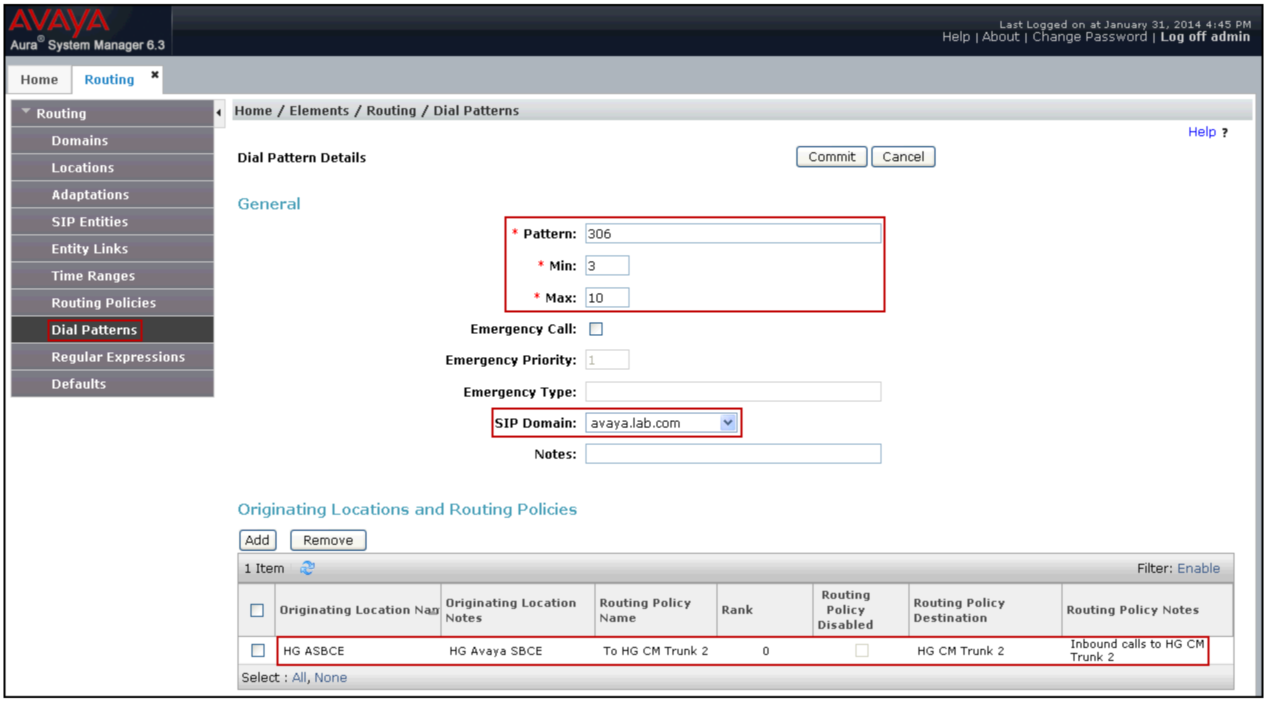
Examples of dial patterns used for the compliance testing are shown below.

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

Note: The SIP Domain was set to –ALL- since dial pattern 1 is shared among multiple SIP Domains in the Avaya lab.



The following dial pattern used for the compliance testing was for inbound calls to the enterprise. It uses dial pattern ***306*** matching the NPA of the DID numbers assigned to the enterprise by SaskTel. This dial pattern was configured with the destination SIP Domain of ***avaya.lab.com***, Originating Location Name ***HG ASBCE,*** and Routing Policy name ***To HG CM Trunk 2.***



6.8. Add/View Avaya Aura® Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add 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 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.

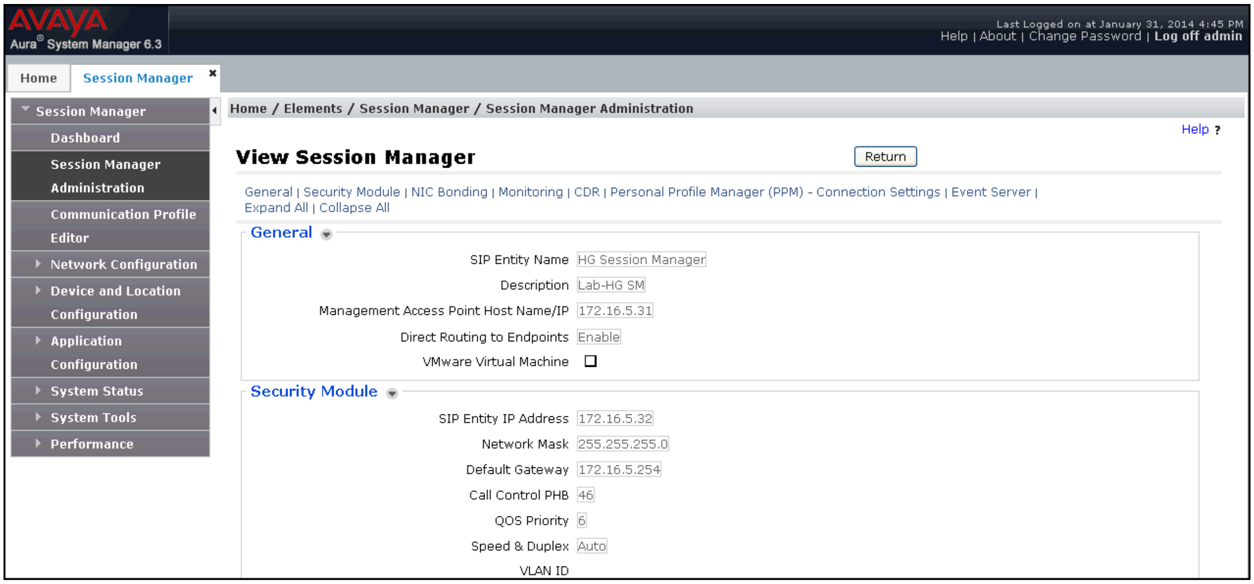
In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of the Session Manager signaling interface.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields.

- Click **Save** (not shown).

The screen below shows the 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 SaskTel's SIP Trunk service.

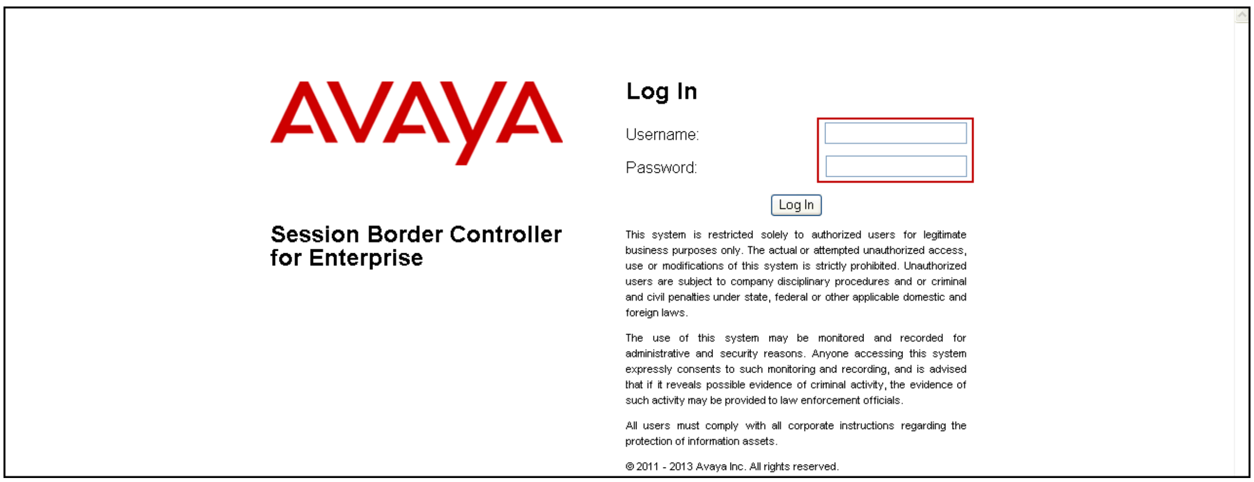
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: During the next pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it.

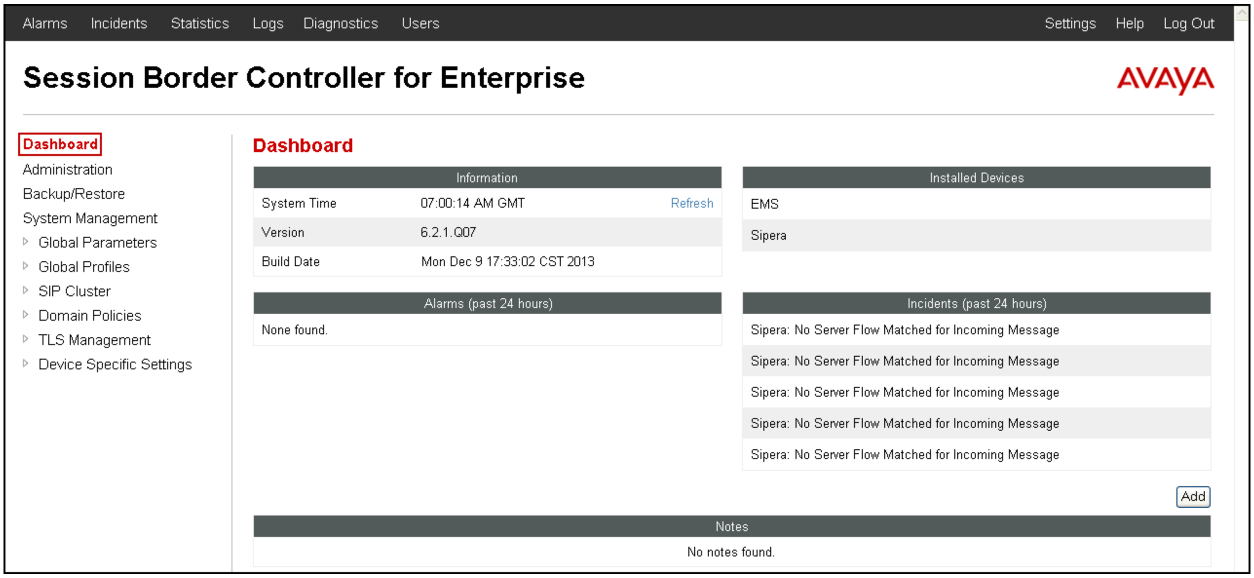
7.1. Log in Avaya SBCE

Use a web browser to access the Avaya SBCE web interface, enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the management IP address of the Avaya SBCE.

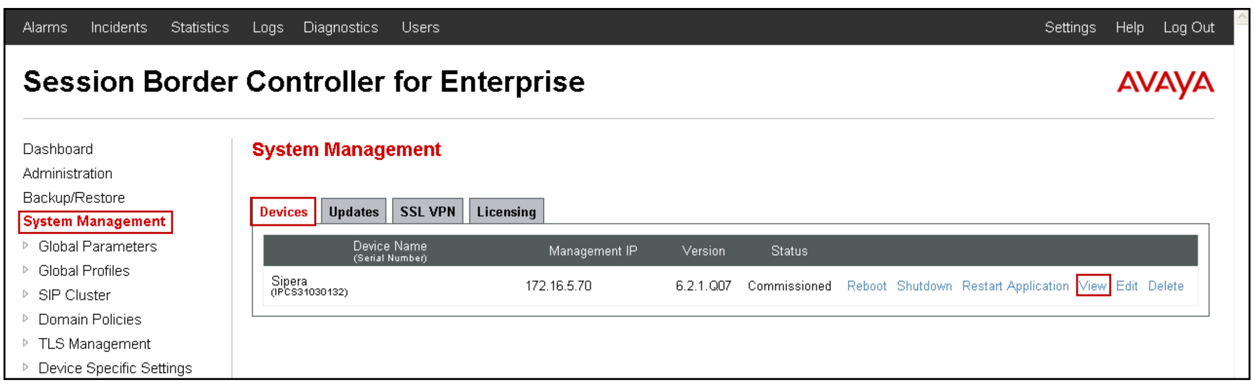
Enter the appropriate credentials and then click **Log In**.



The **Dashboard** main page will appear as shown below.

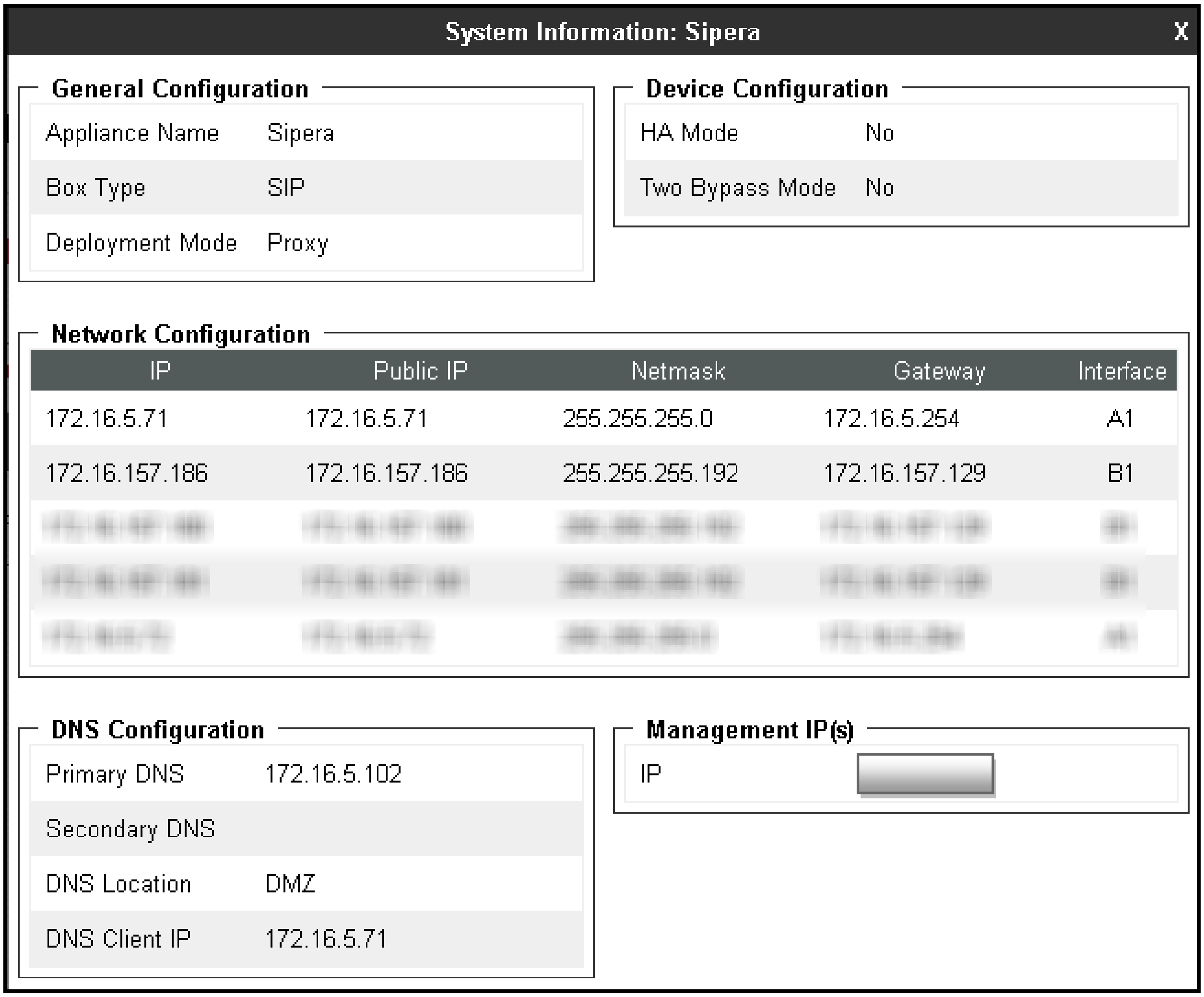


To view the system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Sipera** was already added. To view the configuration of this device, click the **View** as shown in the screenshot below.



To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to ***SIP*** and the **Deployment Mode** was set to ***Proxy***. Default values were used for all other fields.



On the previous screen, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces of the Avaya SBCE, respectively. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to SaskTel. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document. These IP addresses have been blurred out, and the management IP has also been blurred out for security reasons.

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.**

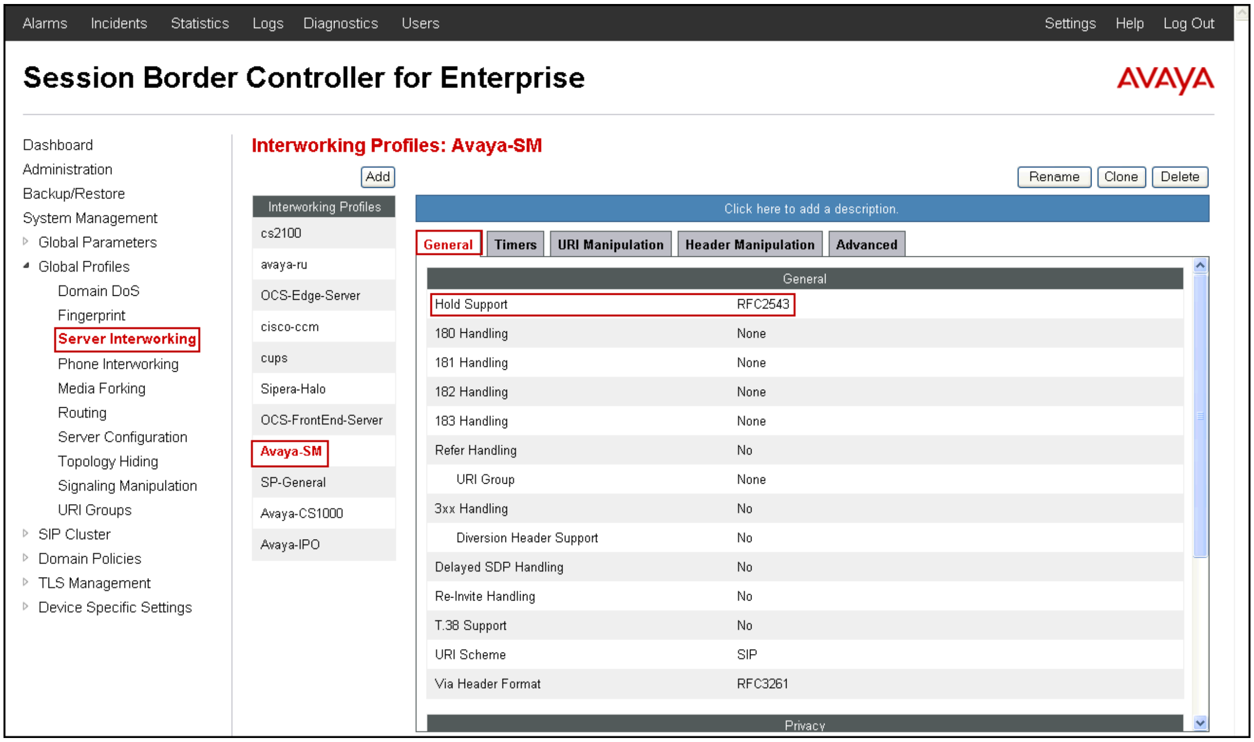
For the newly created **Avaya-SM** profile, click **Edit** (not shown) at the bottom of the **General** tab:

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

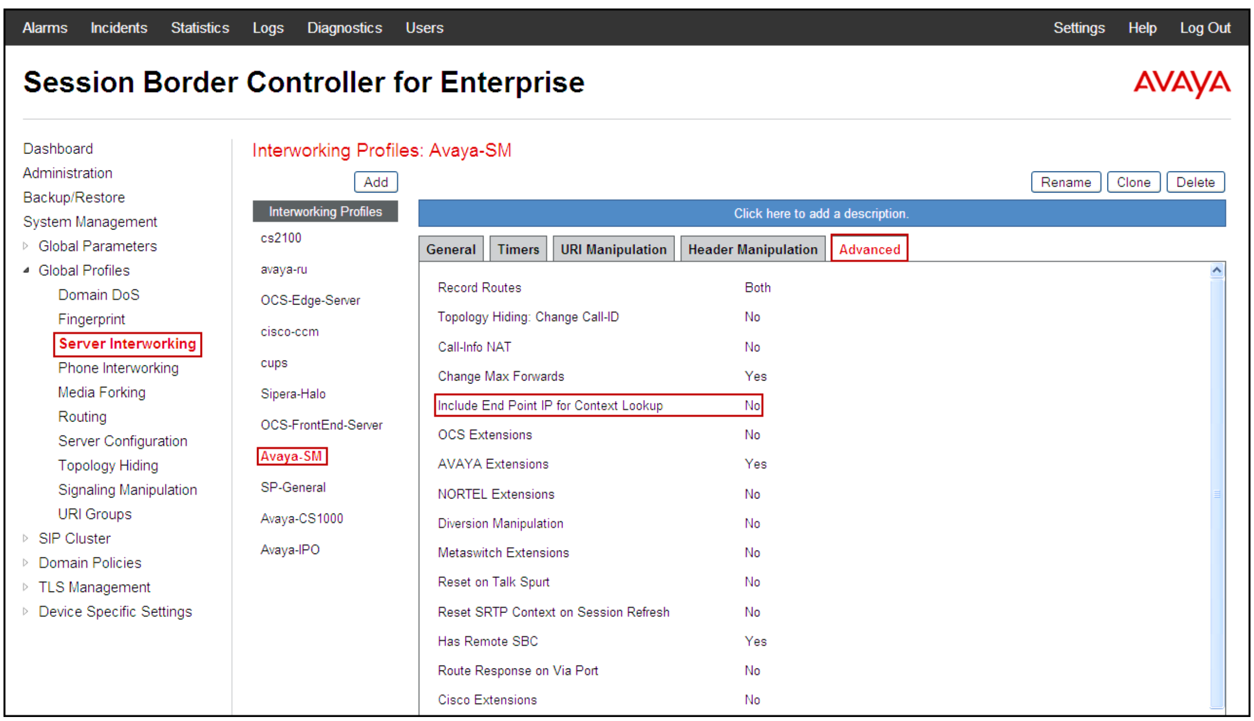
For the newly created **Avaya-SM** profile, click **Edit** (not shown) at the bottom of the **Advanced** tab:

- Uncheck **Include End Point IP for Context Lookup**.
- Leave other fields with their default values.
- Click **Finish**.

The following screen capture shows the **General** tab of the newly created **Avaya-SM** Profile.



The following screen capture shows the **Advanced** tab of the newly created **Avaya-SM** Profile.



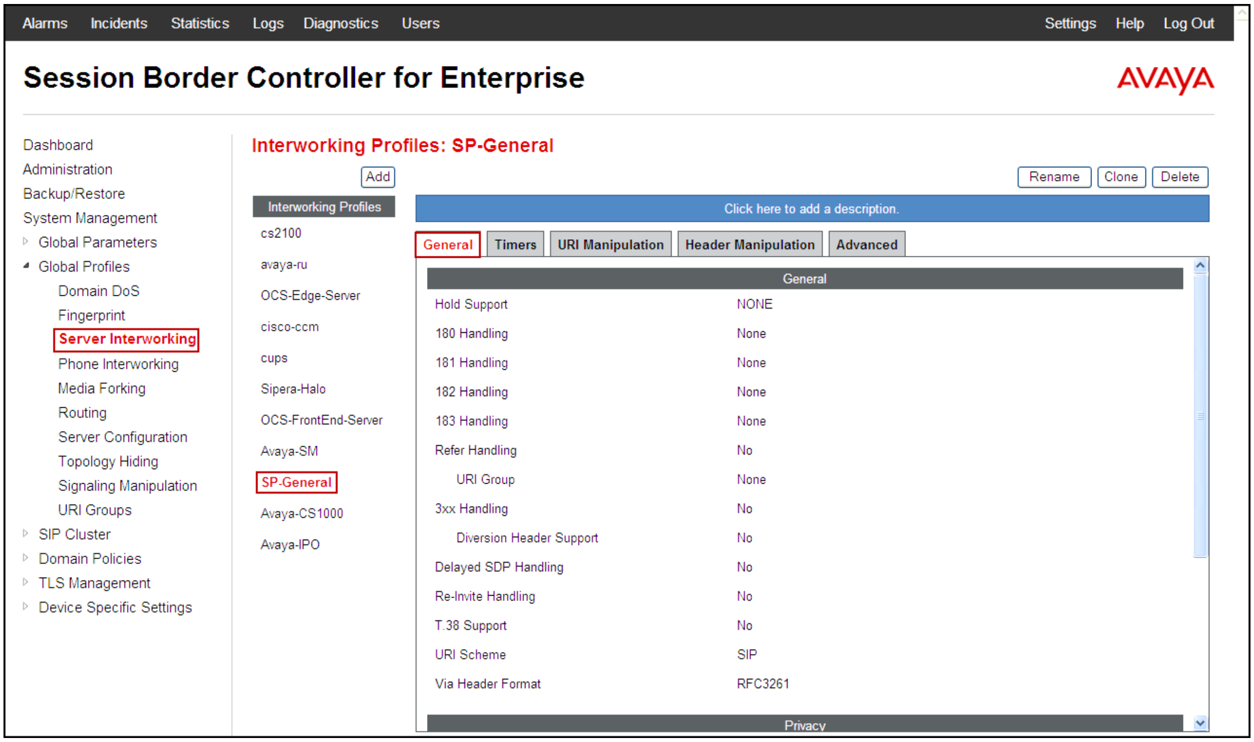
7.2.2. Server Interworking SP-General

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

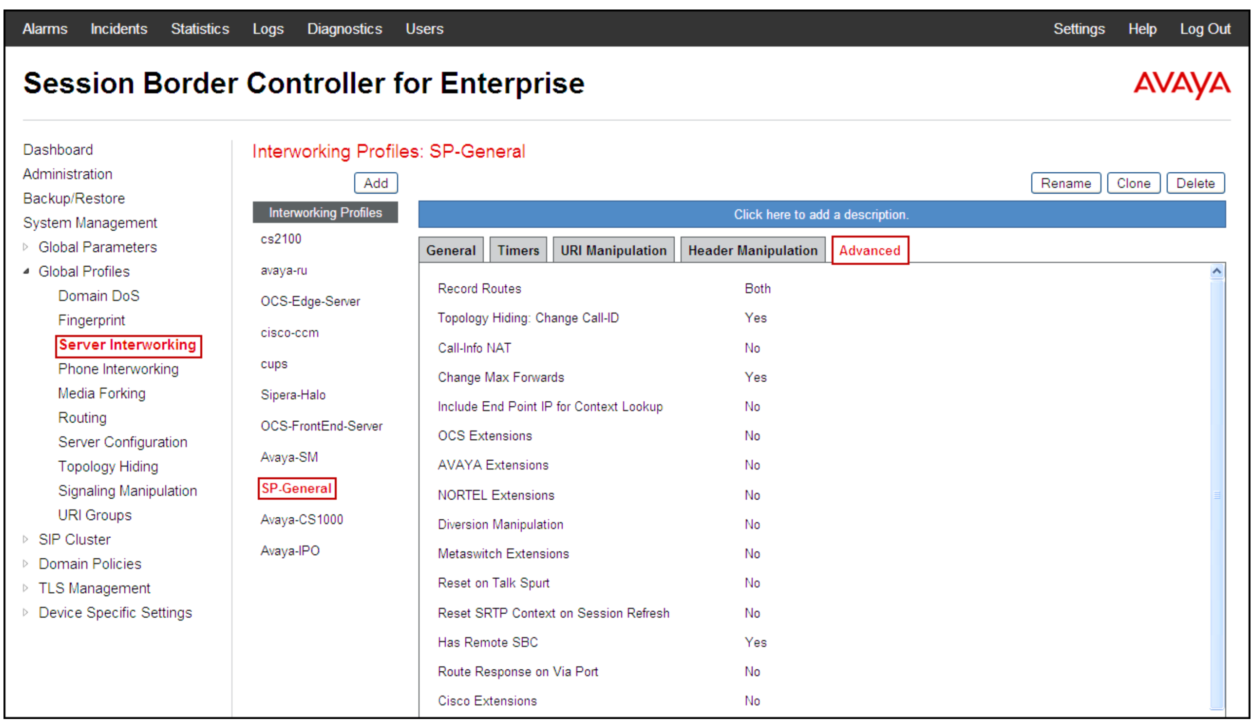
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add.**

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.**

The following screen capture shows the **General** tab of the newly created **SP-General** profile.



The following screen capture shows the **Advanced** tab of the newly created **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.

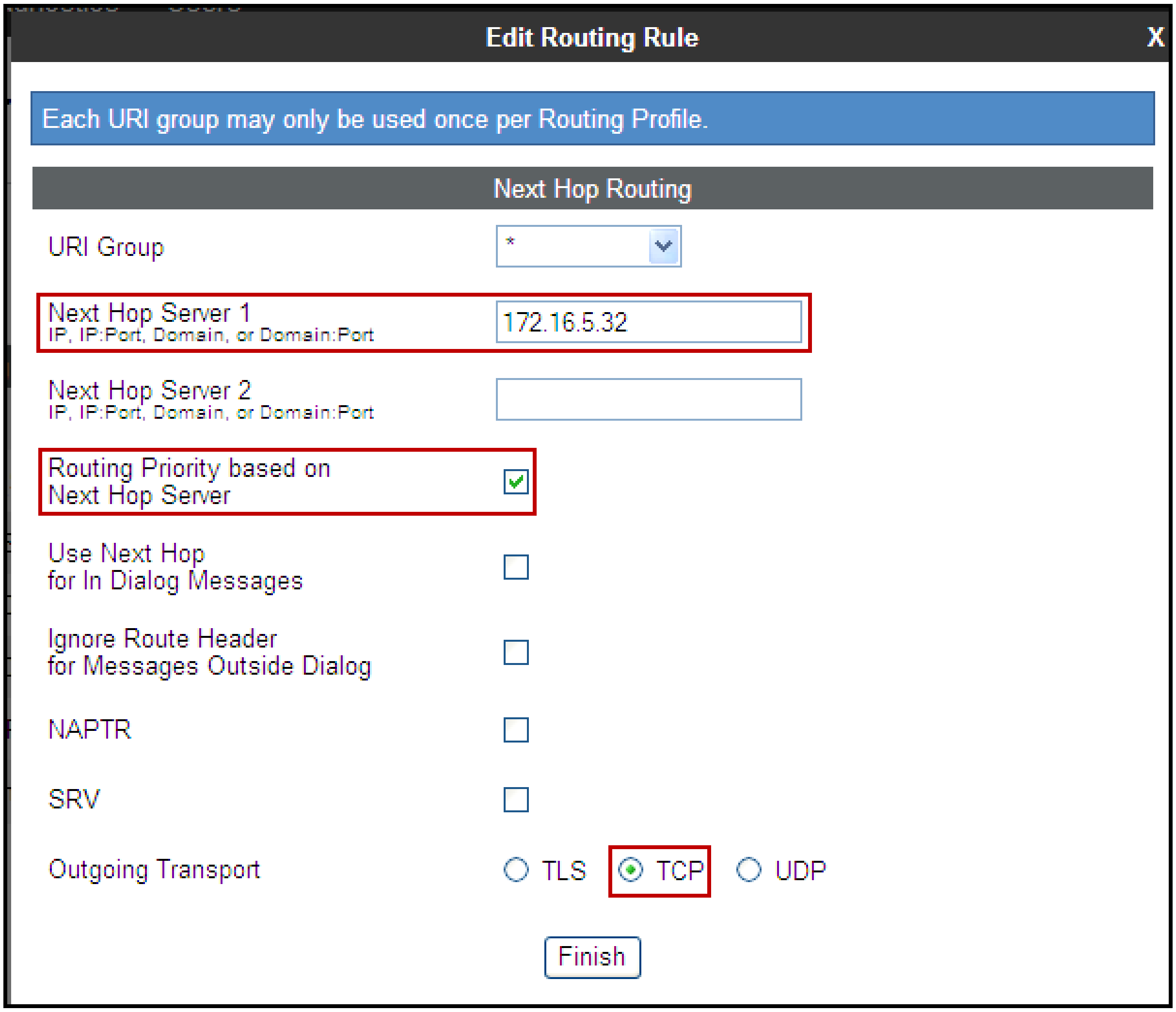
Two Routing profiles were created; one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

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

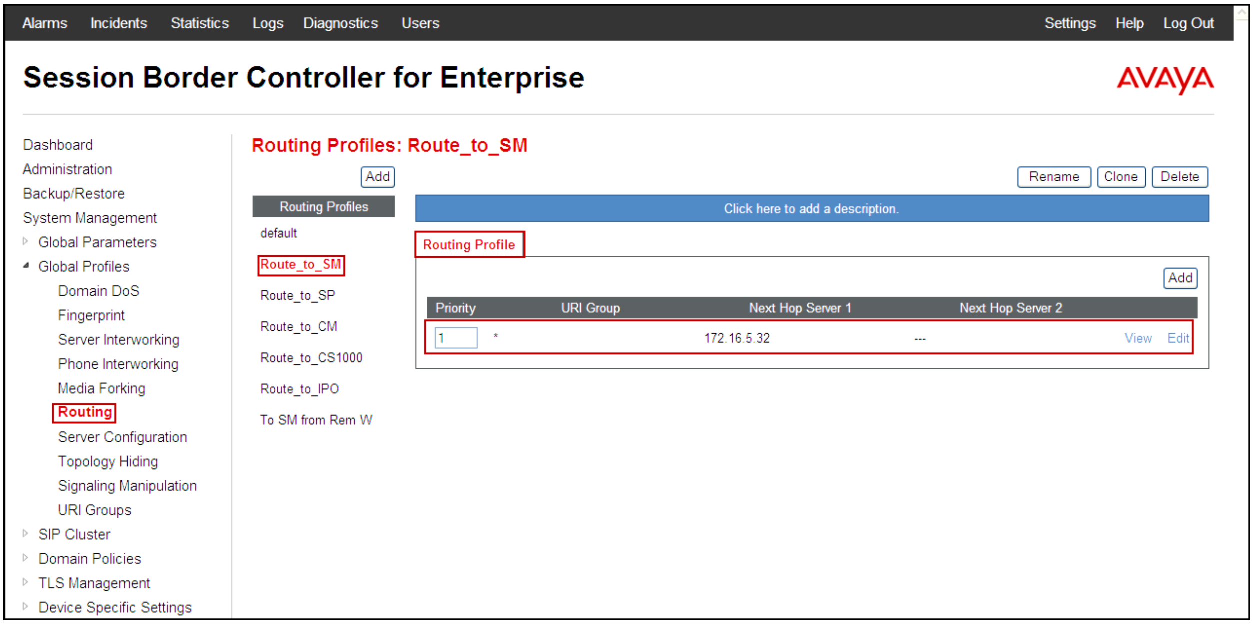
- Select **Routing**.
- Click **Add** in the **Routing Profiles** section**.**
- Enter Profile Name: ***Route_to_SM*.**
- Click **Next.**

On the next screen, complete the following:

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

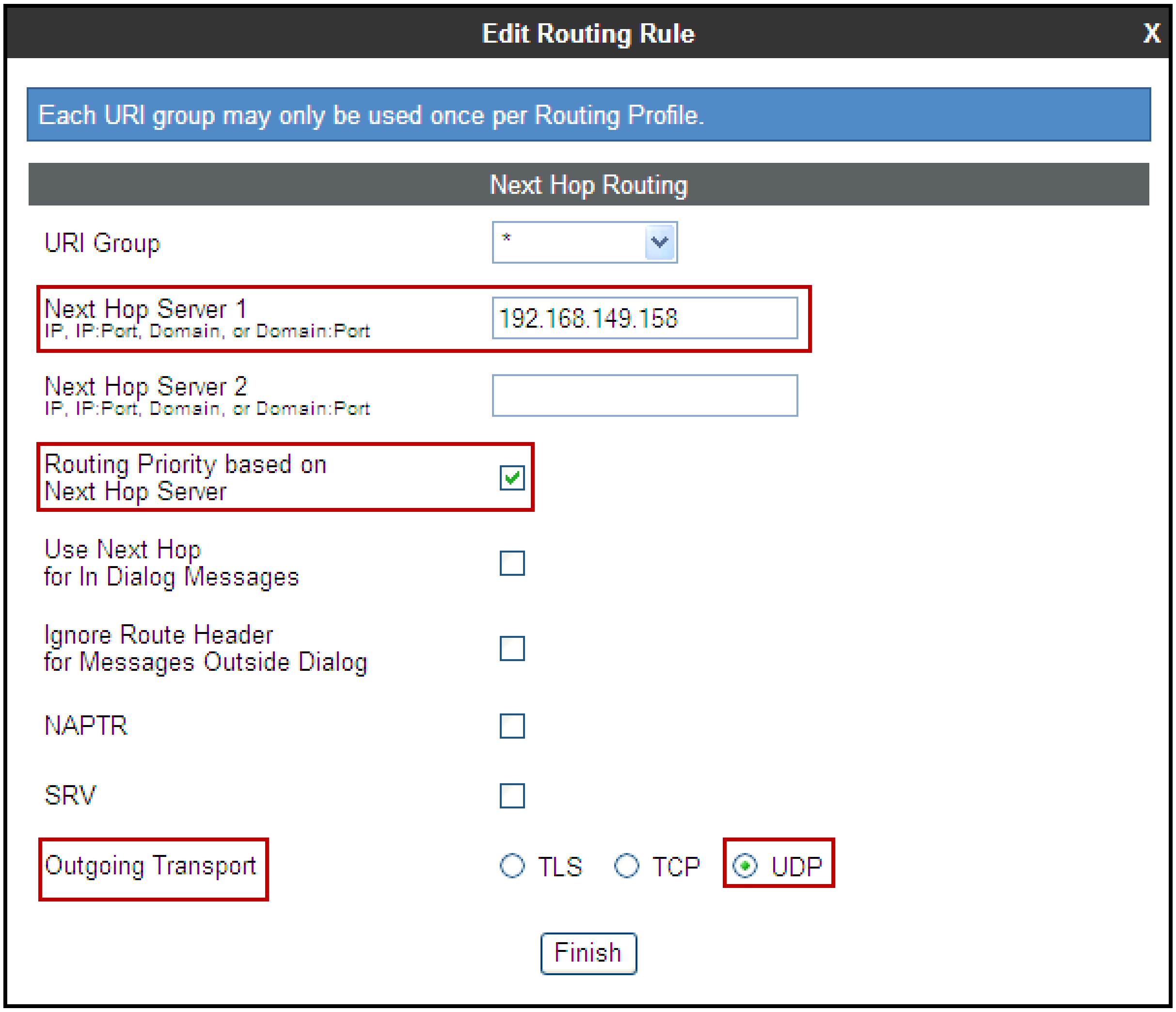

Edit Routing Rule
X
Each URI group may only be used once per Routing Profile.
Next Hop Routing
URI Group
*
Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port
172.16.5.32
Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port
Routing Priority based on Next Hop Server
Use Next Hop for In Dialog Messages
Ignore Route Header for Messages Outside Dialog
NAPTR
SRV
Outgoing Transport
TLS
TCP
UDP
Finish

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



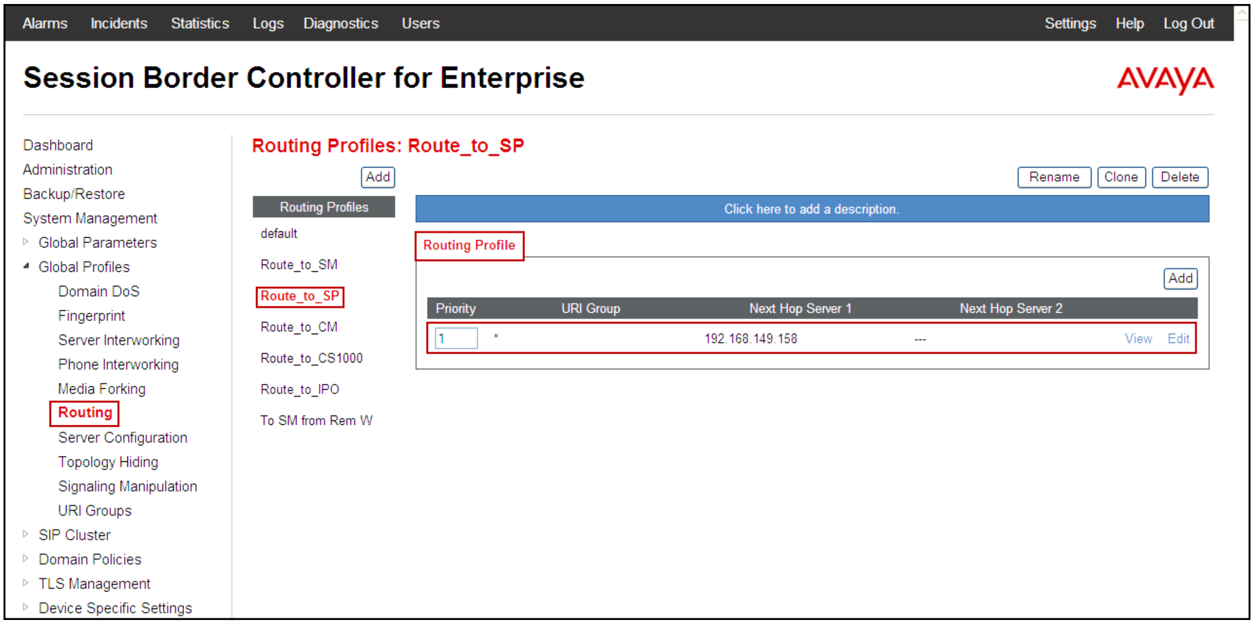
Similarly, for the outbound route:

- Click **Add** in the **Routing Profiles** section**.**
- Enter Profile Name: ***Route_to_SP***
- Click **Next.**
- **Next Hop Server 1:** ***192.168.149.158*** (Service Provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server.**
- **Outgoing Transport:** select ***UDP.***
- Click **Finish.**



Edit Routing Rule
X
Each URI group may only be used once per Routing Profile.
Next Hop Routing
URI Group
*
Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port
192.168.149.158
Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port
Routing Priority based on Next Hop Server
Use Next Hop for In Dialog Messages
Ignore Route Header for Messages Outside Dialog
NAPTR
SRV
Outgoing Transport
TLS
TCP
UDP
Finish

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



7.2.4. Server Configuration

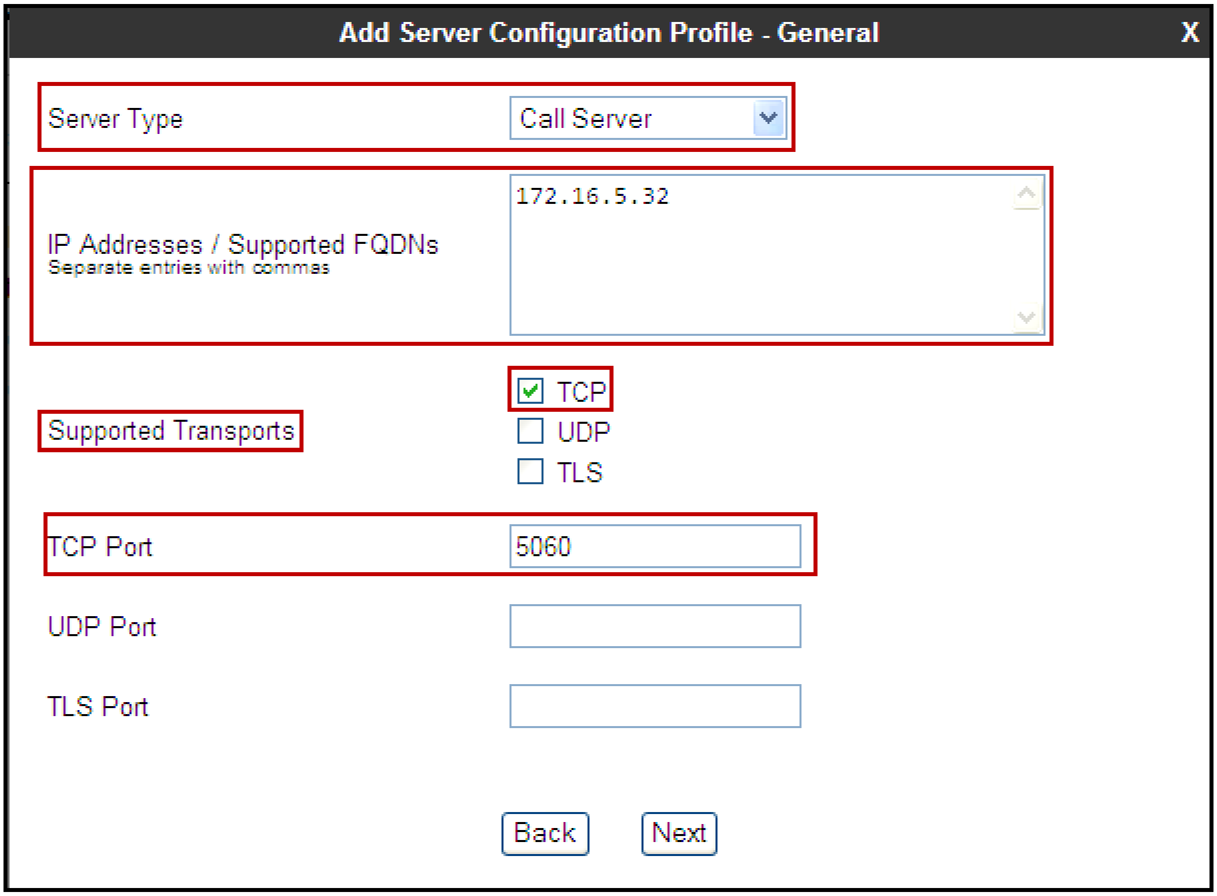
Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server which is the SIP Proxy at the service provider's network.

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 (not shown).
- Click **Next** in the **Heartbeat** window (not shown).

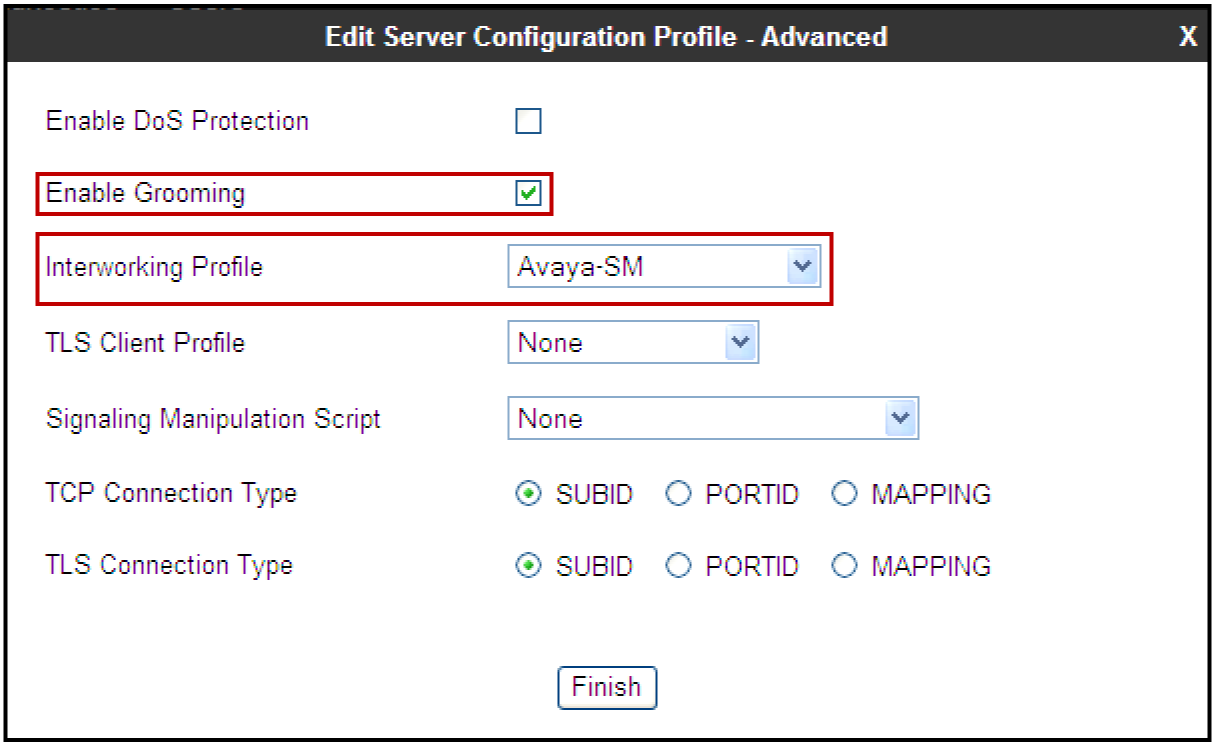
The following screen capture shows the **General** tab of the **Session Manager** profile.



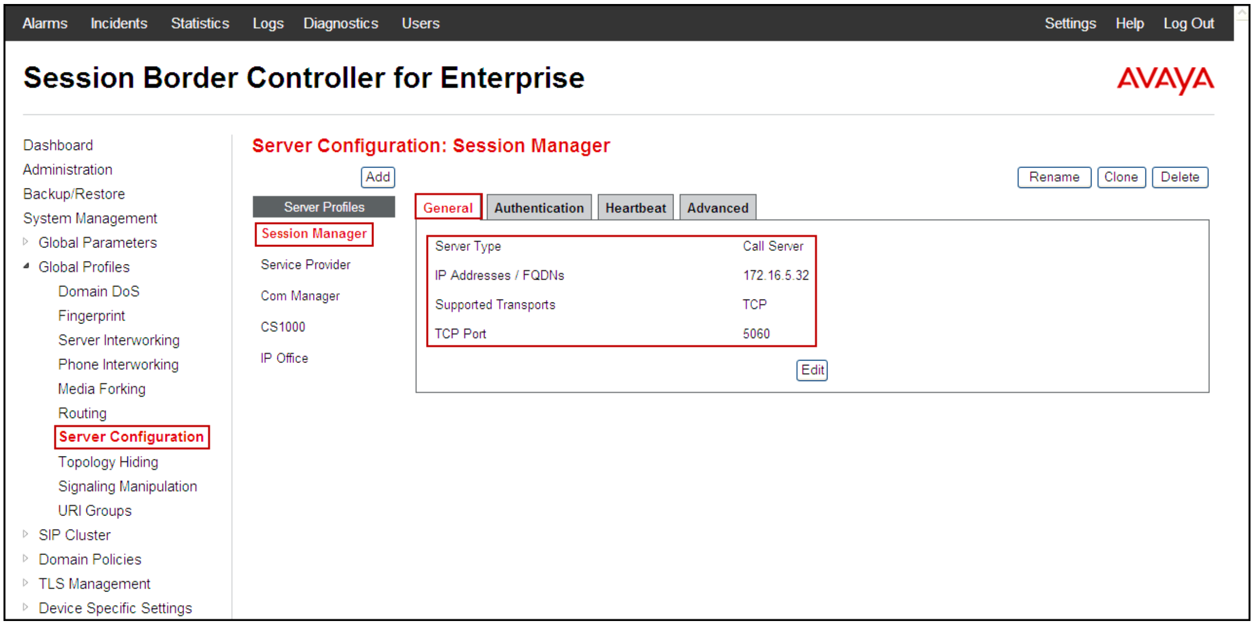
In the **Advanced** window

- Check **Enable Grooming**
- Select ***Avaya-SM*** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default ***None***.
- Click **Finish.**

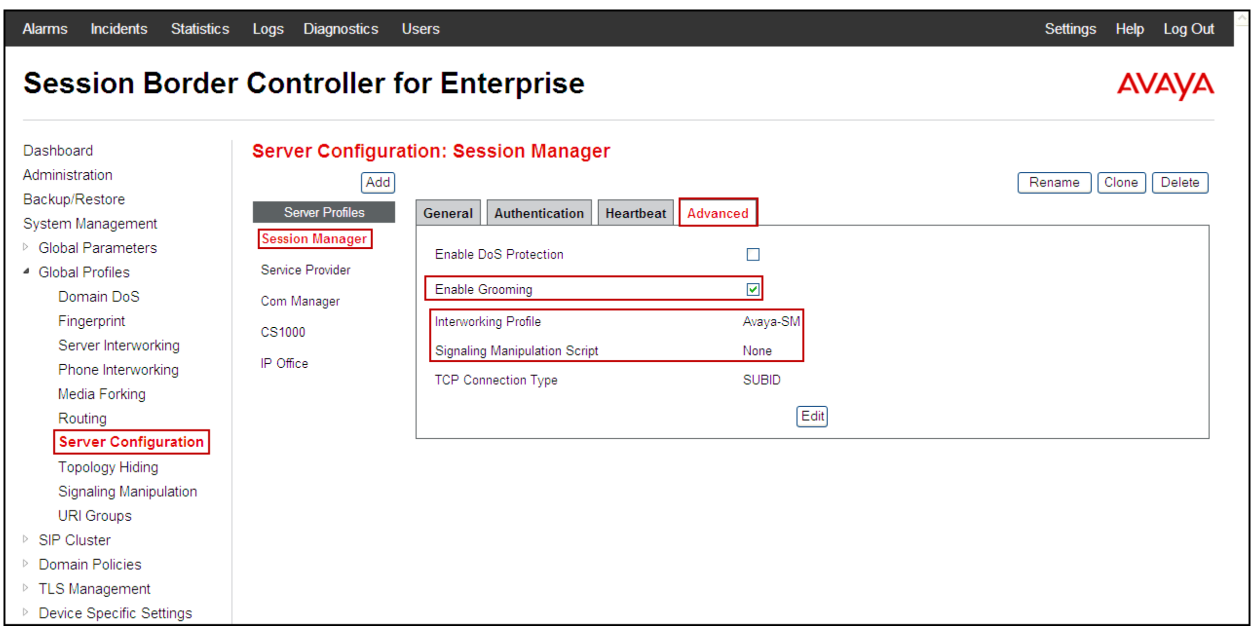
The following screen capture shows the **Advanced** tab of the **Session Manager** profile.



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



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

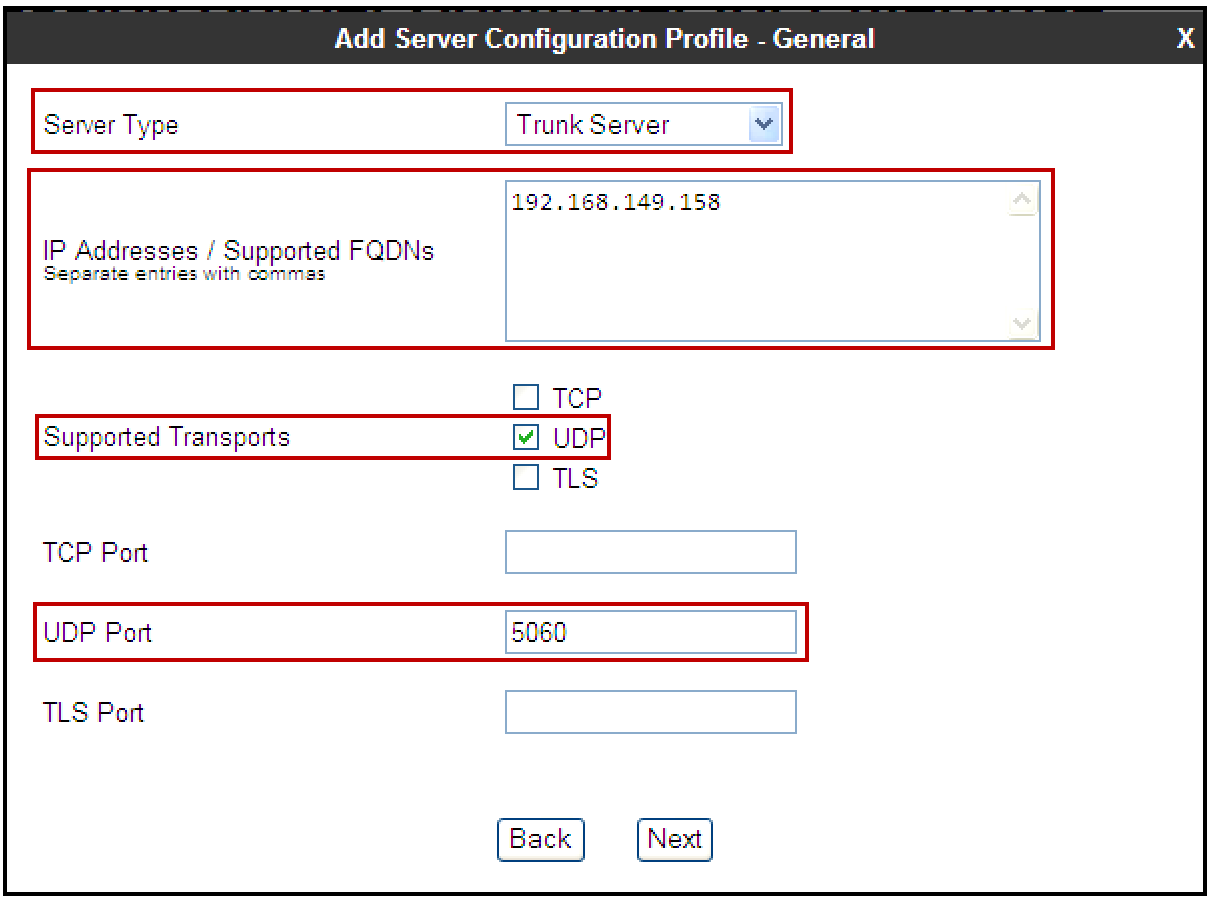


To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** section and enter the profile name: ***Service Provider.***

In the **Add Server Configuration Profile - General** window

- **Server Type:** select ***Trunk Server.***
- **IP Address:** ***192.168.149.158*** (service provider's SIP Proxy IP address).
- **Supported Transports**: check ***UDP***.
- **UDP Port:** enter ***5060***.
- Click **Next**.
- Click **Next** in the **Authentication** window (not shown).
- Click **Next** in the **Heartbeat** window (not shown).

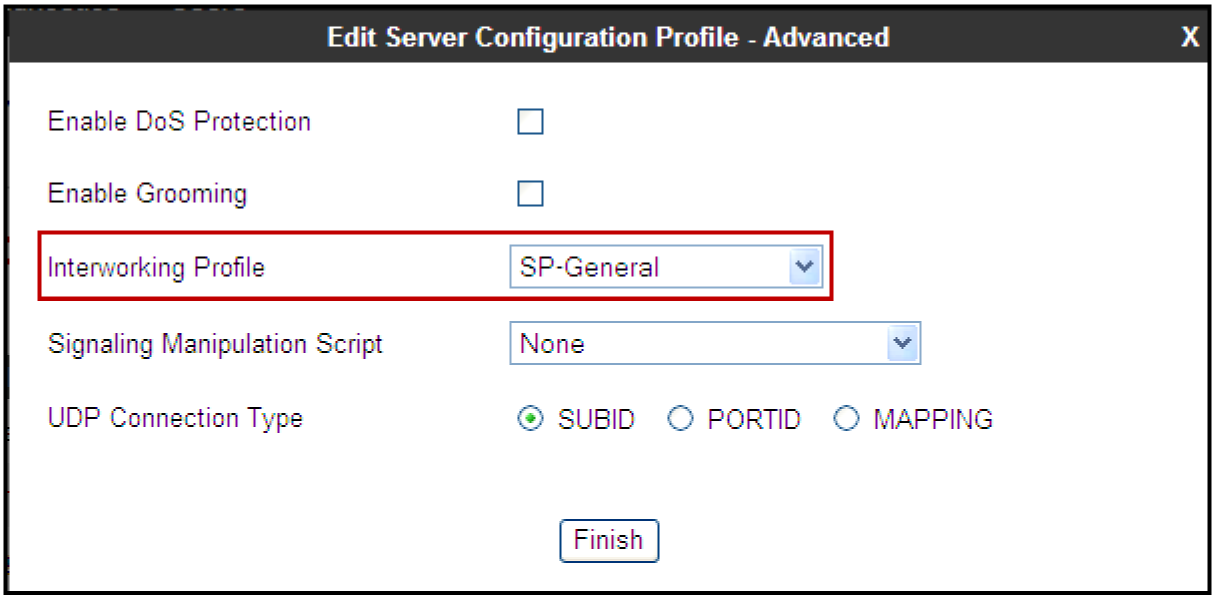
The following screen capture shows the **General** tab of the **Service Provider** profile.



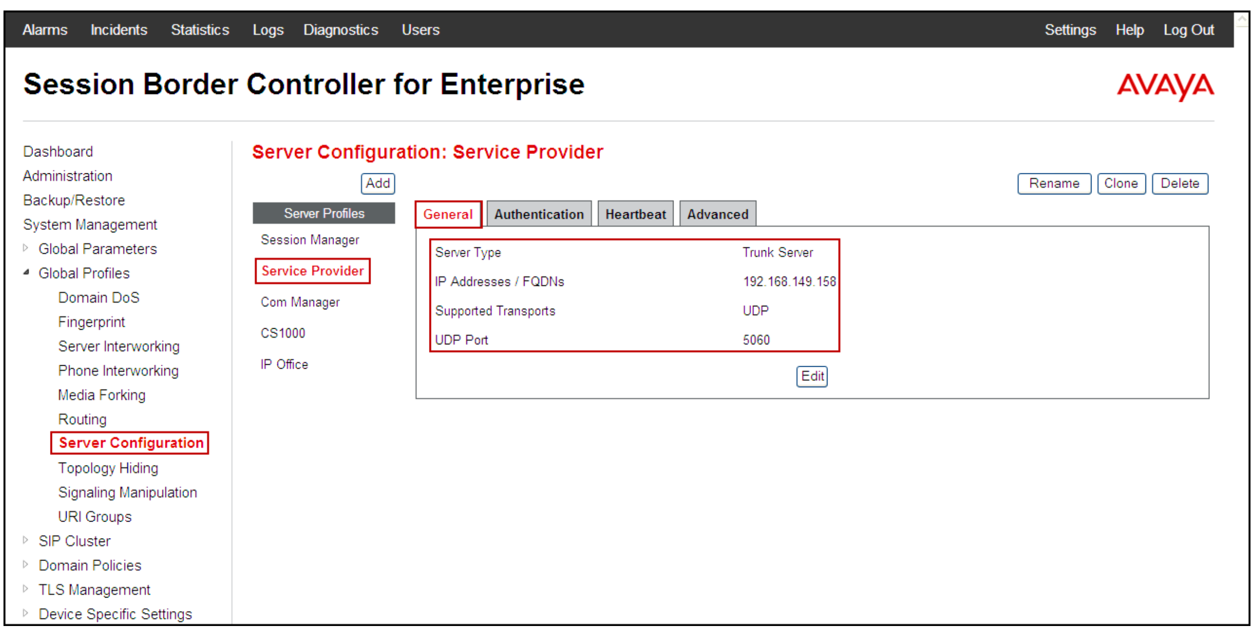
In the **Advanced** window:

- 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.**

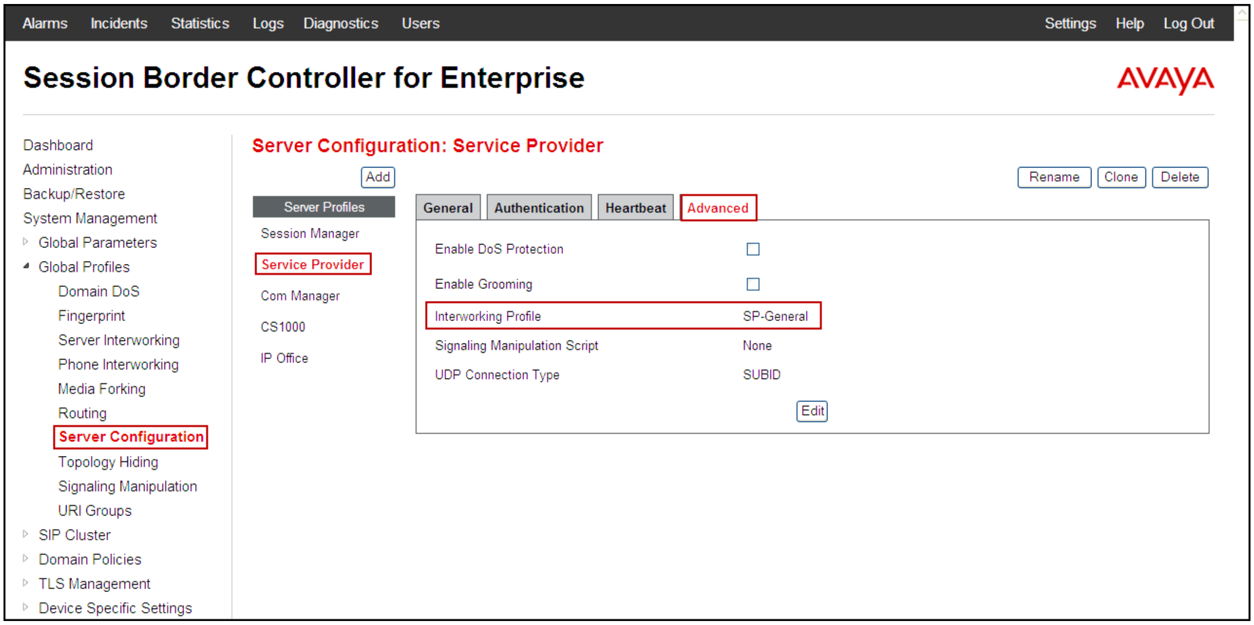
The following screen capture shows the **Advanced** tab of the **Service Provider** profile



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



The following screen capture shows the **Advanced** tab of the newly created **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.

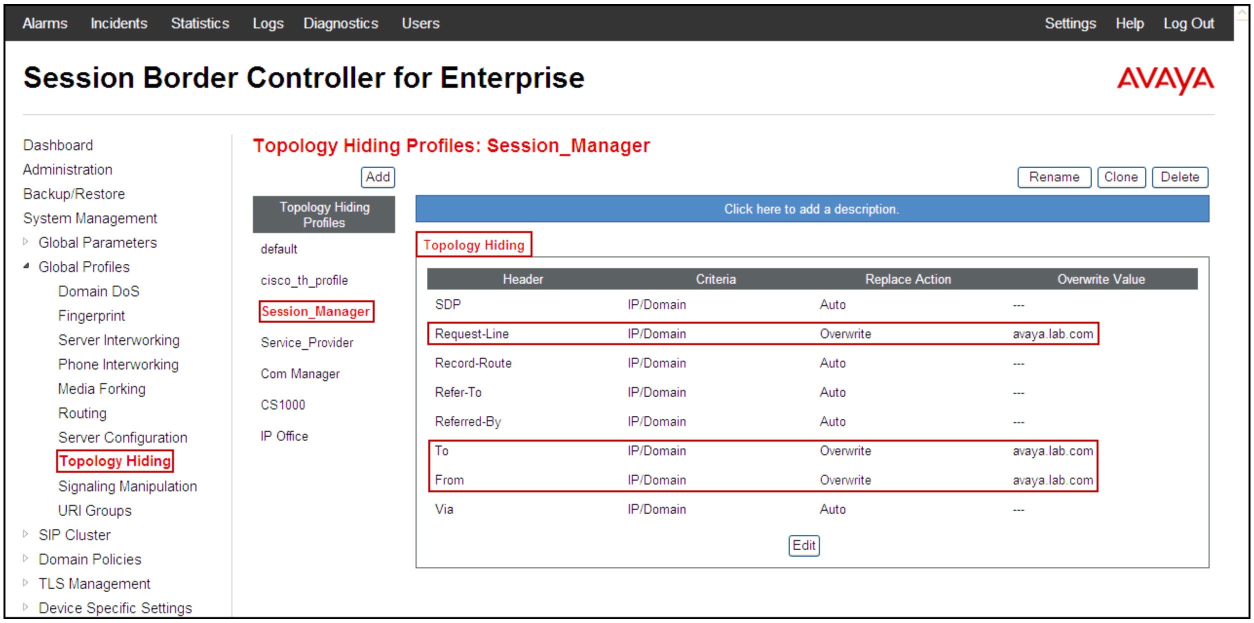
For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

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**.

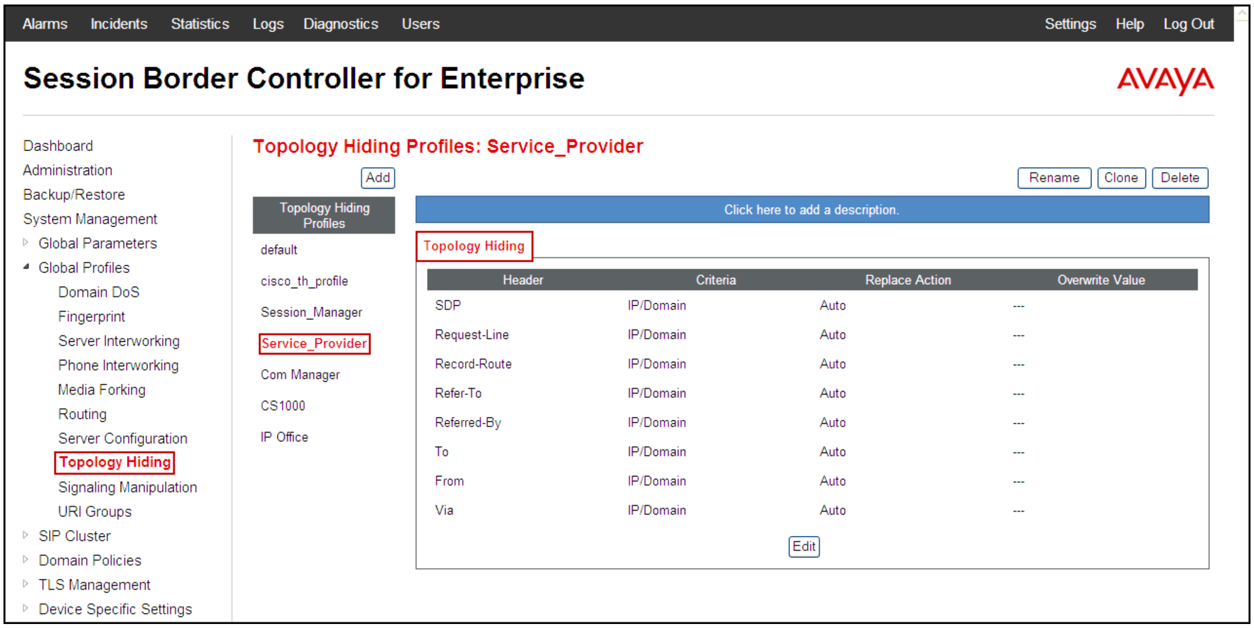
The following screen capture shows the newly created **Session_Manager** profile.



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**.

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



7.2.6. Signaling Manipulation

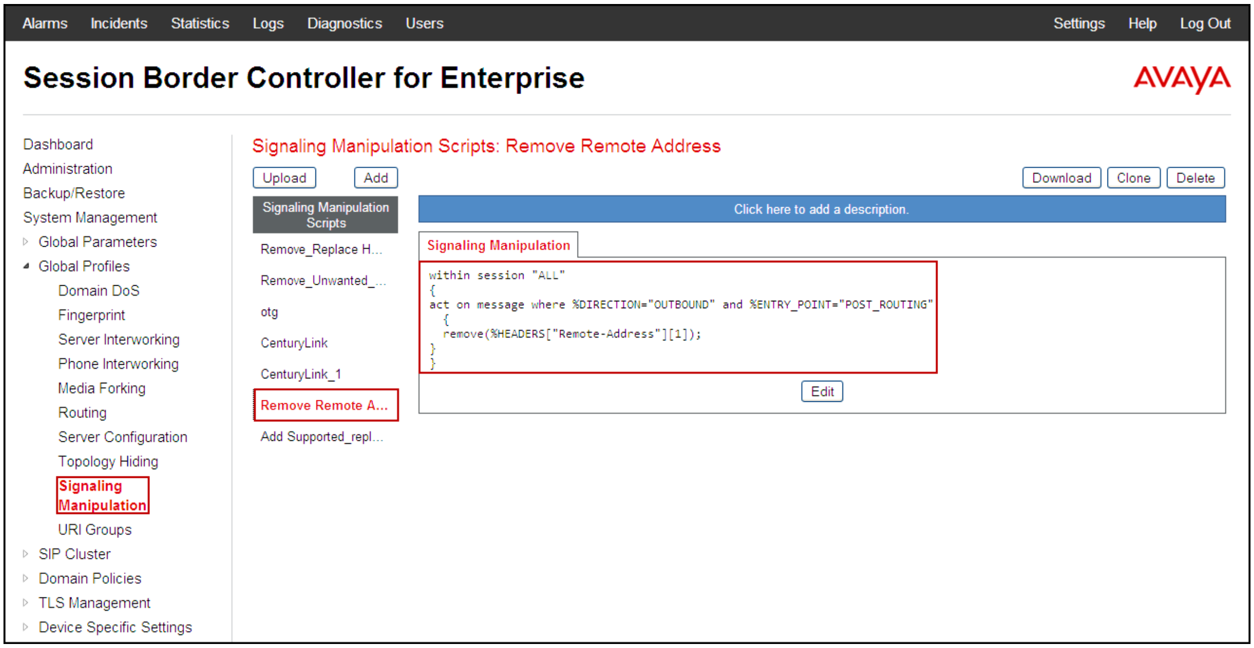
The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described below.

The Signaling Manipulation Script shown below is needed to remove unwanted headers to prevent them from being sent to the Service provider, in this case the **Remote Address** header. This is in addition to the Signaling Rules created to remove headers under **Section 7.3.3**.

From the **Global Profiles** menu on the left panel (not shown), select **Signaling Manipulation** (not shown). Click on **Add Script** (not shown) to open the SigMa Editor screen (not shown).

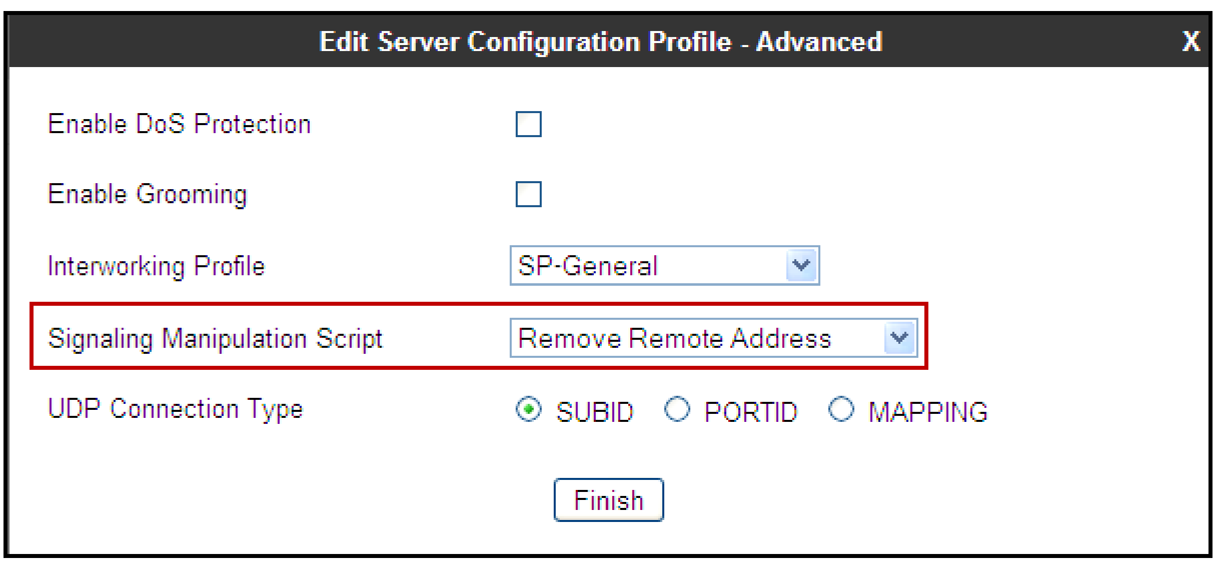
- For **Title** enter a name, the name of ***Remove Remote Address*** was chosen in this example.
- Enter the script as shown on the screen below (**Note**: The script can be copied from **Appendix A**).

- Click **Save**.

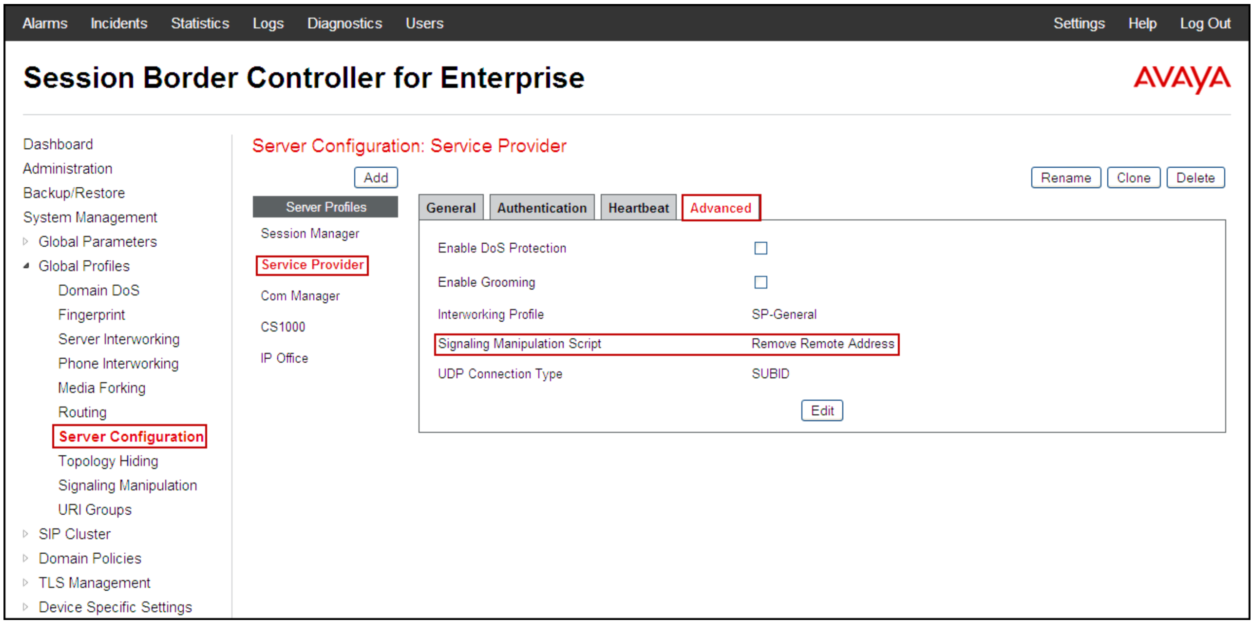


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 7.2.4.**

Go to **Global Profiles → Server Configuration → Service Provider → Advanced** tab **→ Edit**. Select ***Remove Remote Address*** from the drop down menu on the **Signaling Manipulation Script** field. Click **Finish** to save and exit.



The following screen capture shows the **Advanced** tab of the previously added **Service Provider** Profile with the **Signaling Manipulation Script** assigned.



7.3. Domain Policies

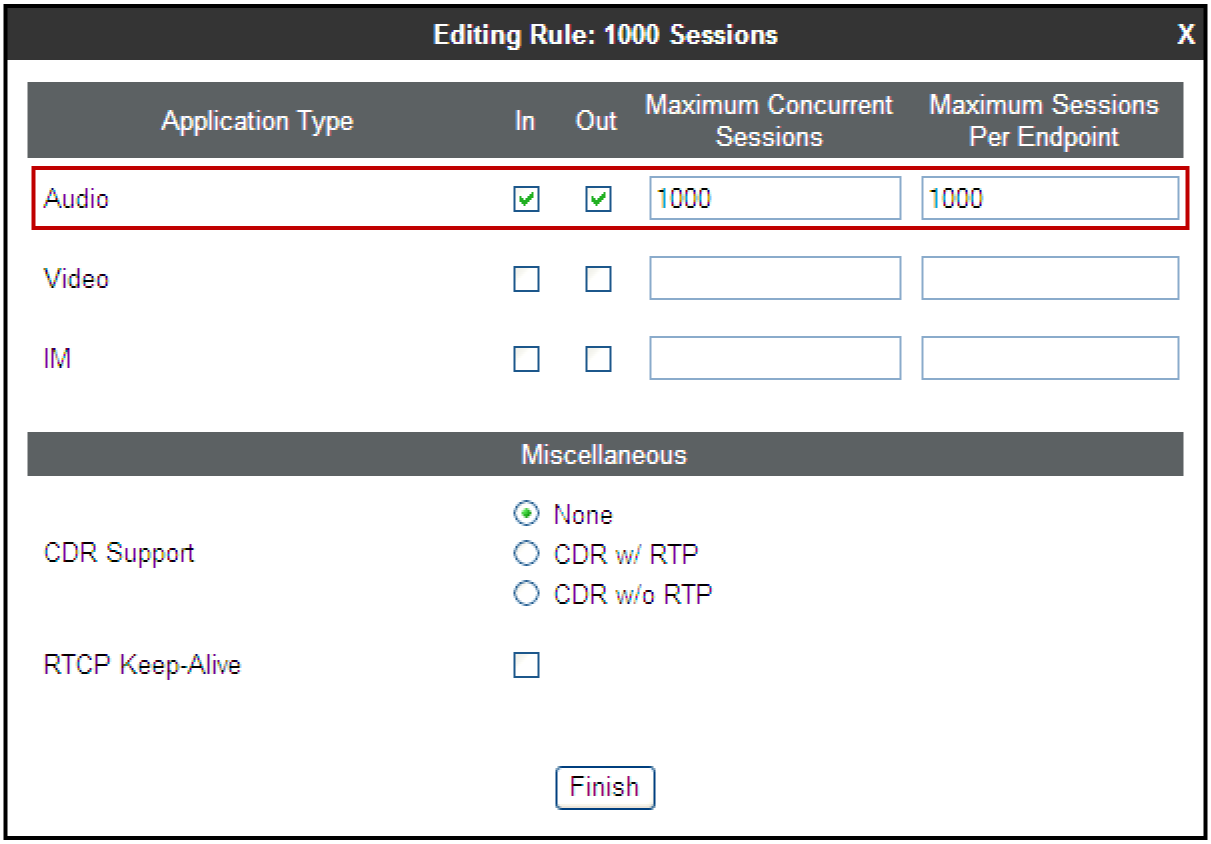
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.3.1. Create Application Rules

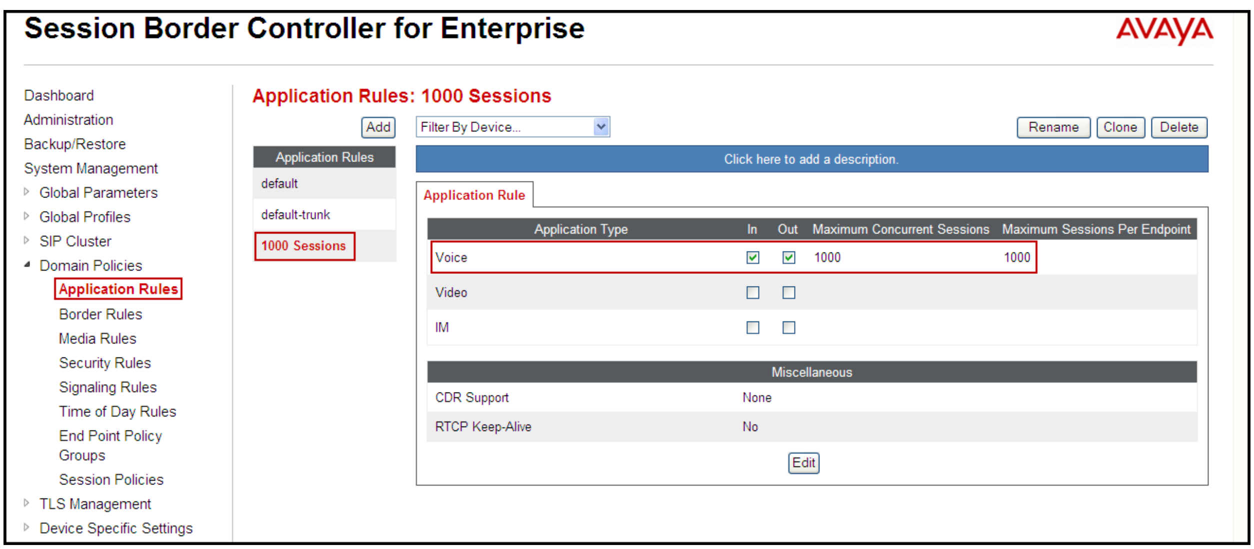
Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in 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*.**
- Click **Finish** (not shown).
- Click **Edit** (not shown).
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values: ***1000*** was used in the sample configuration.
- Click **Finish** (not shown).

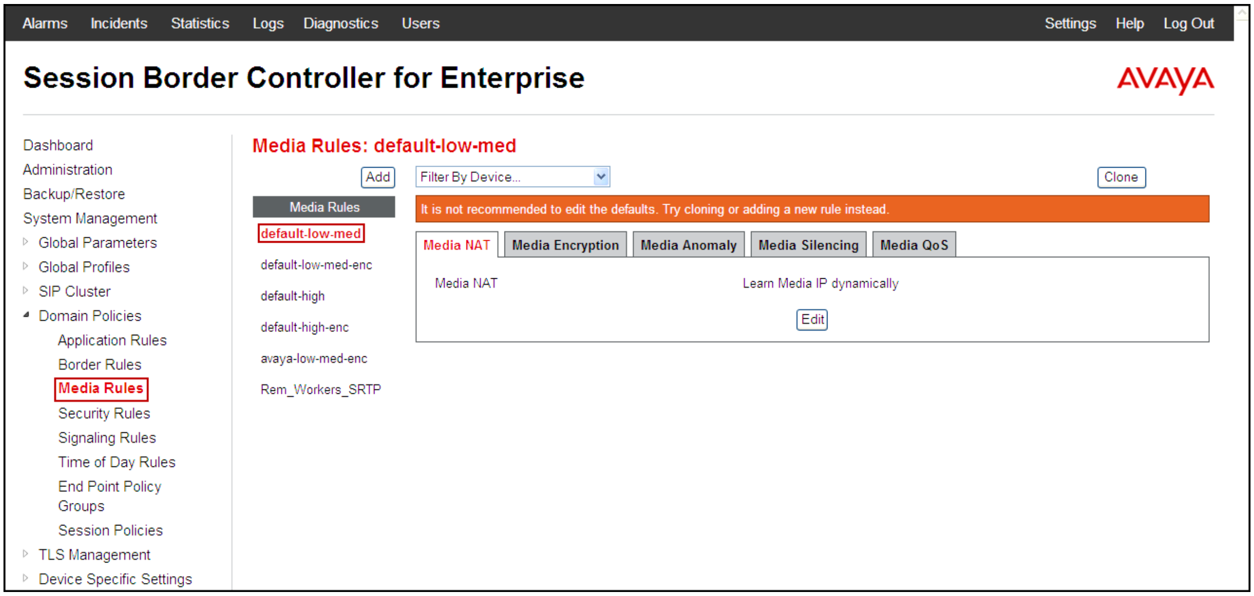


The following screen capture shows the newly created **1000 Sessions** application rule.



7.3.2. Media Rules

For the compliance test, the existing **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 were 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.**

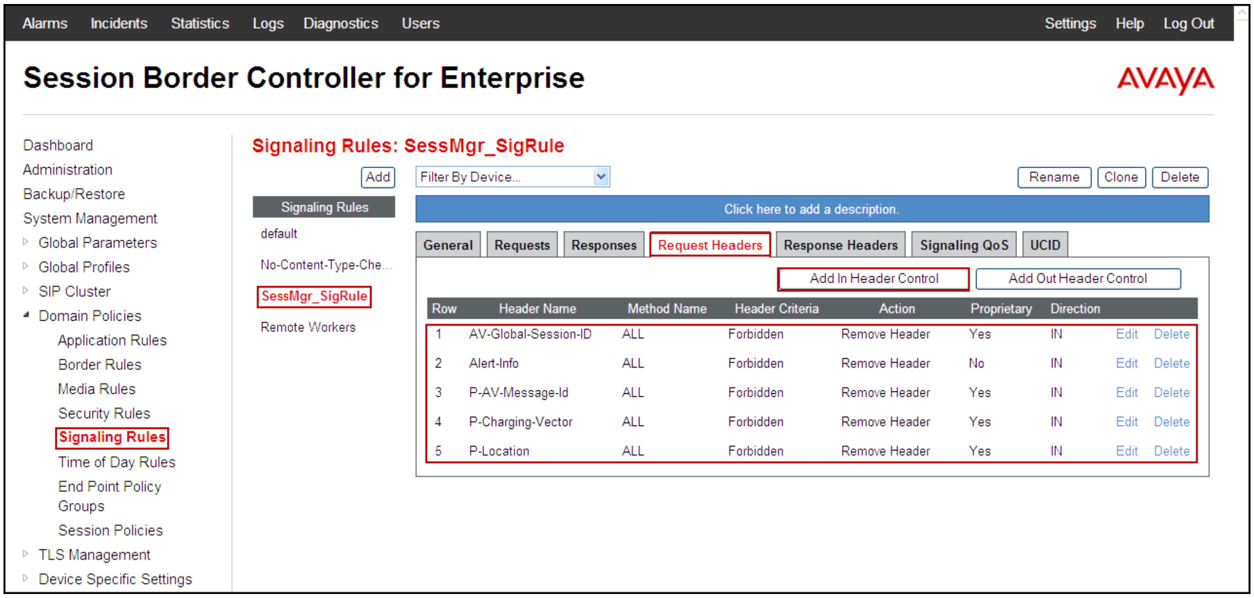
To add the **P-Charging-Vector** header:

- 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:** ***1XX*.**
- **Method Name:** ***ALL*.**
- **Header Criteria:** ***Forbidden*.**
- **Presence Action:** ***Remove Header*.**
- Click **Finish.**

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:** ***1XX*.**
- **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.**

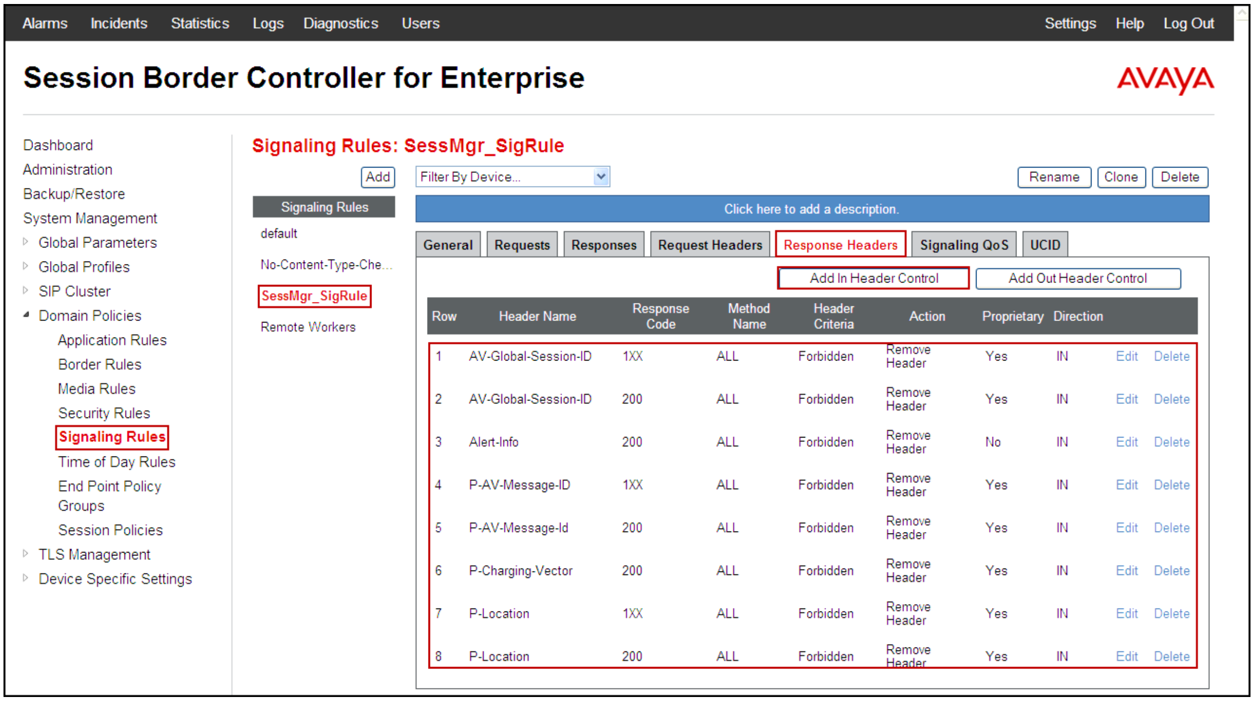
To add the **P-Location** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name:** ***P-Location*****.**
- **Response Code:** ***1XX*****.**
- **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.

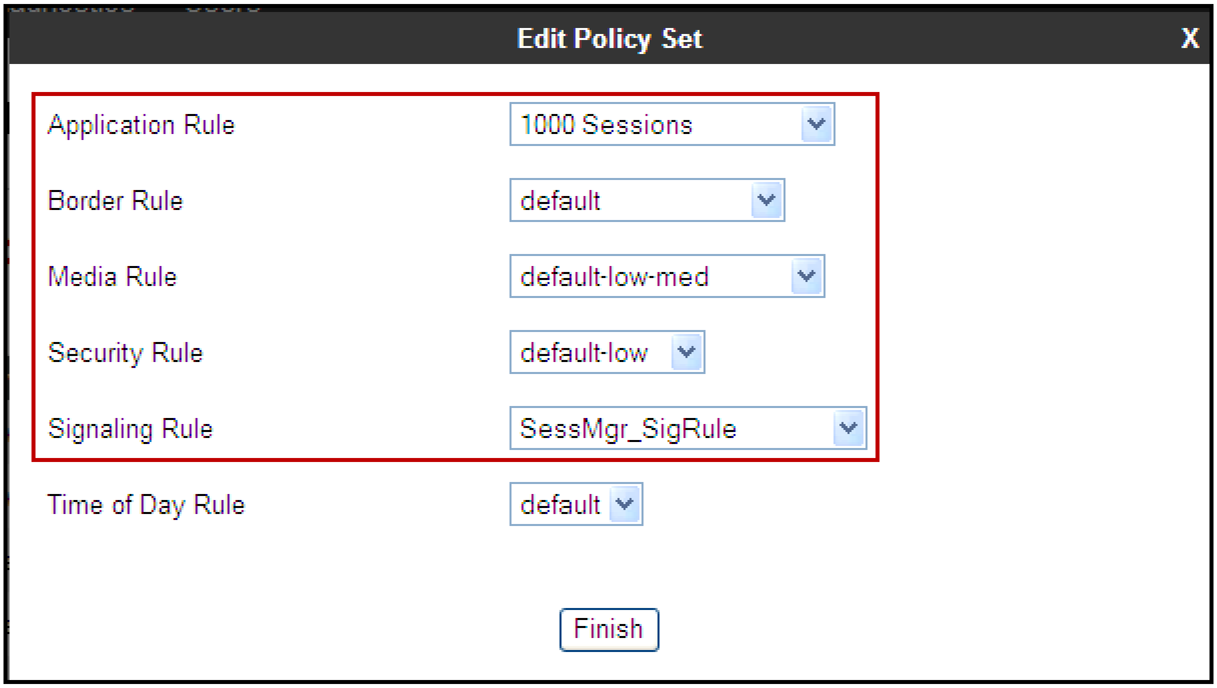


7.3.4. End Point Policy Groups

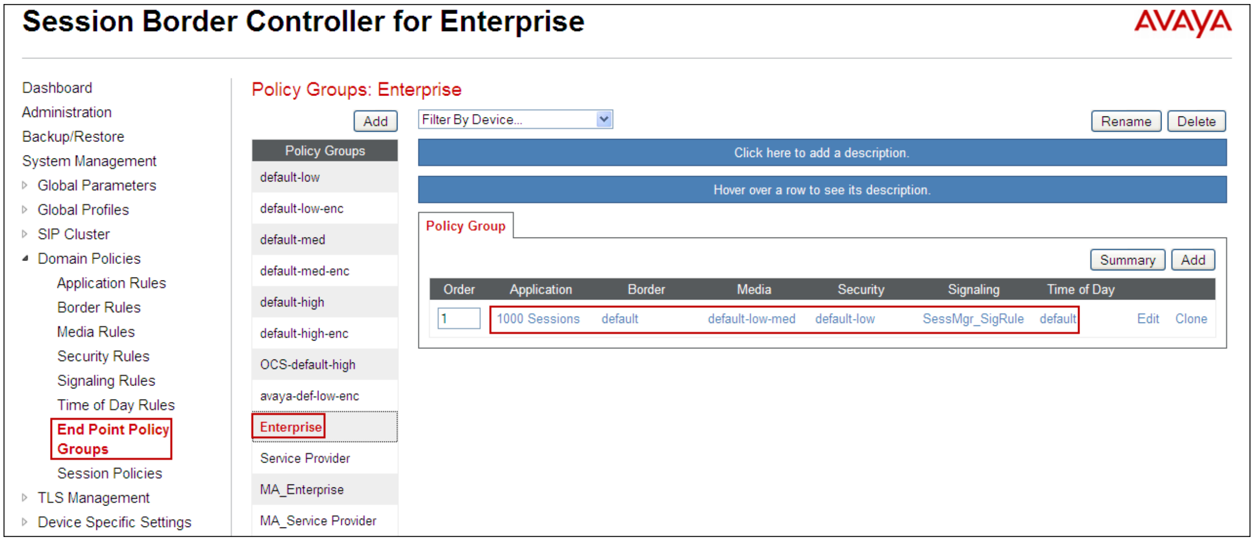
End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE.

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*.**
- Click **Finish**.

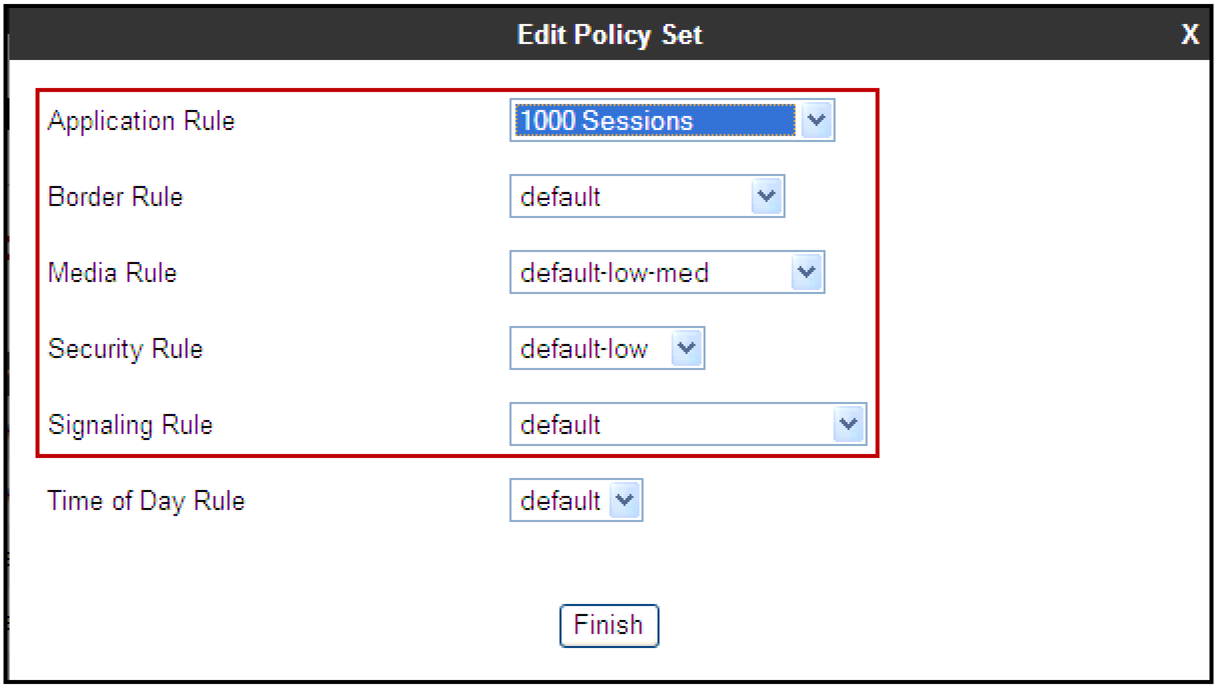

Edit Policy Set
X
Application Rule
1000 Sessions
Border Rule
default
Media Rule
default-low-med
Security Rule
default-low
Signaling Rule
SessMgr_SigRule
Time of Day Rule
default
Finish

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

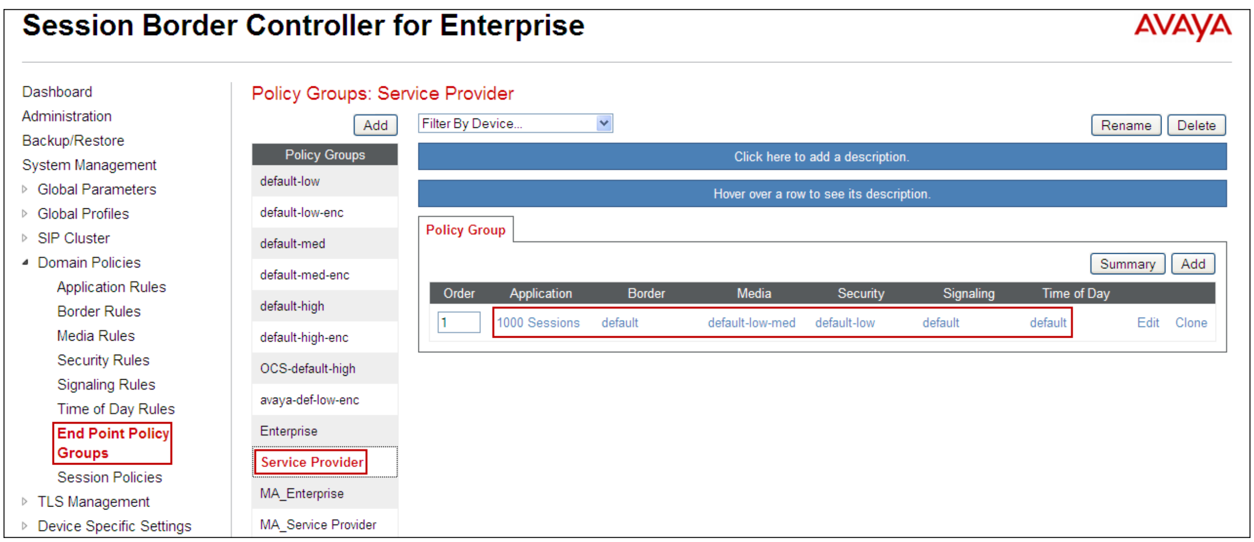


Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add** in the **Policy Groups** section.

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



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

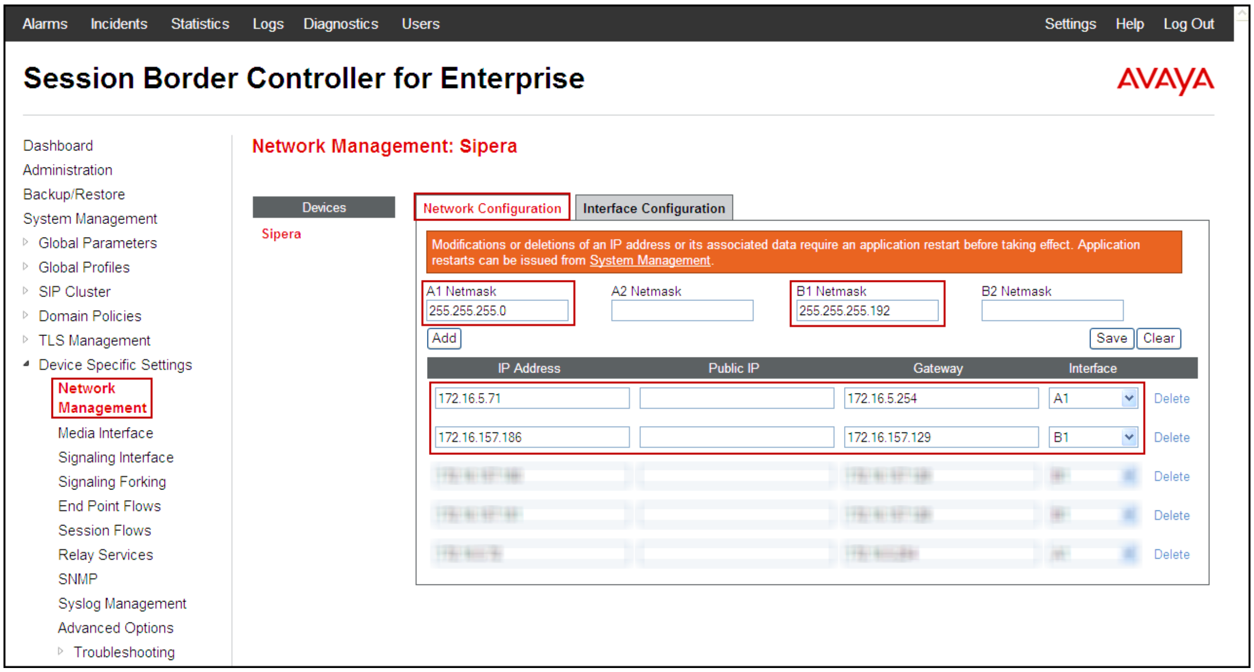


7.4. Device Specific Settings

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.

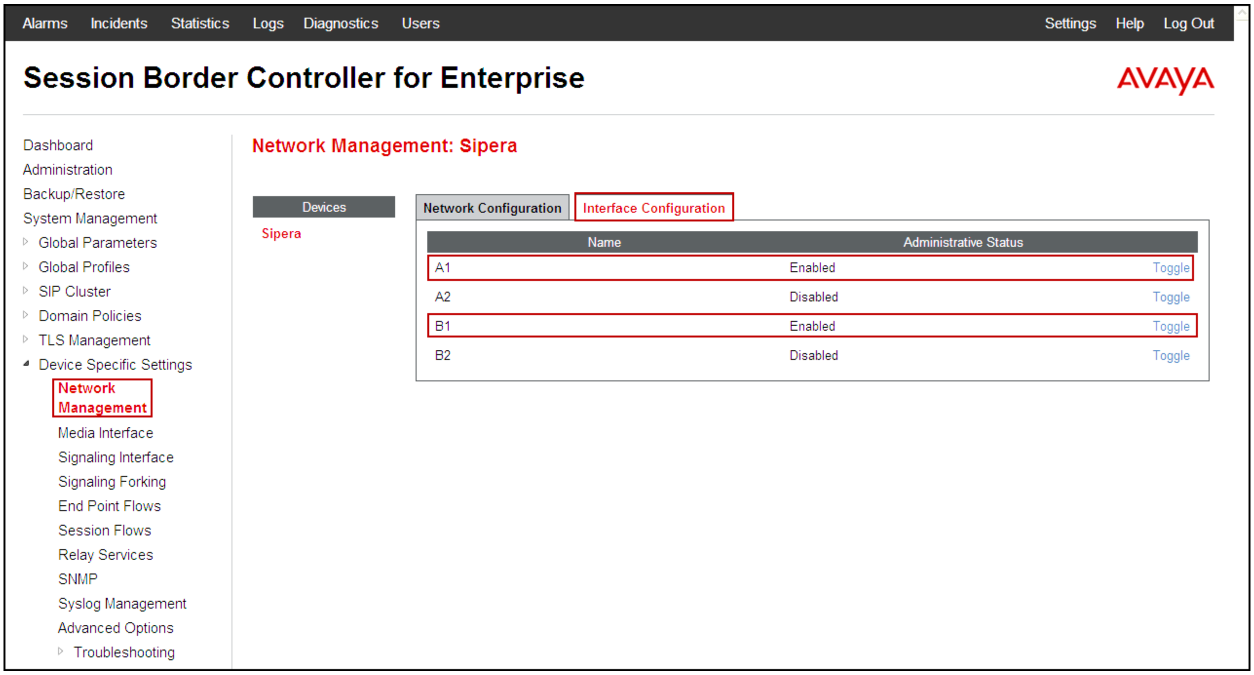
7.4.1. Network Management

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 can 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.

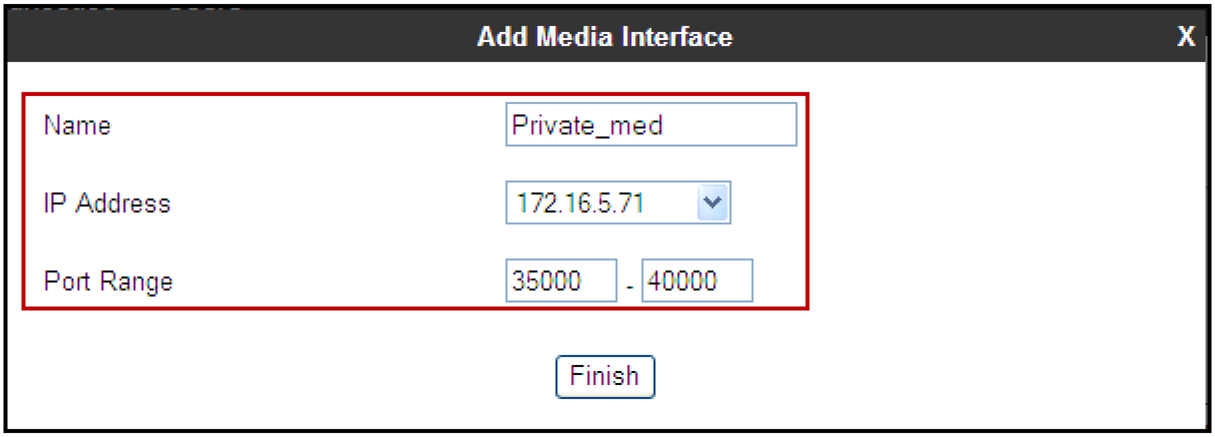


7.4.2. Media Interface

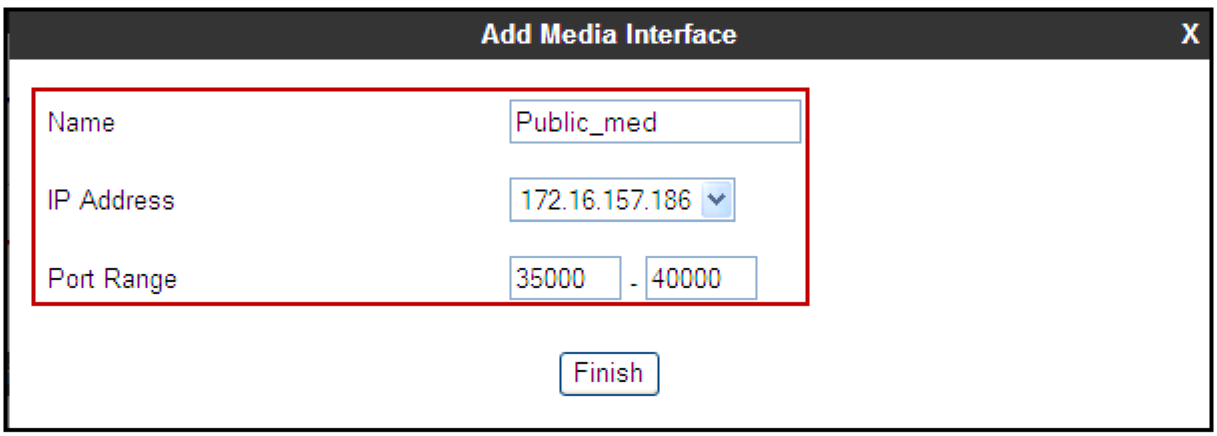
Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

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

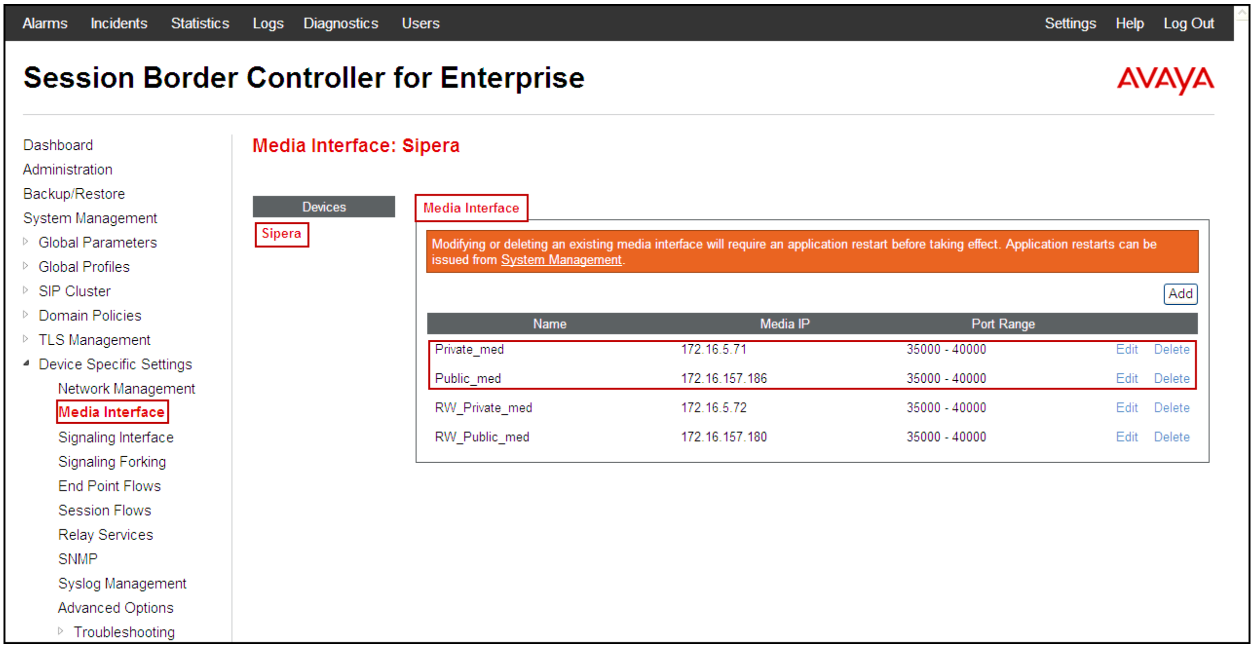
- Select **Add** in the **Media Interface** area**.**
- **Name:** ***Private_med*.**
- Select **IP Address:** ***172.16.5.71*** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range:** ***35000-40000*.**
- Click **Finish.**



- Select **Add** in the **Media Interface** area**.**
- **Name:** ***Public_med*.**
- Select **IP Address:** ***172.16.157.186*** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range:** ***35000-40000*.**
- Click **Finish.**



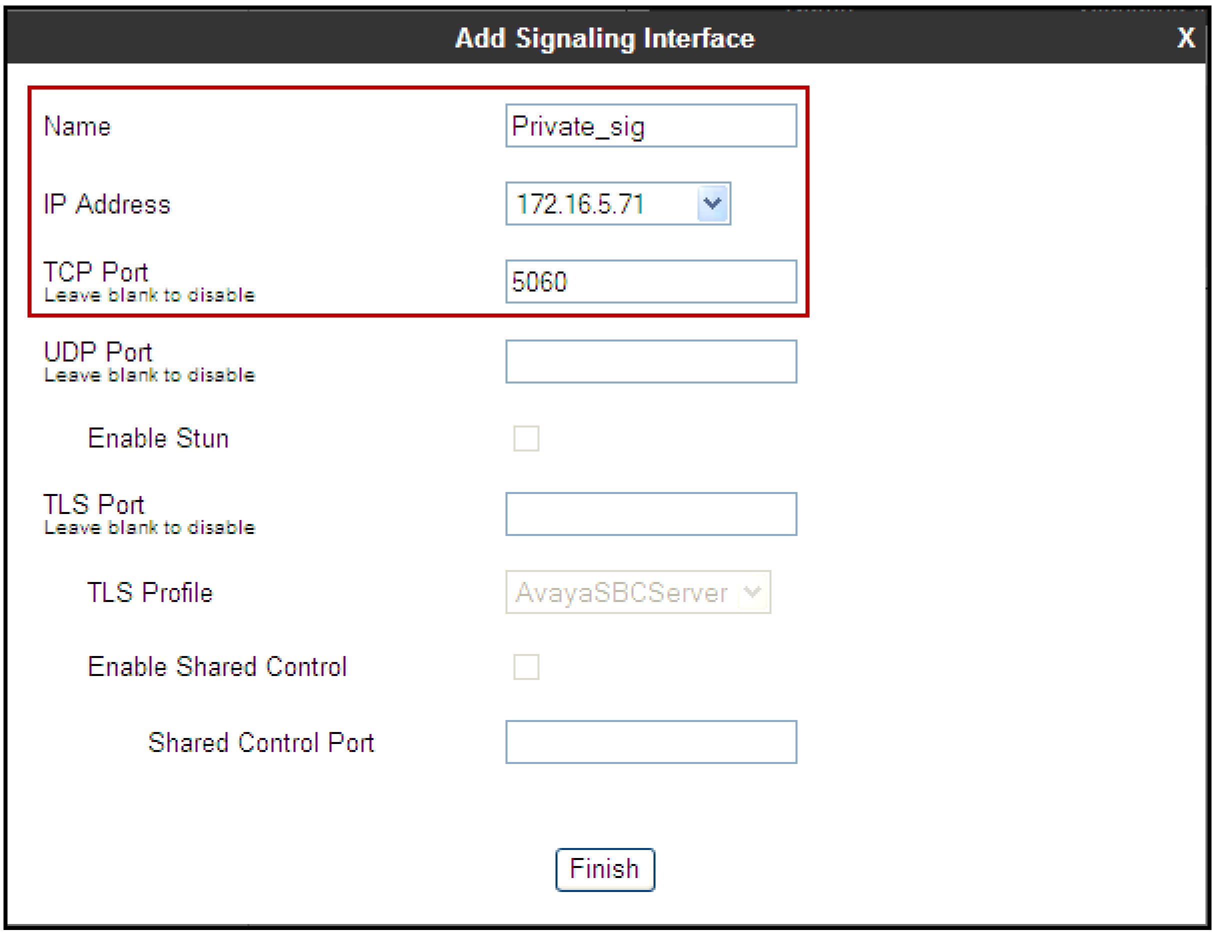
The following screen capture shows the newly created media interfaces.



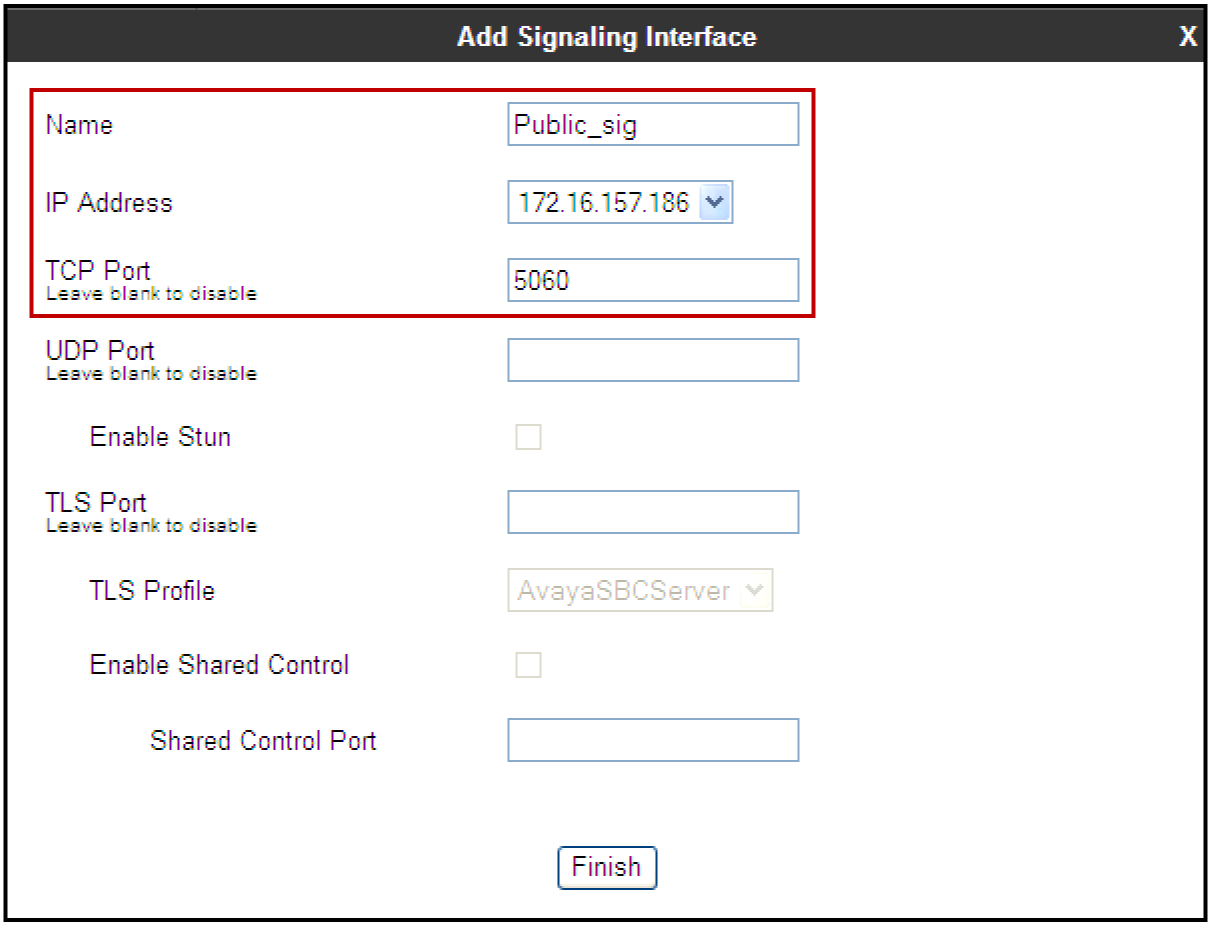
7.4.3. Signaling Interface

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

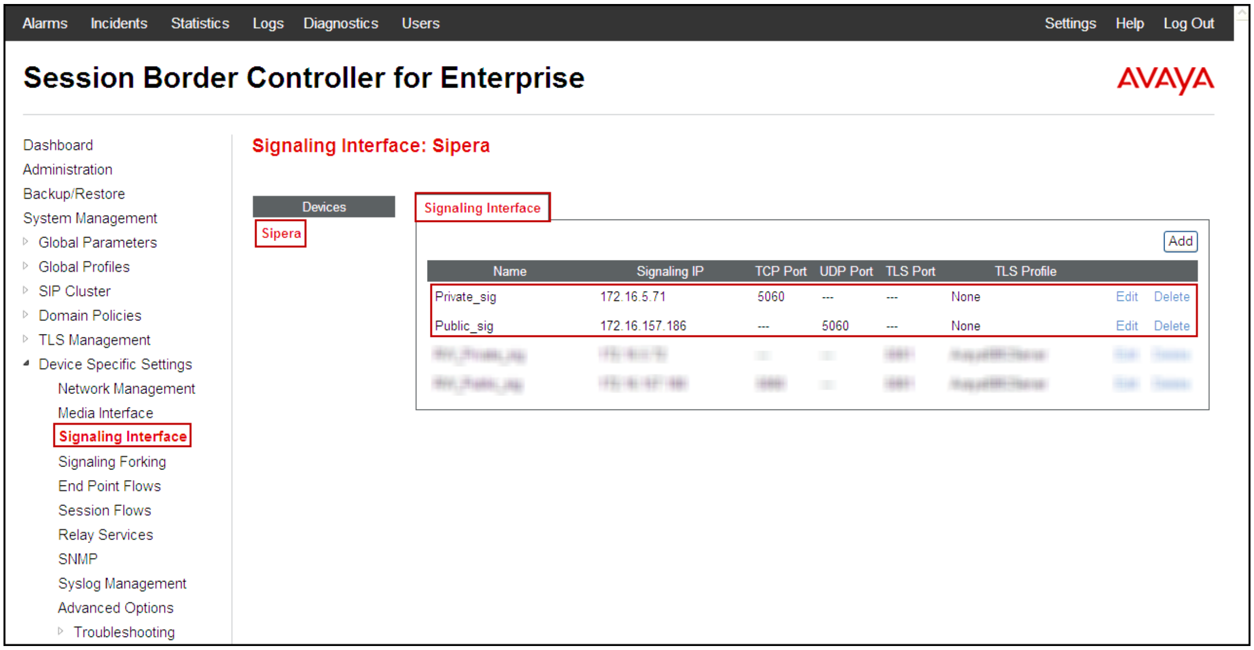
- Select **Add** in the **Signaling Interface** area.
- **Name:** ***Private_sig*.**
- Select **IP Address:** ***172.16.5.71*** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **TCP Port:** ***5060*.**
- Click **Finish.**



- Select **Add** in the **Signaling Interface** area.
- **Name:** ***Public_sig*.**
- Select **IP Address:** ***172.16.157.186*** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** ***5060*.**
- Click **Finish.**

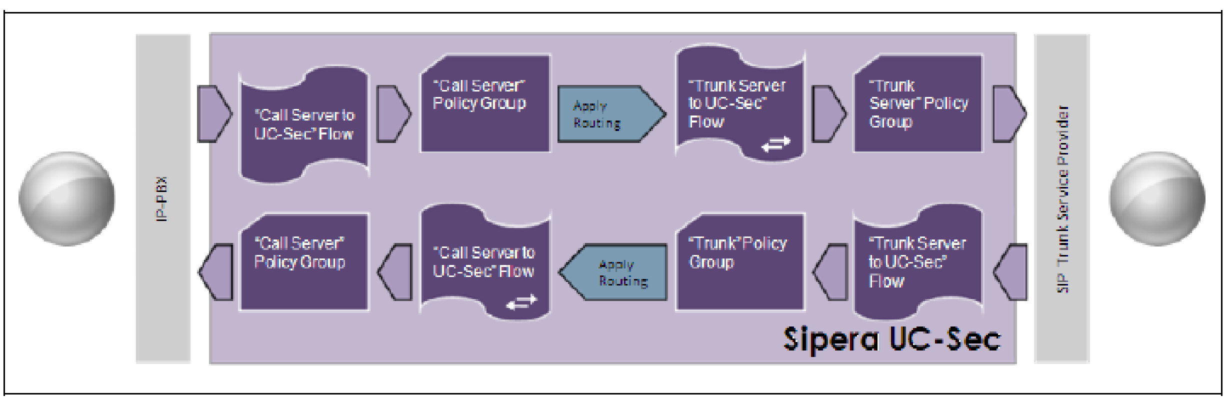


The following screen capture shows the newly created signaling interfaces.



7.4.4. End Point Flows

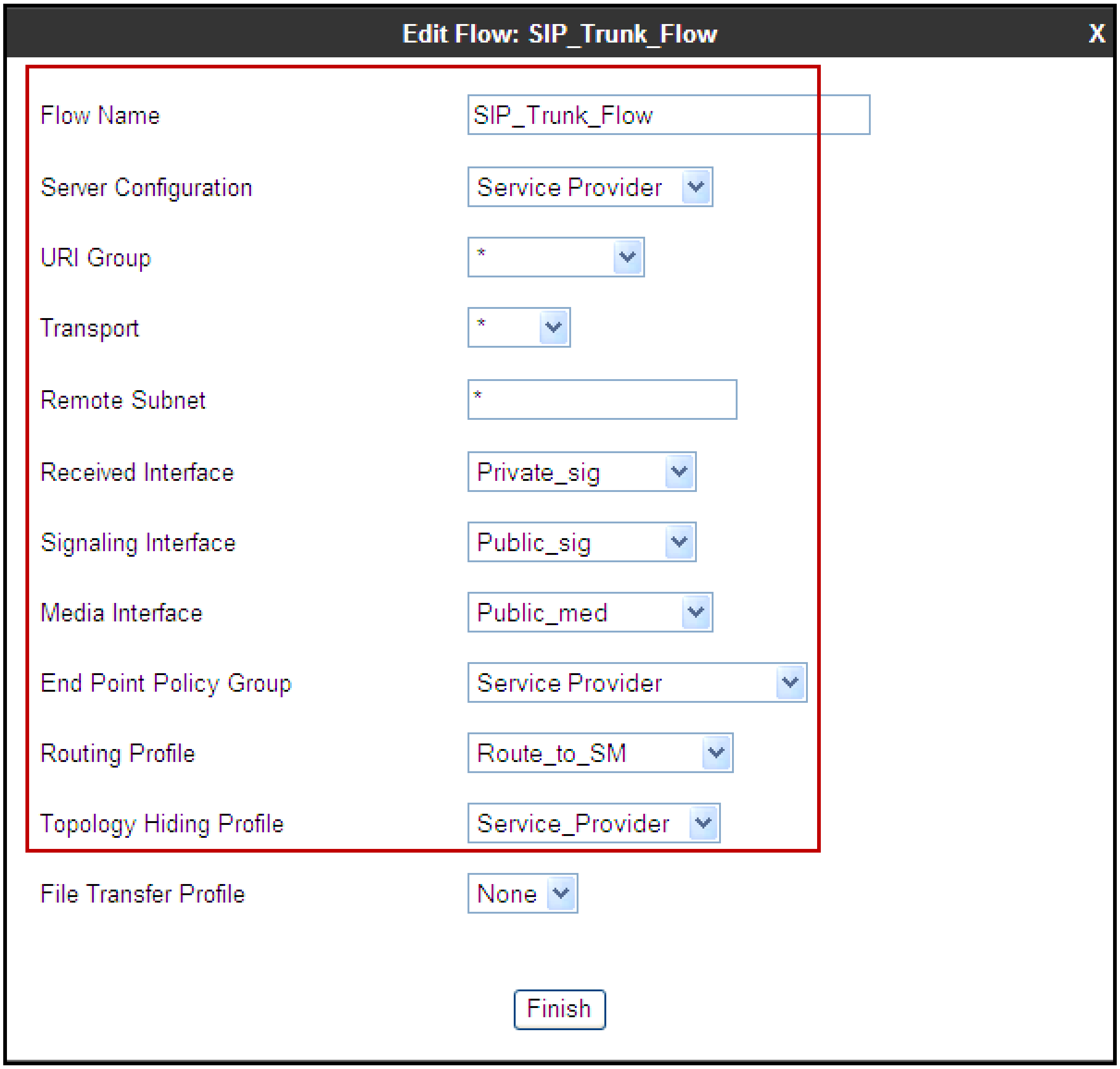
When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing 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 the **Server Flows** tab. Click **Add**.

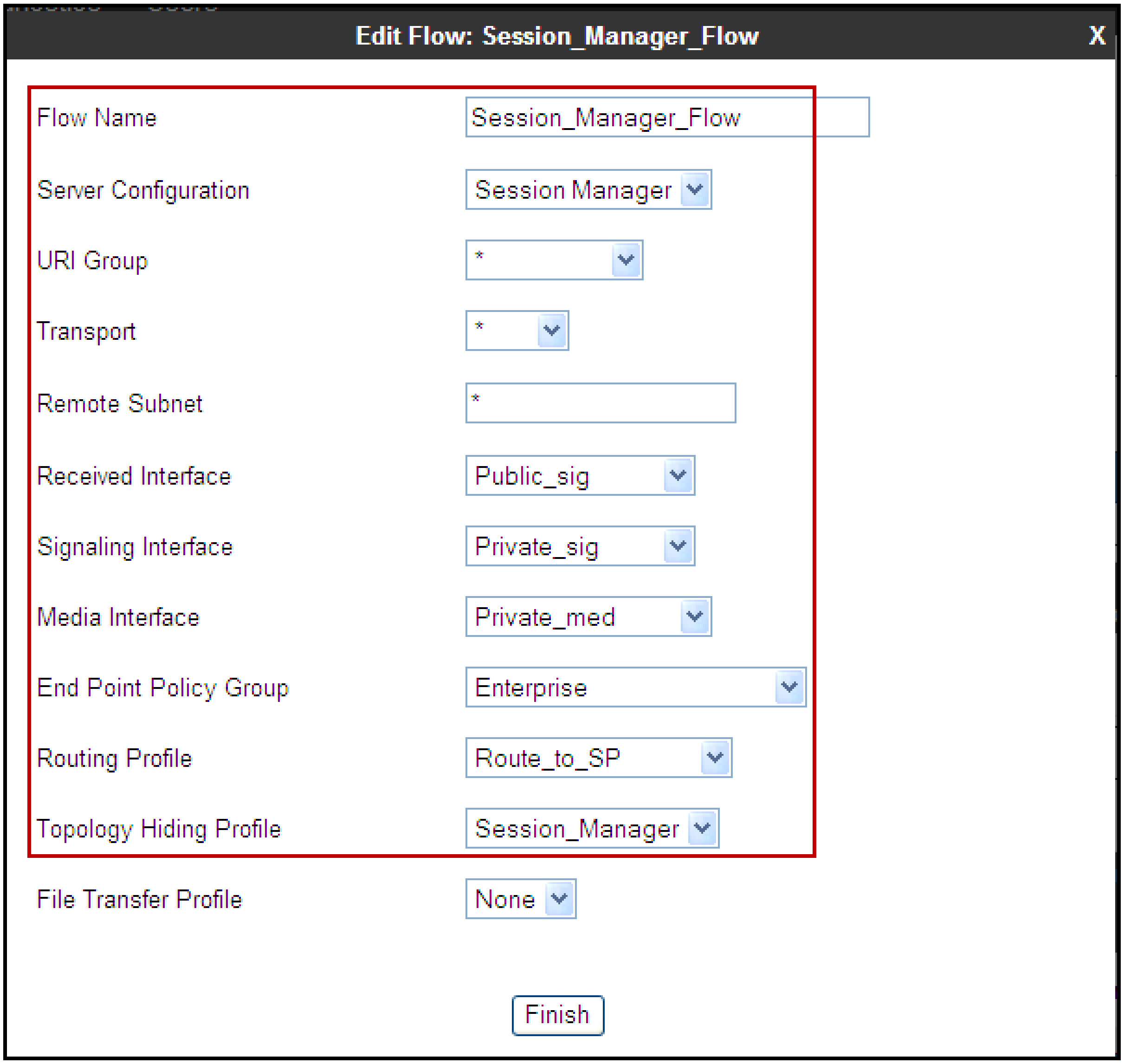
- **Name: *SIP_Trunk_Flow*.**
- **Server Configuration**: ***Service Provider*.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Private_sig*.**
- **Signaling Interface: *Public_sig*.**
- **Media Interface**: ***Public_med*.**
- **End Point Policy Group: *Service 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.**



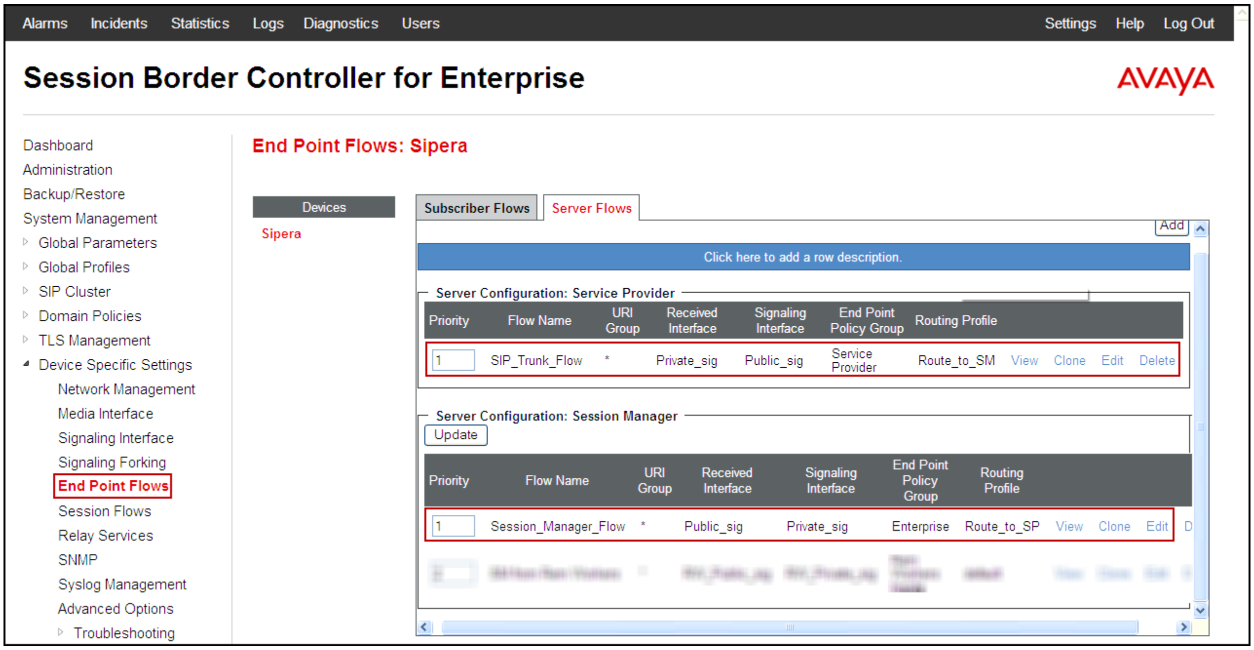
To create the call flow toward Session Manager, click **Add**.

- **Name:** ***Session_Manager_Flow*.**
- **Server Configuration**: ***Session Manager*.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Public_sig*.**
- **Signaling Interface: Private_sig.**
- **Media Interface**: ***Private_med*.**
- **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 newly created **End Point Flows.**



8. SaskTel SIP Trunk Service Configuration

To use SaskTel SIP Trunk service, a customer must request the service from SaskTel using the established sales processes. The process can be started by contacting SaskTel via the corporate web site at: https://www.sasktel.com/support or by calling the Toll Free number at 1-888-773-2122 and requesting information.

During the signup process, SaskTel will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise. SaskTel will provide the IP address of the SIP proxy/SBC, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and the Avaya Session Border Controller for Enterprise 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 with two-way audio 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. Avaya SBCE:
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, policy 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 for 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. Packet captures files (pcap) can be viewed using wireshark.

10. Conclusion

These Application Notes describe the procedures necessary for configuring SaskTel SIP Trunk service with Avaya 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**.

SaskTel 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.

Product documentation for Avaya Aura® Communication Manager, including the following, is available at: http://support.avaya.com/

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3.1, Issue 1, October 2013.

[2] *Administering Avaya Aura® Communication Manager*, Release 6.3 03-300509, Issue 9, October 2013.

Product documentation for Avaya Aura® System Manager, including the following, is available at: http://support.avaya.com/

[3] *Administering Avaya Aura® System Manager*, Release 6.3, Issue 3, October 2013.

Product documentation for Avaya Aura® Session Manager, including the following, is available at: http://support.avaya.com/

[4] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013.

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: http://support.avaya.com/

[5] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014.

[6] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 2013.

[7] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, July 2013.

Product documentation for Avaya one-X® Communicator and Avaya Flare® Experience for Windows, including the following, is available at: http://support.avaya.com/

[8] *Administering Avaya one-X® Communicator*, July 2013.

[9] *Administering Avaya Flare® Experience for Windows*, Release 1.1, Document Number: 18-604156, Issue 4, September 2013.

[10] *Implementing Avaya Flare® Experience for Windows*, Release 1.1, Documents Number: 18-604153, Issue 2, February 2013.

[11] *Using Avaya one-X® Communicator*, Release 6.1, October 2011.

Other resources:

[12] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/.

[13] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

12. Appendix A: SigMa Script

The following Signaling Manipulation script was used in the configuration of the Avaya SBCE, **Section 7.2.6**:

Title: Remove Remote Address

```
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
  {
  remove(%HEADERS["Remote-Address"][1]);
}
}
```

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.