Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5 with Servicio Troncal SIP de Axtel – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the service provider Axtel and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise 4.0.5.

The Servicio Troncal SIP de Axtel (Axtel SIP Trunking Service) provides customers with PSTN access via a SIP trunk between the enterprise and the Axtel network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the service provider Axtel and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, Avaya Session Border Controller for Enterprise (Avaya SBCE) 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya SBCE or Avaya Aura® Session Manager.

The Axtel SIP Trunking Service referenced within these Application Notes is designed for enterprise business customers in Mexico. Customers using this service with the Avaya SIP-enabled enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Axtel SIP Trunking Service via a broadband connection to the public Internet.

During the compliance test, Axtel required the SIP trunk to be registered to their network, using a set of credentials supplied. The Avaya SBCE was configured to provide the registration and authentication of the SIP trunk for the enterprise site to the service provider.

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

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- SIP trunk registration with the service provider.
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones.
- Avaya one-X® Communicator supports placing and receiving calls using the local computer or by controlling an external telephone. Usage modes "This Computer" and "Other Phone" were tested. Avaya one-X® Communicator also supports two signaling protocols: H.323 and SIP. Each supported protocol was tested.
- Various call types, including: local, long distance and international.
- Codecs G729B and G.711A and proper codec negotiation.
- DTMF tone transmissions passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection, using the 302 Moved Temporarily method for the transfer of inbound calls back to PSTN.

Items not supported or not tested included the following:

- T.38 fax is not supported.
- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test
- SIP REFER for Network Call Redirection situations involving Communication Manager vectors is not supported. The SIP REFER method is supported and it was successfully tested in all manual call transfer scenarios to the PSTN.
- Operator services such as dialing 0 or 0 + 10 digits are not supported.

2.2. Test Results

Interoperability testing of the Axtel SIP Trunk Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations and limitations described below:

- **Shuffling**: shuffling needed to be disabled on the SIP trunk, on the corresponding signaling group form in Communication Manager, in order to avoid problems of no audio path observed during the tests for some incoming calls.
- **Outbound Caller Party Number (CPN) Restriction**: On outbound calls where the user activates CPN Block, “anonymous” is sent by the enterprise in the user part of the From header, while the actual number of the calling party is sent in the P-Asserted-Identity header for authentication and billing purposes, as expected. The number from the PAI header is being propagated by Axtel to the PSTN user, who can still see the number of the calling party.
- **Calls from EC500 mobile telephones**: Axtel uses a “phone-context” parameter as part of the user of SIP URIs on incoming calls to the enterprise. On incoming calls from EC500 mobile phones, Communication Manager was unable to properly identify the CLI of these mobile phones and match the number with valid administered entries in the “off-pbx-telephone station-mapping” form, preventing the use of feature-name-extensions capabilities, such as the dialing of Idle Appearance FNE.
- **Incoming Call - All Trunks Busy Condition**: In a situation when all channels on the SIP trunk are in a busy state and a new incoming call is attempted, the enterprise sends an error code “500 Service Unavailable” as a response to the new INVITE, but there is no indication to the PSTN caller, who hears silence (local calls) or ring (international calls).

2.3. Support

For technical support on the Axtel SIP Trunk Service offer, visit www.axtel.mx.

3. Reference Configuration

Figure 1 illustrates the sample configuration used during the compliance testing, where the Avaya SIP-enabled enterprise solution is connected to the Axtel SIP Trunking Service through a public Internet WAN connection.

For security purposes, private addresses are shown in these Application Notes for the Avaya SBCE and the Service Provider public network interfaces, instead of the real public IP addresses used during the tests. Also, SIP trunk credential information shown has been changed to fictitious values, and PSTN routable phone numbers used in the compliance test have been changed to non-routable ones.

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

- Avaya Aura® Communication Manager, running on the Avaya Common Server HP Proliant DL360.
- Aura® Session Manager, running on the Avaya Common Server HP Proliant DL360.
- Avaya Aura® System Manager, running on the Avaya Common Server HP Proliant DL360.
- Avaya Session Border Controller for Enterprise running on a Dell R210 V2 Server.
- Avaya Aura® Messaging running on a Dell PowerEdge R610 server.
- Avaya G450 Media Gateway
- Avaya 96x0 and 96x1 Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise infrastructure. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. Other functions of the Avaya SBCE include providing registration capability of the SIP trunk with the service provider, as well as performing network address translation at both the IP and SIP layers.

The transport protocol between the Avaya SBCE and Axtel across the public IP network is UDP. The transport protocol between the Avaya SBCE and the enterprise Session Manager across the enterprise IP network is TCP.

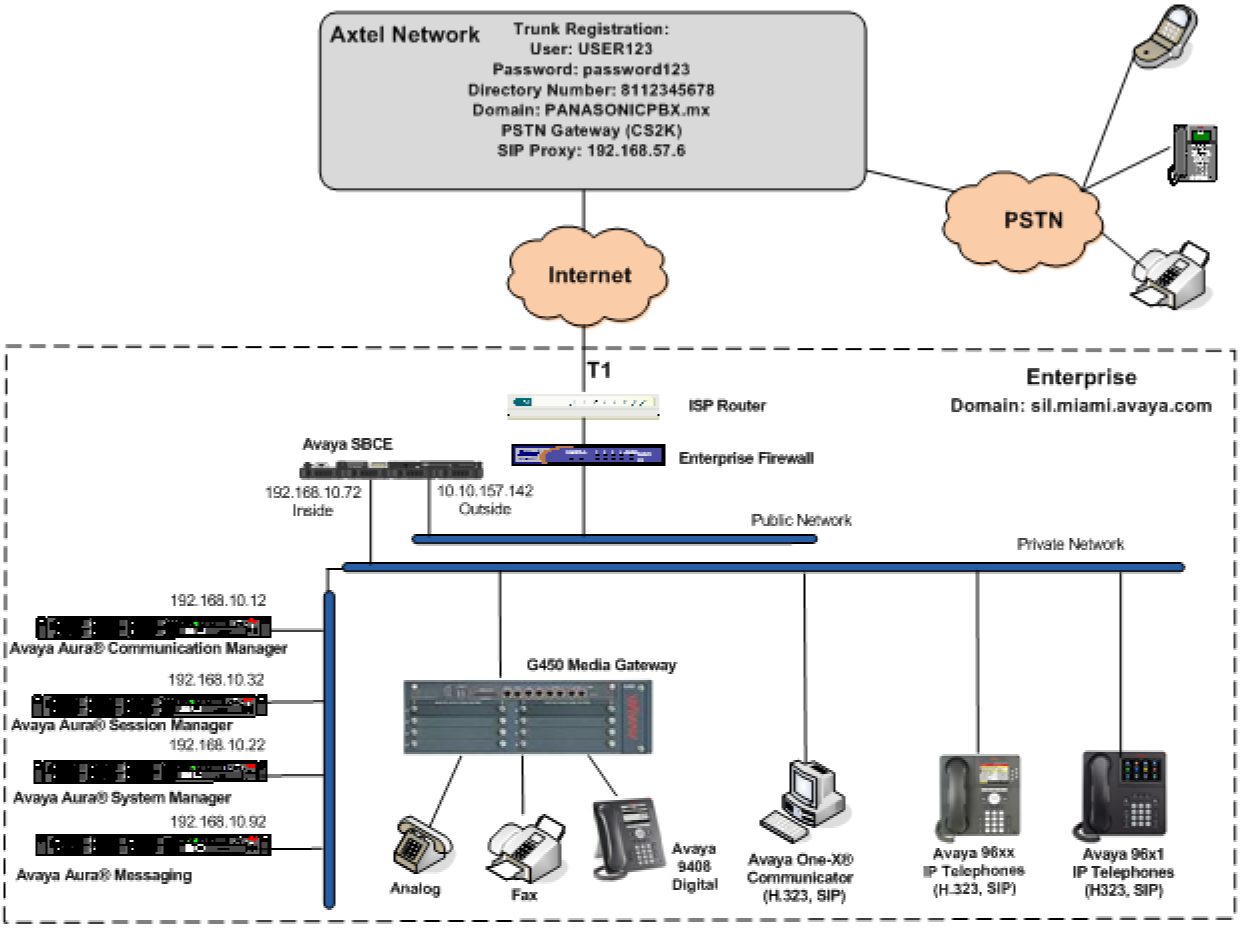


Figure 1: Avaya SIP Enterprise Solution connected to Axtel SIP Trunking Service

For inbound calls, the calls flow from the service provider to the external firewall, to the Avaya SBCE, then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case the Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Axtel network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk and not affect other enterprise SIP traffic. The trunk carried both inbound and outbound traffic.

Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of MWI (Message Waiting Indicator) messages to the enterprise telephones. Messaging was installed on a single standalone server located on the enterprise network, administered as a separate SIP entity in Session Manager. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the Axtel SIP Trunking Service, they are not included in these Application Notes.

During the compliance test, users dialed 9 + N digits to make calls across the SIP trunk to Axtel. For outbound local calls in Monterrey, Mexico, Axtel expected eight digits numbers in the destination headers (Request-URI and To), but the complete 10 digit number (including the area code 81) in the source headers (From, Contact, P-Asserted-Identity). Calls to other endpoints, like mobile phones, Toll Free, long distance, international, etc., used different number lengths in the destination headers, and were provisioned accordingly in Communication Manager and Session Manager.

For inbound calls, Axtel sent to the enterprise the last 4 digits of the 10 digit DID number in the destination headers of inbound INVITE messages, and the complete 10 digit number of the calling party, including the area code, in the From header.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager on a HP® Proliant DL360 G7 Server.	6.2 Service Pack 2
Avaya Aura® Session Manager on a HP® Proliant DL360 G7 Server.	6.2 Service pack 2
Avaya Aura® System Manager on a HP® Proliant DL360 G7 Server.	6.2 Service Pack 2
Avaya Aura® Messaging on a Dell PowerEdge R610 Server.	6.2 Service pack 0
Avaya Session Border Controller for Enterprise	4.0.5.Q09
Avaya G450 Media Gateway	31.22.0
Avaya 96x0 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 3.1 SP 4
Avaya 96x0 Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.6.6
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 6.2
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X® Deskphone Edition SIP 6.2
Avaya one-X® Communicator (H.323, SIP)	6.1.5.07-SP5-37595
Avaya 9408 Digital Telephone	2.00
Avaya 6210 Analog Telephone	n/a
Servicio Troncal SIP de Axtel	
Nortel CS2K	SESM 12.0.0.6

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Axtel SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Axtel. It is assumed that the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **287** 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: 12000 10
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 2
                   Maximum Video Capable IP Softphones: 18000 4
                       Maximum Administered SIP Trunks: 24000 287
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   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: 100   0

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

5.2. System Features

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

```
change system-parameters features                               Page   1 of  19
                            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: attd
    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  19
                        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:
```

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 Communication Manager (**procr**) and Session Manager (**asm**). 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
asm                    192.168.10.32
default                0.0.0.0
msgserver              192.168.10.12
procr                  192.168.10.12
procr6                 ::
rselab                 192.168.0.220
```

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 3 was used for this purpose. The Axtel SIP Trunking Service supports codecs G.729B and G.711A, in this order of preference. Enter **G.729B** and **G.711A** in the **Audio Codec** column of the table. Default values can be used for all other fields.

```
change ip-codec-set 3                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 3

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

Since T.38 is not supported, set the **Fax Mode** field to **off** on **Page 2**.

```
change ip-codec-set 3                                           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 Regions

Create a separate IP network region for the service provider trunk group. 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 3 was chosen for the service provider trunks. Use the **change ip-network-region 3** command to configure region 3 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **sil.miami.avaya.com** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the "From" header of SIP messages originating from this IP region. Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes,** the default setting. This will 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. 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 3                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 3
Location: 1        Authoritative Domain: sil.miami.avaya.com
    Name: Axtel
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 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 3 and region 1 (the rest of the enterprise). 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 following example shows the settings used for the compliance test. It indicates that codec set **3** will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 3                                      Page   4 of  20

 Source Region: 3     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    3     y    NoLimit                                             n       t
 2
 3    3                                                                 all
 4
```

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 trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. To facilitate tracing and fault analysis, the compliance test was conducted with the **Transport Method** set to **tcp** and the **Near-end Listen Port** and **Far-end Listen Port** set to **5075**. (For TCP, the well-known port value is 5060).
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer is a Session Manager.

```
change signaling-group 3                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 3             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


   Near-end Node Name: procr                    Far-end Node Name: asm
 Near-end Listen Port: 5075                   Far-end Listen Port: 5075
                                           Far-end Network Region: 3
                                    Far-end Secondary Node Name:
Far-end Domain: sil.miami.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                       IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                  Alternate Route Timer(sec): 6
```

- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **asm**. 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 the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **n**. This setting will effectively disable media shuffling on the SIP trunk. This was needed as a workaround to the no audio path situation on incoming calls described in **Section 2.2**.
- Default values may be used for all other fields.

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 3 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 3                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 3                    Group Type: sip          CDR Reports: y
  Group Name: Axtel                           COR: 1       TN: 1        TAC: 603
   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: 3
                                                     Number of Members: 6
```

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 default value of **600** seconds was used.

```
change trunk-group 3                                            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
```

On **Page 3**, set the **Numbering Format** field to **public.** 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.

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


                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
```

On **Page 4**, set the **Network Call Redirection** field to **y**. This enables the use of the SIP REFER method for calls that are transferred back to the PSTN. Set the **Send Diversion Header** field to **y**. 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**, and **Convert 180 to 183 for Early Media** to **y**, the values preferred by Axtel. Set **Identity for Calling Party Display** to **From**. This setting will instruct Communication Manager to use the From header as the source for caller ID information on incoming calls. Default values were used for all other fields.

```
change trunk-group 3                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
                             Prepend '+' to Calling Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? y
                                     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: From
            Block Sending Calling Party Location in INVITE? 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 public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs), and they are used to authenticate the caller. In the sample configuration, 5 DID numbers were assigned for testing. These 5 numbers were mapped to 5 extensions, 3001 to 3005. These 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 5 extensions.

```
change public-unknown-numbering 1                                Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext             Trk       CPN          CPN
Len Code            Grp(s)    Prefix       Len
                                                 Total Administered: 12
 4  2                                      4        Maximum Entries: 9999
 4  3                                      4
 4  3001            3         8112345678   10    Note: If an entry applies to
 4  3002            3         8112345679   10    a SIP connection to Avaya
 4  3003            3         8112345680   10    Aura(R) Session Manager,
 4  3004            3         8112345681   10    the resulting number must
 4  3005            3         8112345682   10    be a complete E.164 number.
```

In a real customer environment, DID numbers are usually comprised of the local extension plus a prefix. If this is true, then a single public unknown numbering entry could be applied for all extensions. In the example below, all stations with a 4-digit extension length, beginning with 3, will send the calling party number as the **CPN Prefix** plus the extension number.

```
change public-unknown-numbering 1
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext             Trk       CPN          CPN
Len Code            Grp(s)    Prefix       Len

 4  3               3         811234       10
```

5.9. Inbound Routing

In general, the "incoming call handling treatment" form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Axtel is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. During the compliance test, the last 4 digits of the DID number was sent from Axtel to the enterprise. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 3                        Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    4  5678             4   3001
 public-ntwrk    4  5679             4   3002
 public-ntwrk    4  5680             4   3003
 public-ntwrk    4  5681             4   3004
 public-ntwrk    4  5682             4   3005
 public-ntwrk
 public-ntwrk
```

5.10. Outbound Routing

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

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

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   1            4    ext
   2            4    ext
   3            4    ext
   4            4    ext
   5            4    ext
   6            3    dac
   7            4    ext
   8            1    fac
   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  11
                               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: #1
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    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:
```

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 3 which contains the SIP trunk group to the service provider.

```
change ars analysis 0                                           Page   2 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all             Percent Full: 1

          Dialed             Total     Route     Call    Node    ANI
          String           Min  Max   Pattern    Type    Num     Reqd
    001                    13   13     3         intl            n
    01                     12   12     3         natl            n
    13                     8    8      3         hnpa            n
    83                     8    8      3         hnpa            n
    84                     8    8      3         hnpa            n
    86                     8    8      3         hnpa            n
                                                                 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 3 for 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 3 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.

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

6. Configure Avaya Aura® Session Manager

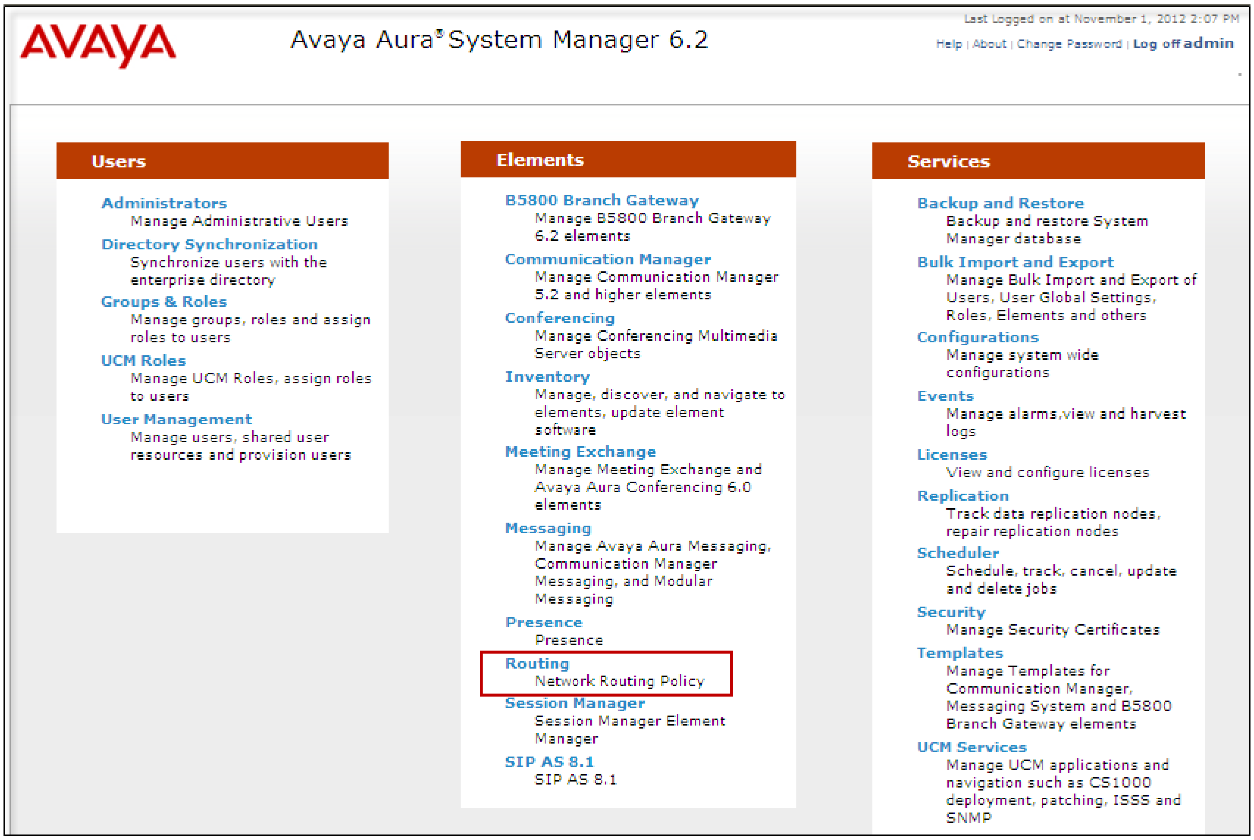
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE
- 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
- Session Manager Instance, corresponding to the Session Manager Server to be managed by System Manager

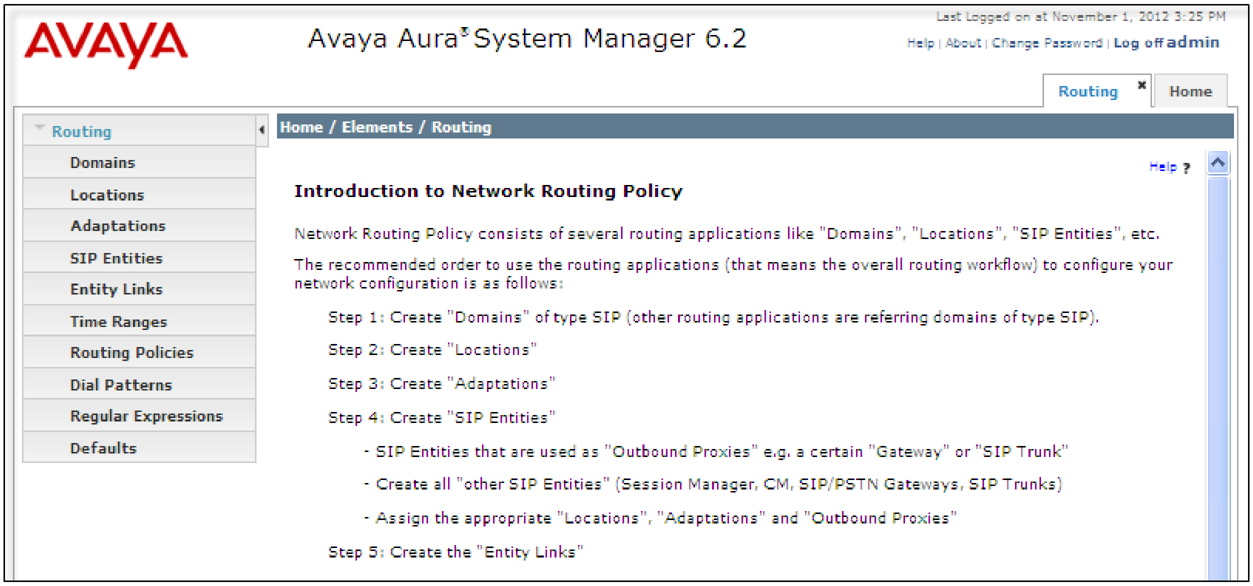
It may not be necessary to create all the items above when creating a connection to the service provider, since some of them would have already been defined as part of the initial Session Manager installation. This includes entries such as certain SIP domains, locations, SIP entities, and Session Manager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

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 and click on **Log On** (not shown). The **Home** screen shown below is then displayed. Some of the links below will be referenced in subsequent sections of the Session Manager configuration. Most items will be located under the **Routing** section highlighted below.



Clicking the **Elements → Routing** link brings up the **Introduction to Network Routing Policy** screen. The left-hand pane navigation tree contains many of the items to be configured in the following sections.



6.2. SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this will be the enterprise domain, **sil.miami.avaya.com**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

6.3. Locations

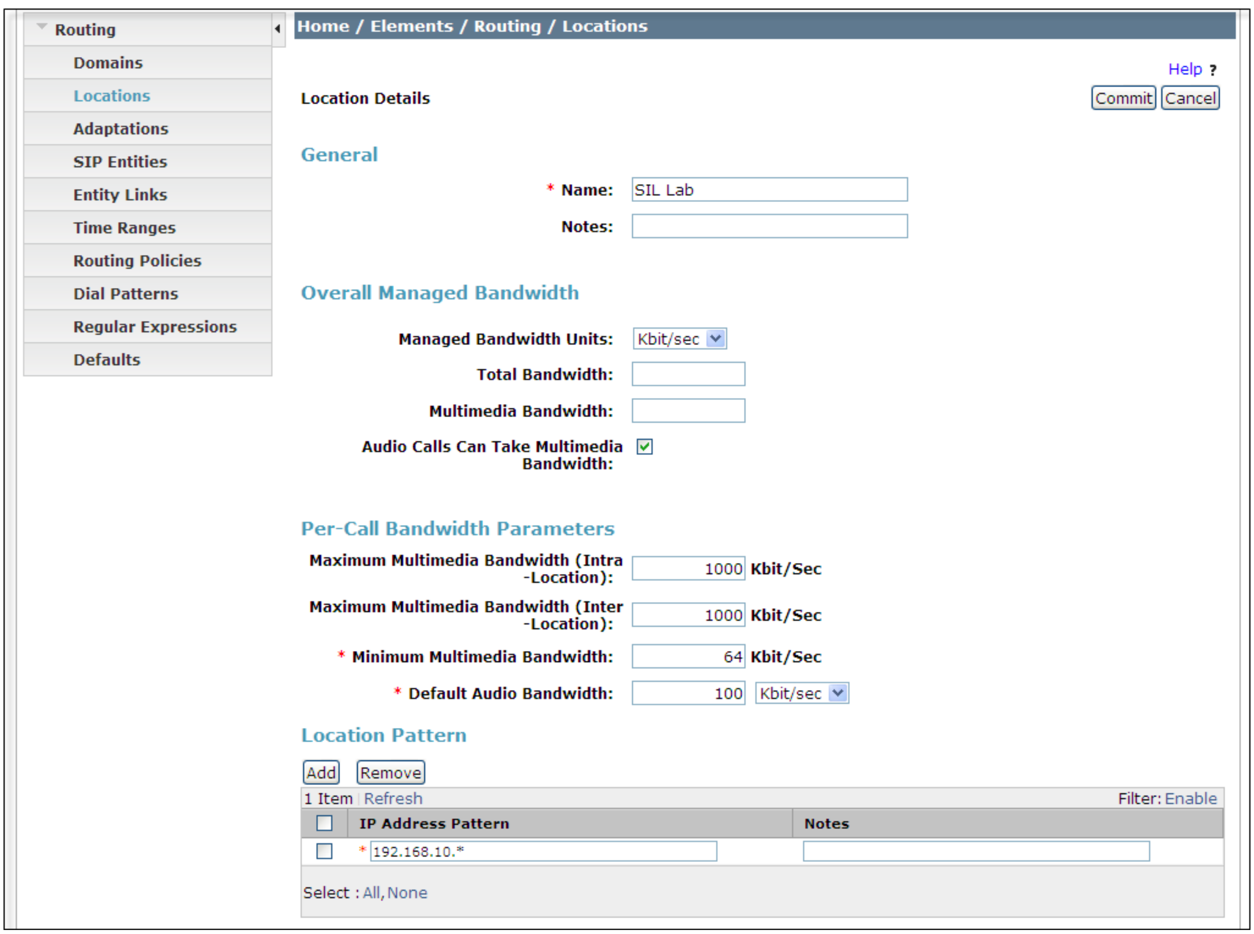
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).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

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

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

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

The abbreviated screen below shows the addition of the location **SIL Lab**, which includes all the equipment on the enterprise network. Note that call bandwidth management parameters should be set per customer requirements. Click **Commit** to save.

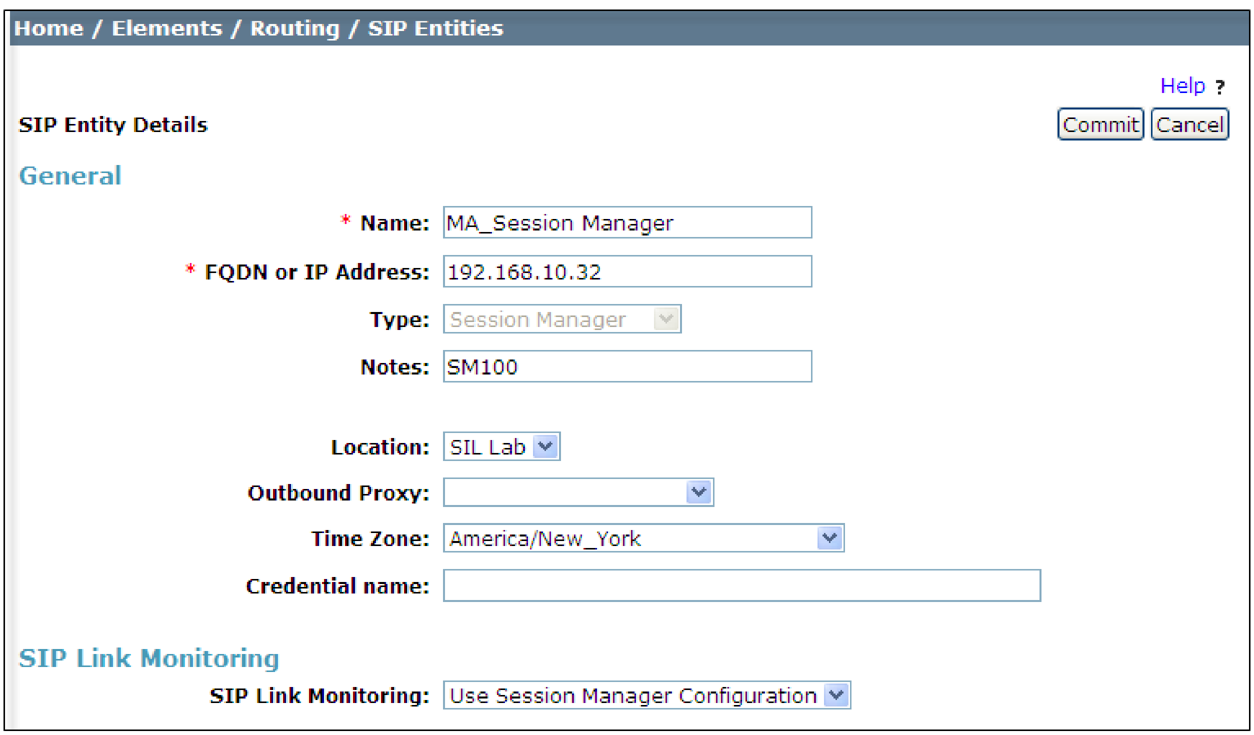


6.4. SIP Entities

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 navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager** If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created. For the compliance test, all components were located in location **SIL Lab**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager Security Module is entered for **FQDN or IP Address**.

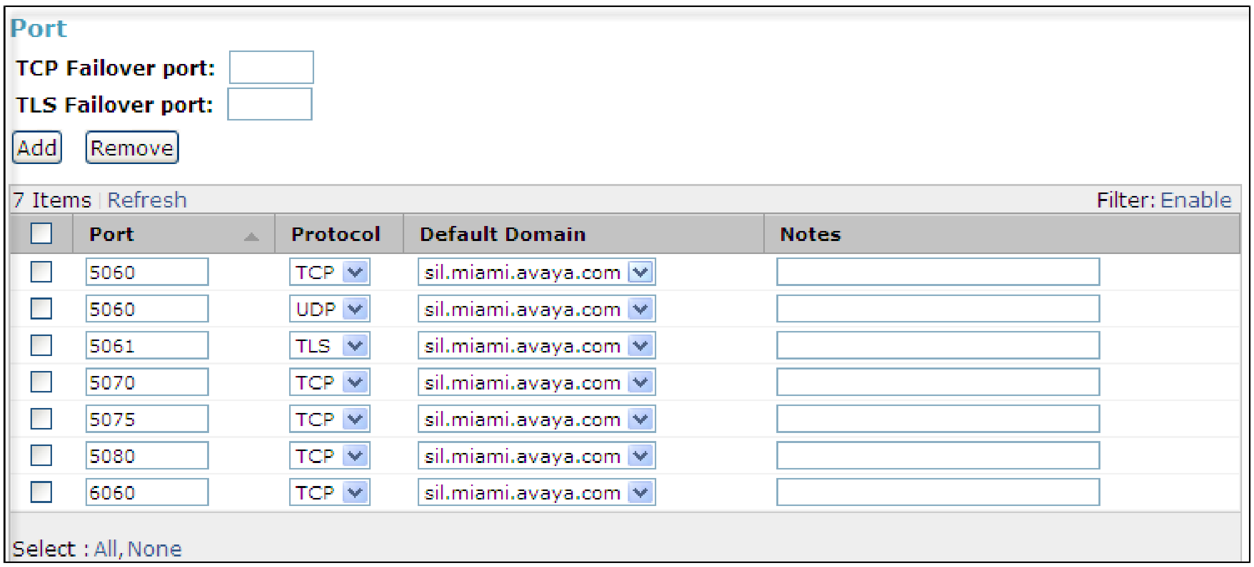


To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

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

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

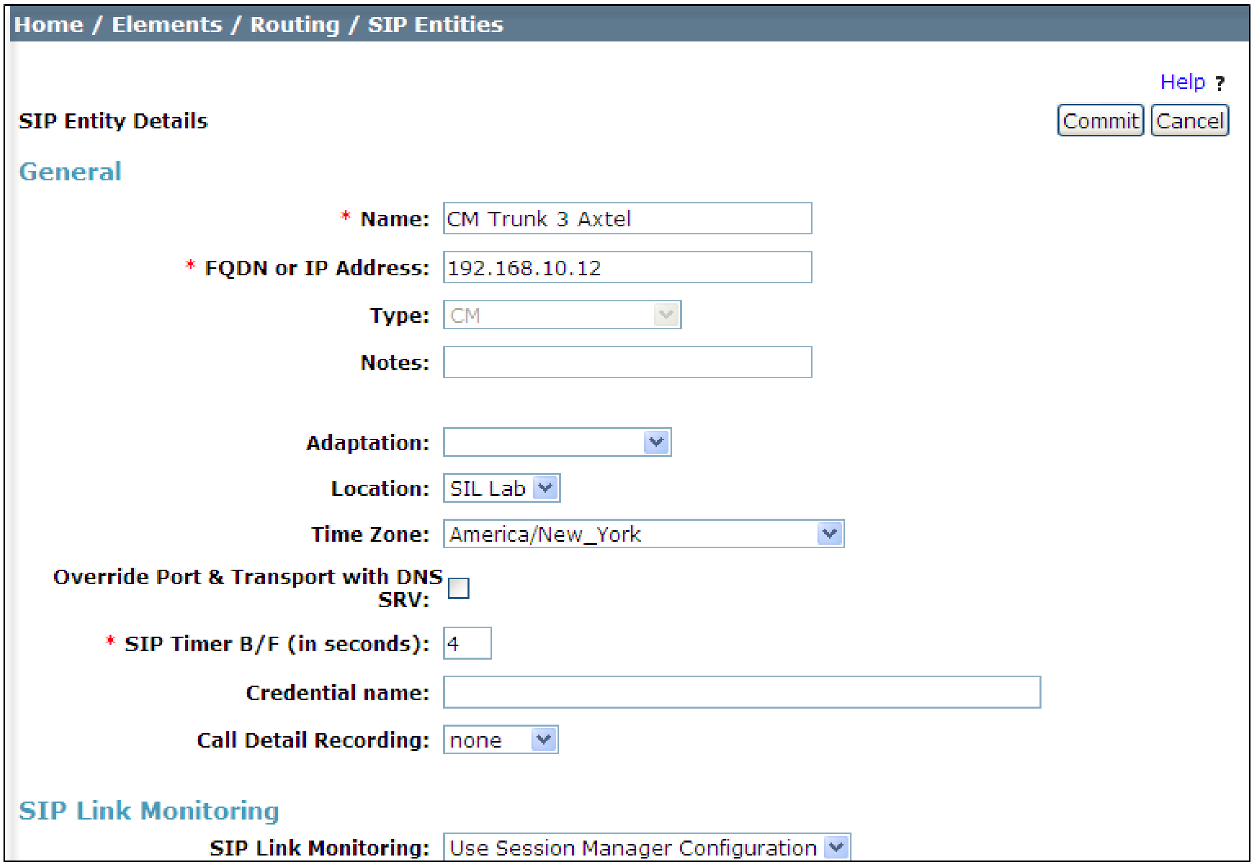
The screen below shows the ports used by Session Manager in the shared lab environment. Only TCP ports 5060 and 5075 are directly relevant to these Application Notes.



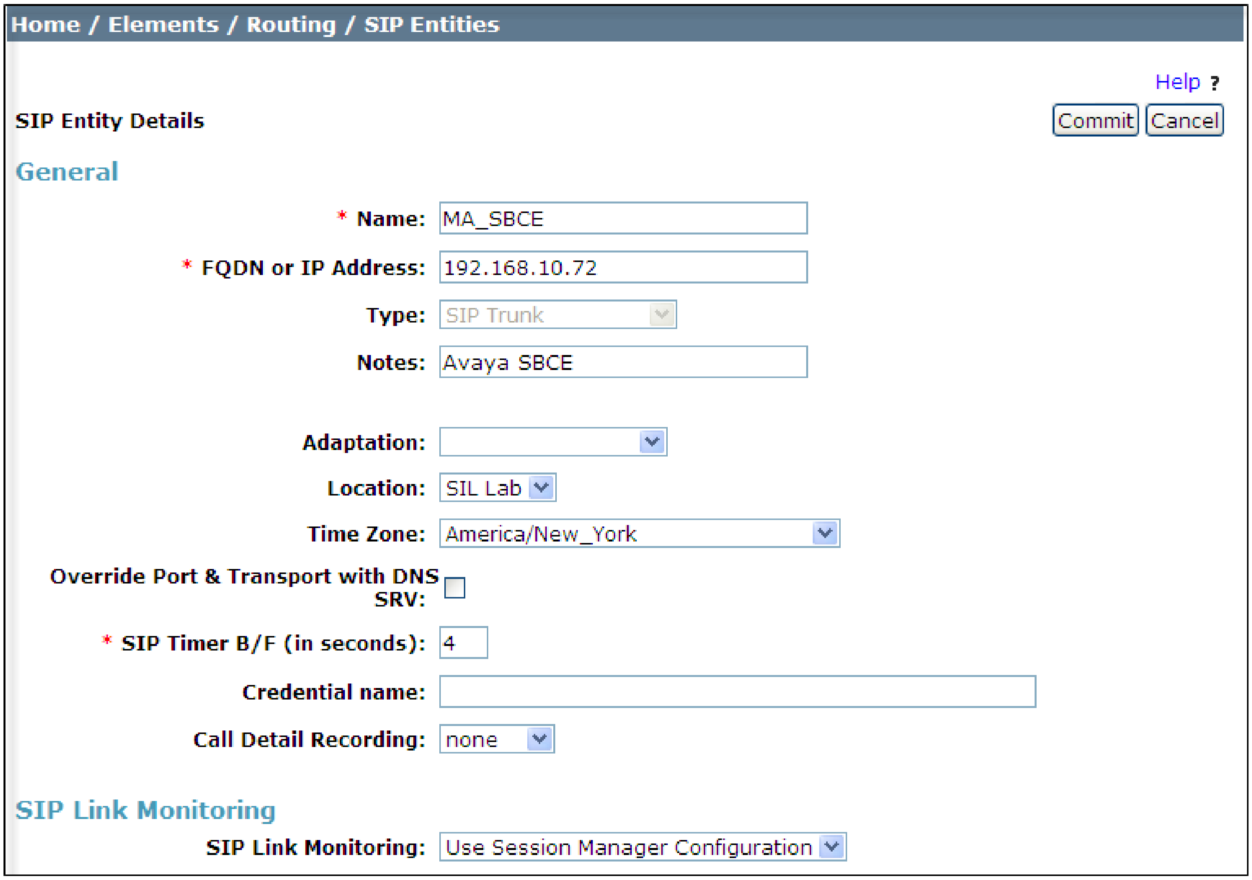
Port	Protocol	Default Domain	Notes
5060	TCP	sil.miami.avaya.com	
5060	UDP	sil.miami.avaya.com	
5061	TLS	sil.miami.avaya.com	
5070	TCP	sil.miami.avaya.com	
5075	TCP	sil.miami.avaya.com	
5080	TCP	sil.miami.avaya.com	
6060	TCP	sil.miami.avaya.com	

In order for Session Manager to route SIP service provider traffic on a specific trunk group in Communication Manager, a separate link to Communication Manager is required. This requires the creation of a separate SIP entity for Communication Manager, other than the one created at Session Manager installation for use by all other SIP traffic between the two servers.

The following screen shows the addition of this SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the "**procr"** interface in Communication Manager.



The following screen shows the addition of the Avaya SBCE Entity. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).



6.5. Entity Links

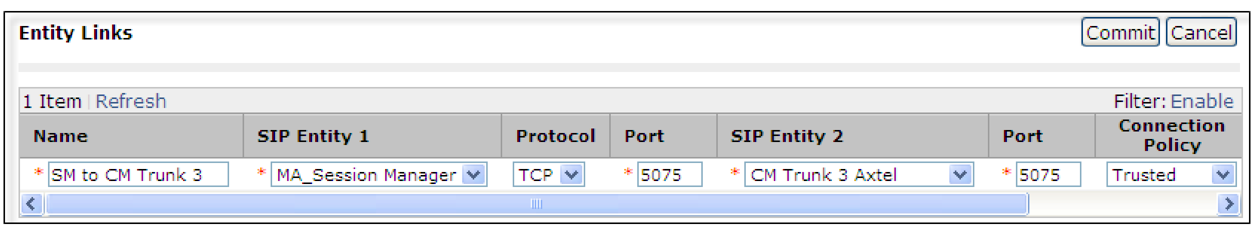
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation 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 from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

Click **Commit** to save.

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 facilitate troubleshooting since the signaling traffic would not be encrypted.

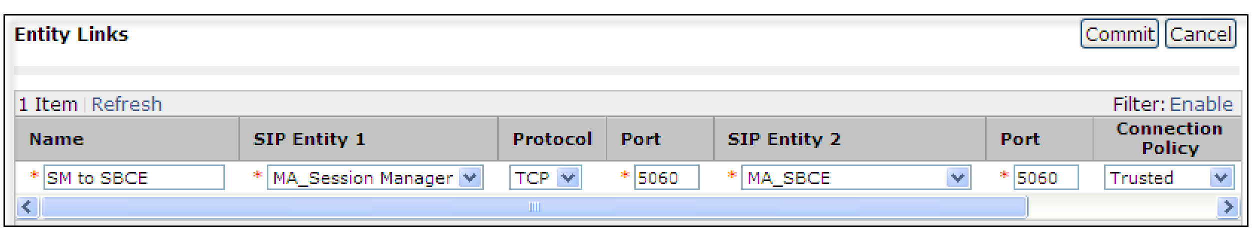
The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.


Entity Links Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM to CM Trunk 3	* MA_Session Manager	TCP	* 5075	* CM Trunk 3 Axtel	* 5075	Trusted

Entity Link to the Avaya SBCE:


Entity Links Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM to SBCE	* MA_Session Manager	TCP	* 5060	* MA_SBCE	* 5060	Trusted

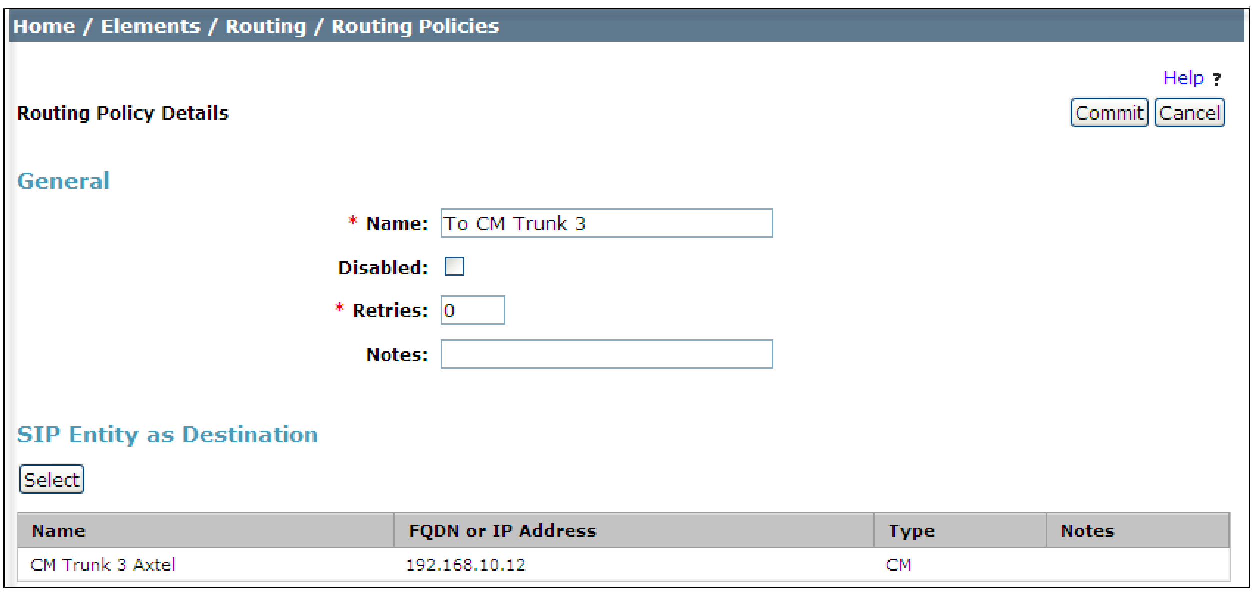
6.6. Routing Policies

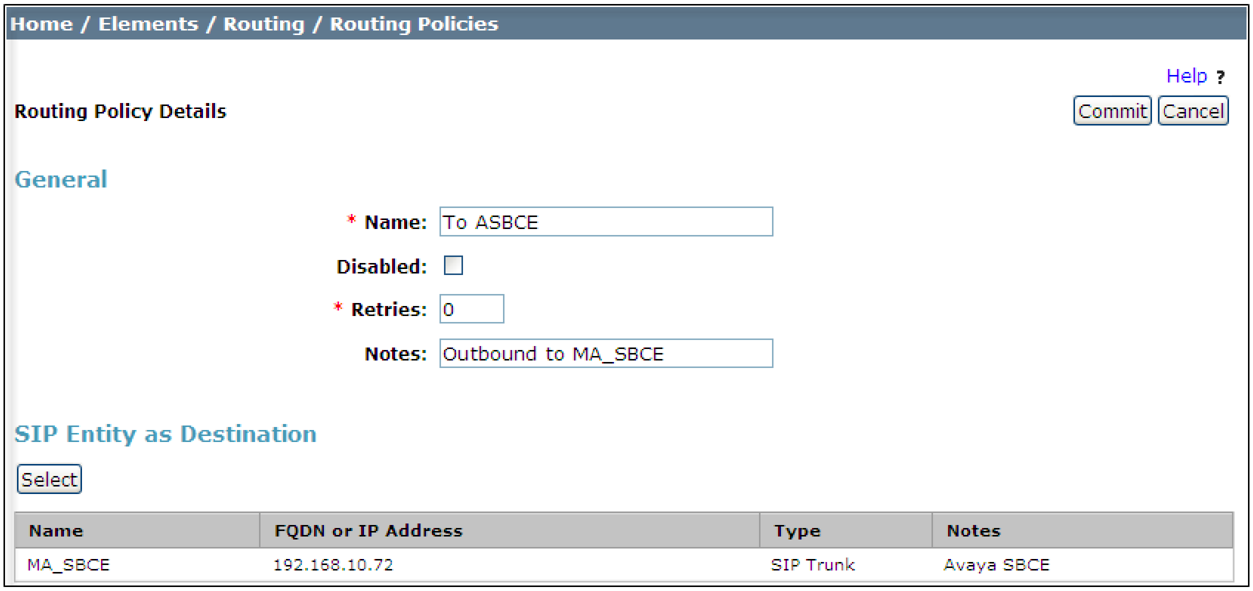
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter the following values:

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

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

The following screens show the Routing Policies for Communication Manager and the Avaya SBCE





6.7. Dial Patterns

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

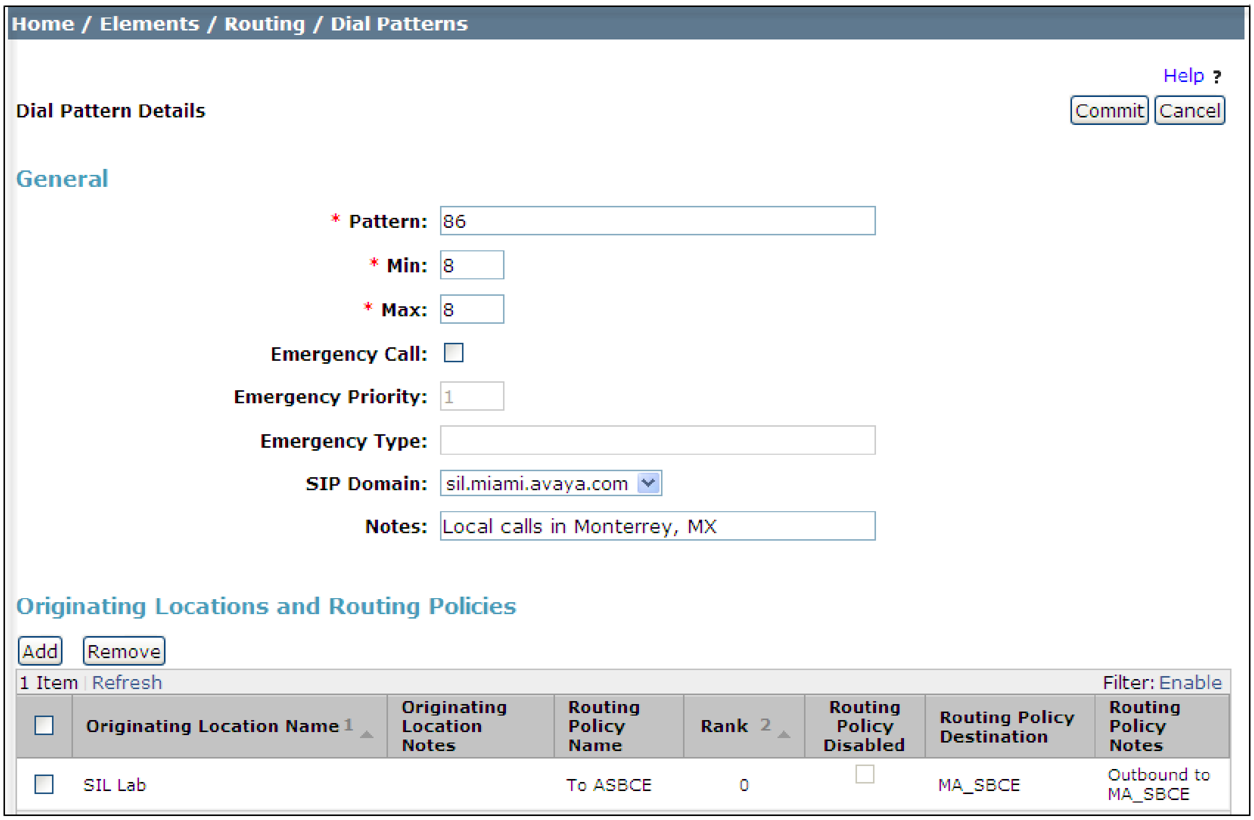
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:**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

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

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

Two examples of the Dial Patterns used for the compliance test are shown, one for outbound calls from the enterprise to the PSTN and one for inbound calls. Other Dial Patterns (e.g., 01 long distance national, 001 international calls to the U.S., etc.) were similarly defined.

The example in this screen shows that in the test environment, 8 digit dialed numbers for outbound local calls in Monterrey, Mexico, beginning with 84 and originating from the SIL Lab location uses route policy **To ASBCE**, which sends the call out to the PSTN via the Avaya SBCE to the Axtel SIP Trunk.


Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

Commit Cancel

General

* Pattern: 86

* Min: 8

* Max: 8

Emergency Call:

Emergency Priority: 1

Emergency Type:

SIP Domain: sil.miami.avaya.com

Notes: Local calls in Monterrey, MX

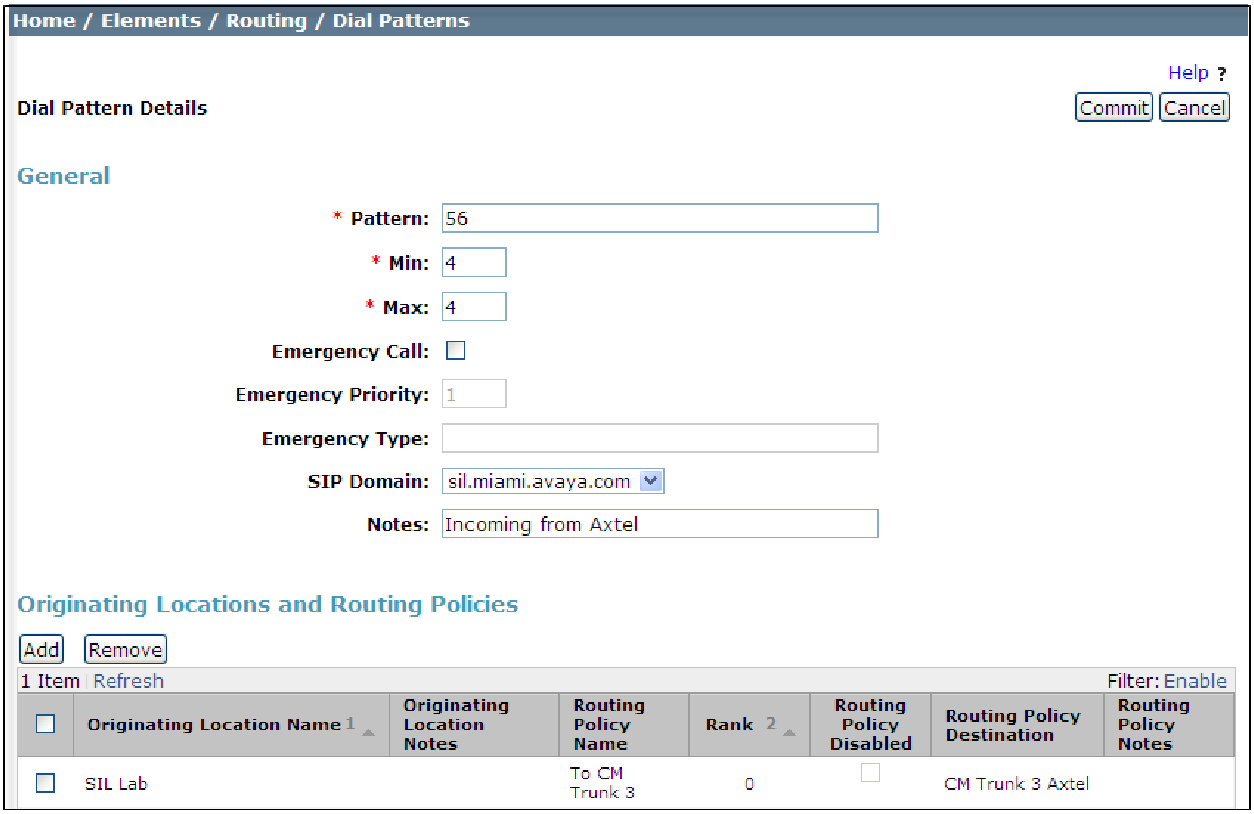
Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
	SIL Lab		To ASBCE	0		MA_SBCE	Outbound to MA_SBCE

The second example shows that a 4 digit number starting with **56**, which is the DID range assigned by Axtel to the enterprise, will use route policy **To CM Trunk 3** to Communication Manager.



6.8. Add/View Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If the 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:

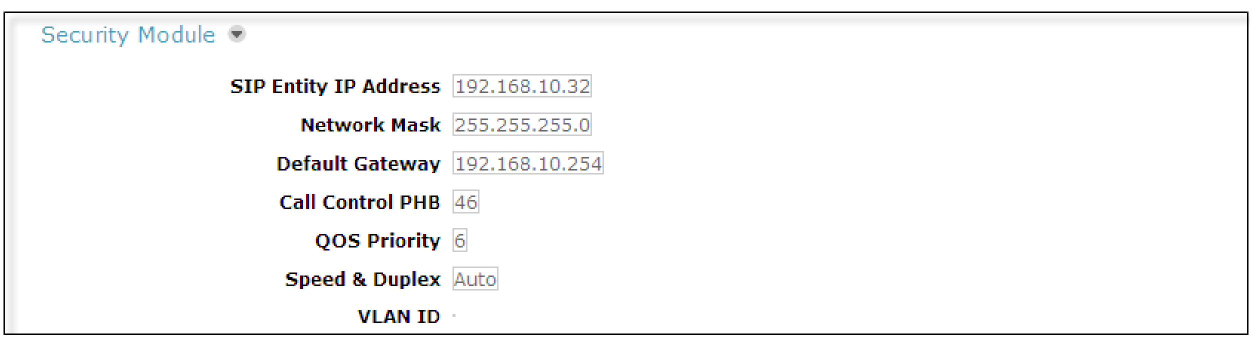
- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

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

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

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

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows Security Module values used for the compliance test.



7. Configure Avaya Session Border Controller for Enterprise

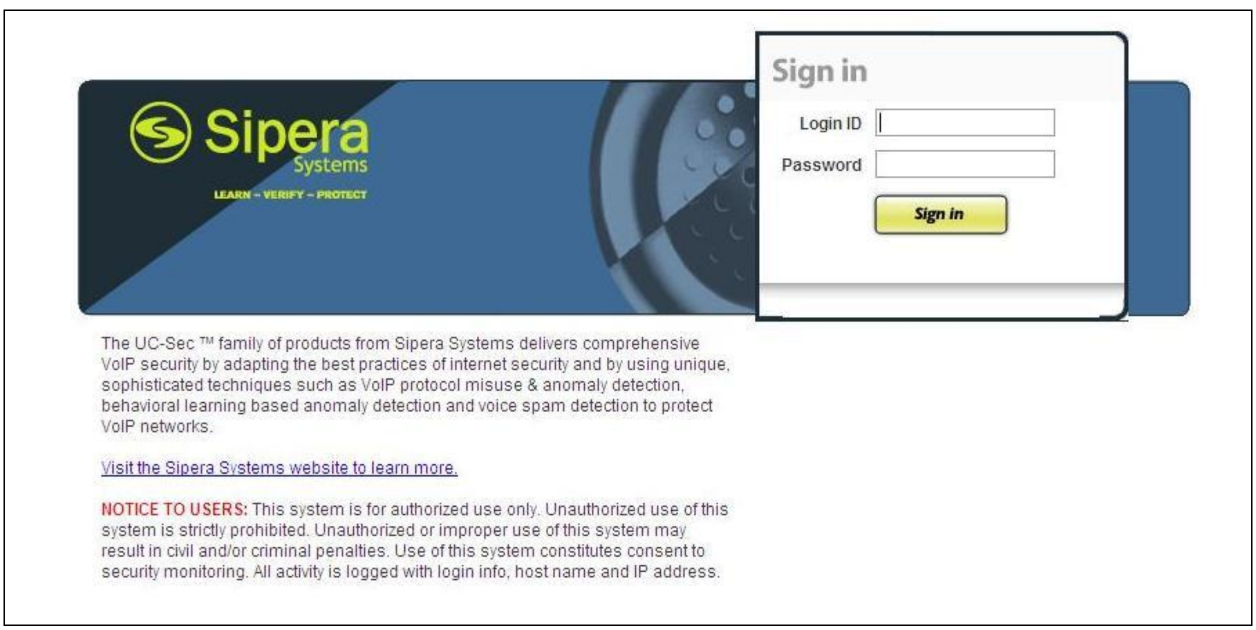
In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Axtel SIP Trunking Service.

These Application Notes assume that the initial installation of the Avaya SBCE and the assignment of a management IP Address have already been completed.

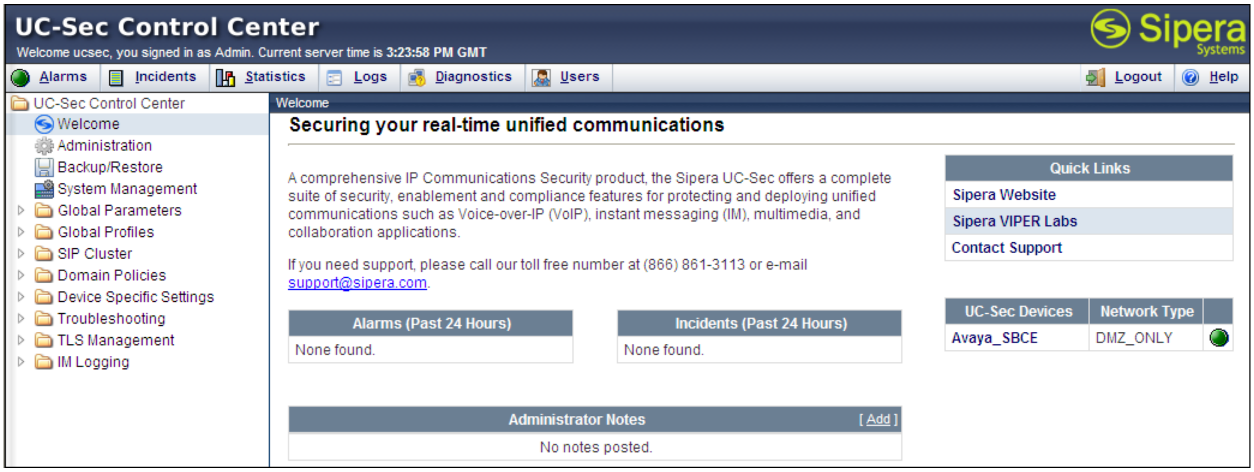
7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Select the **UC-Sec Control Center.**

Log in using the appropriate credentials.

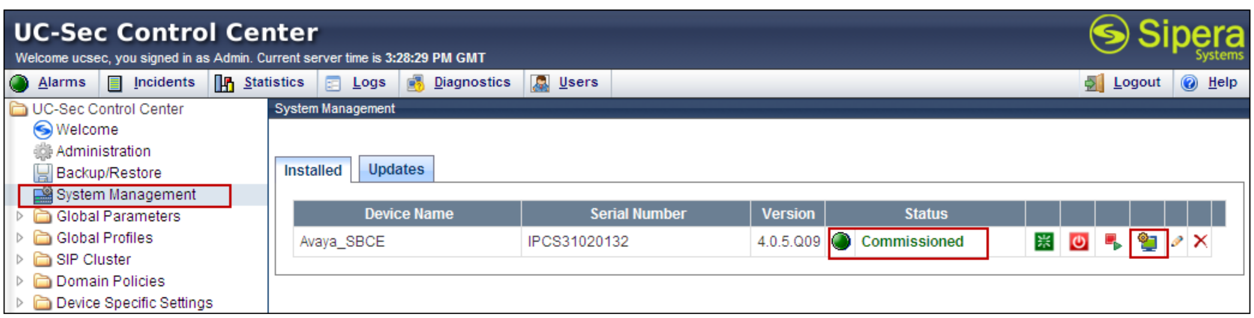


Once logged in, the Welcome screen of the UC-Sec Control Center is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.

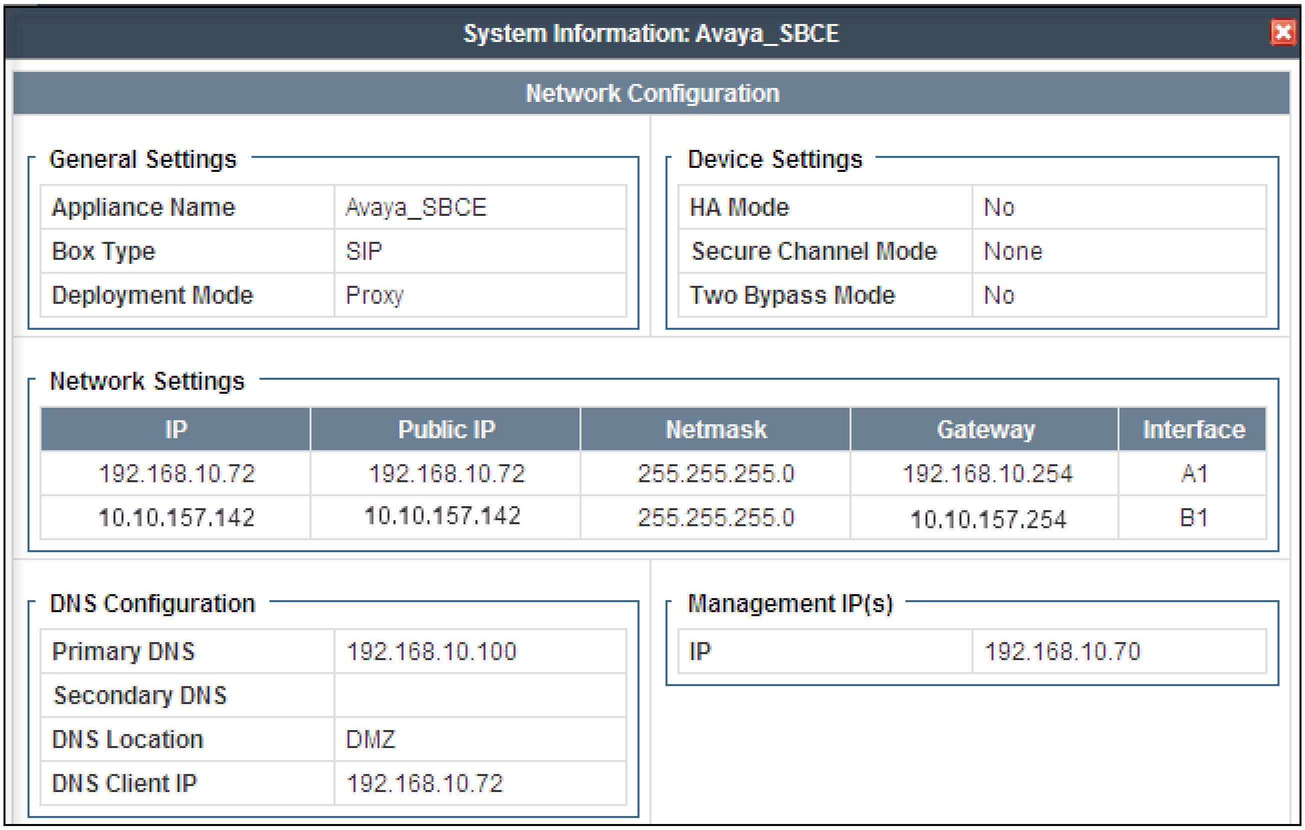


7.2. System Information

To view system information that was configured during installation, select **System Management** on the left navigation pane. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **Avaya_SBCE** is shown. Verify the device is showing the status of **Commissioned,** like in the screen below.



To view the network information assigned to the Avaya SBCE, click the **View Config** icon (third icon from the right). The **System Information** window is displayed as shown on the next screen.



The **System Information** screen shows the **Network Settings, DNS Configuration** and **Management IP** information provided during installation. Note that the A1 and B1 interfaces correspond to the inside and outside interfaces for the A-SBCE, as shown in **Figure 1**.

7.3. Global Profiles

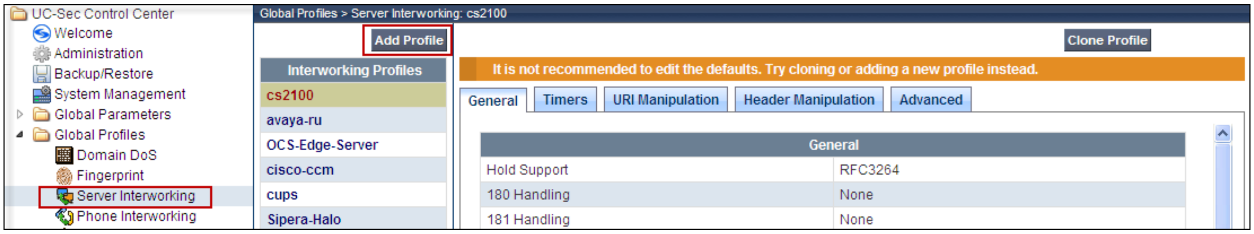
The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all UC-Sec appliances.

7.3.1. Server Interworking

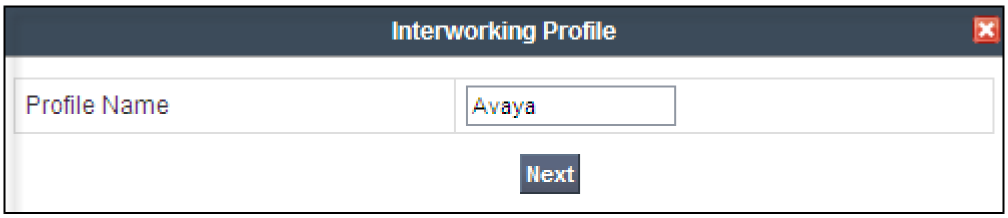
Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. These default profiles may be used as is, they can be cloned and modified, or new profiles can be configured as described next.

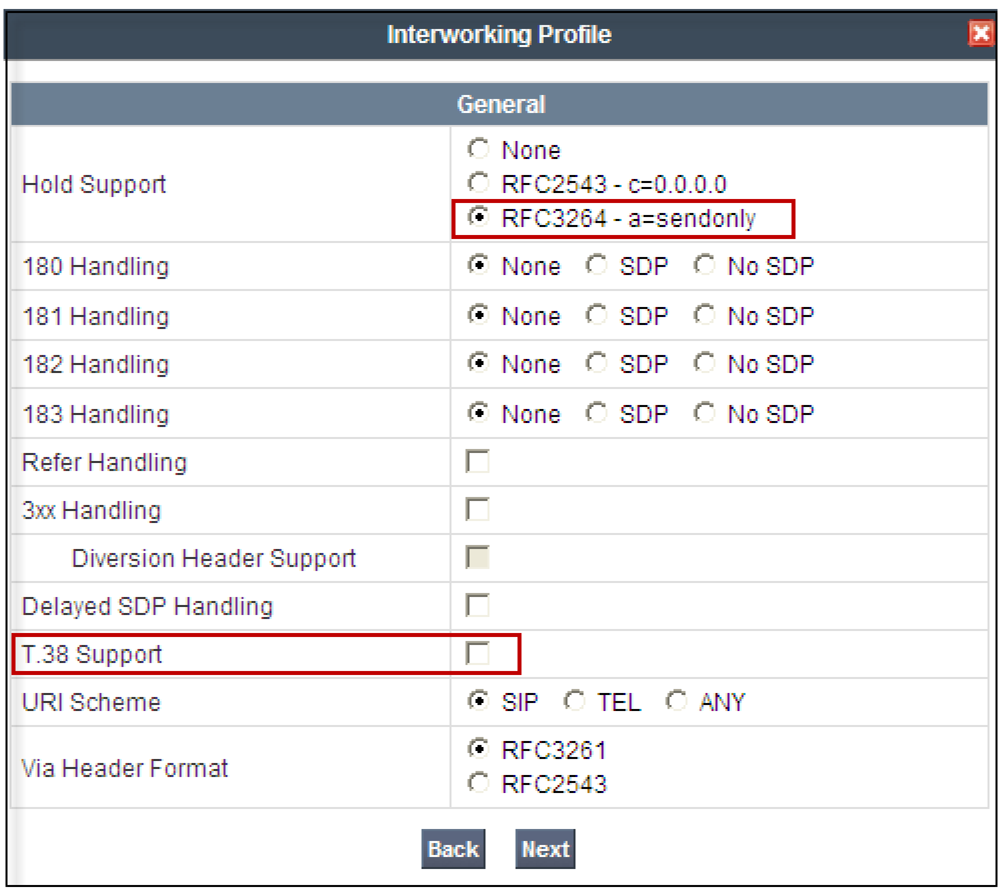
On the left navigation pane, select **Global Profiles → Server Interworking**. Click **Add Profile.**



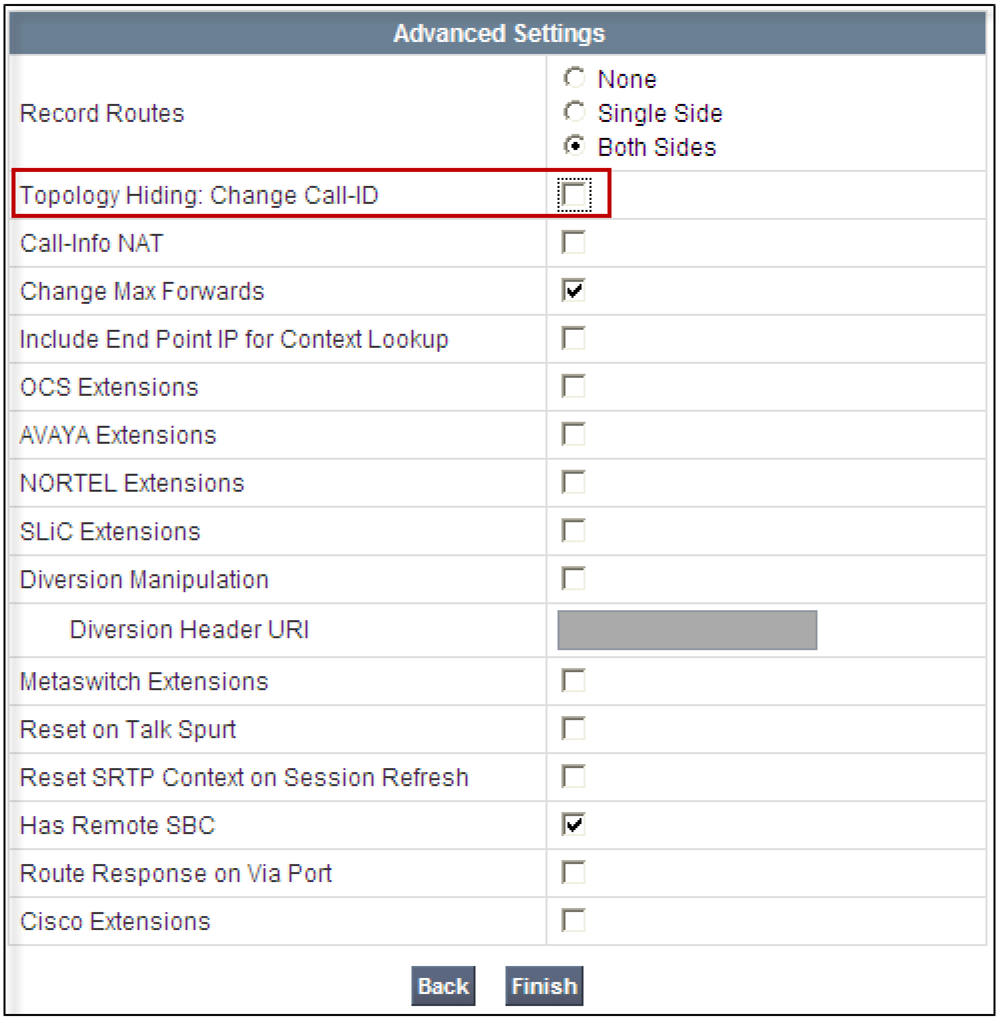
Enter a descriptive name for the new profile. Click **Next**.



On the **General** screen, under **Hold Support** check **RFC3264-a=sendonly**. Since T.38 is not to be used with this solution, leave the **T.38 Support box** unchecked. All other parameters retain their default values. Click **Next**.



Click **Next** on the **Privacy** and **Timers** tabs (not shown). On the **Advanced Settings** tab, uncheck the **Topology Hiding: Change Call-ID** box. Click **Finish** to save and exit.



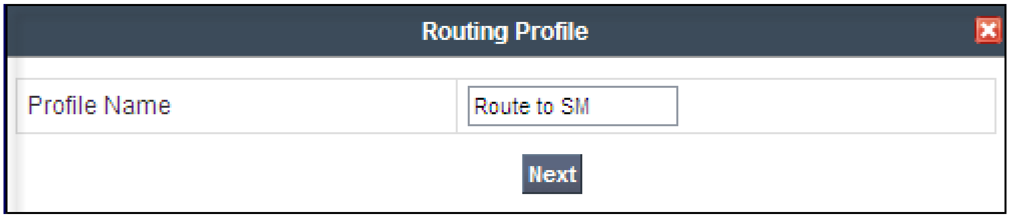
7.3.2. Routing Profiles

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces.

Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the Axtel SIP trunk.

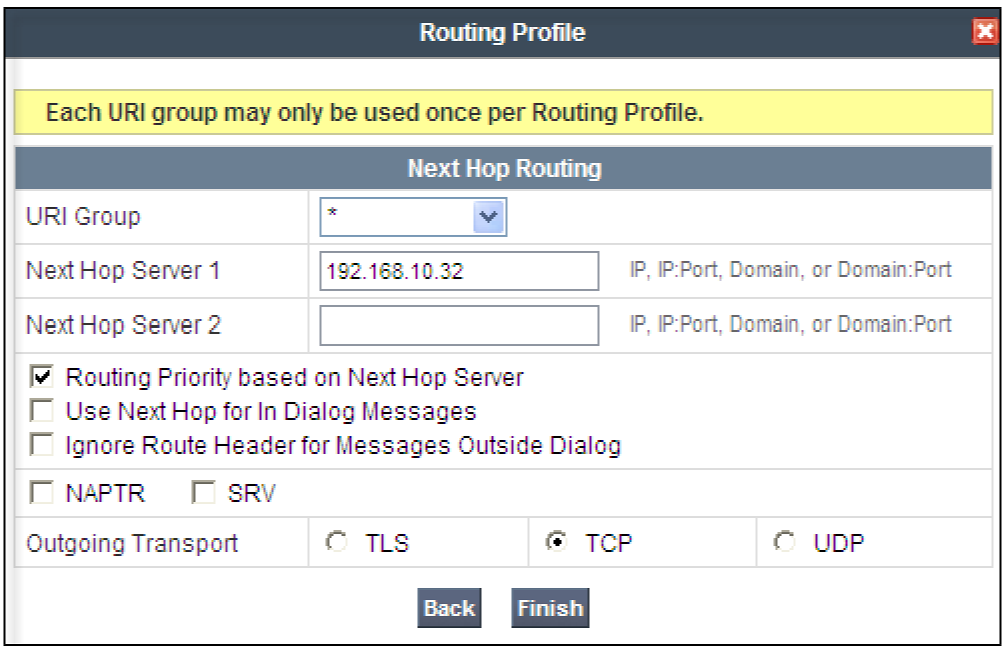
To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side. Select **Add Profile** (not shown).

Enter Profile Name: **Route to SM.** Click **Next.**



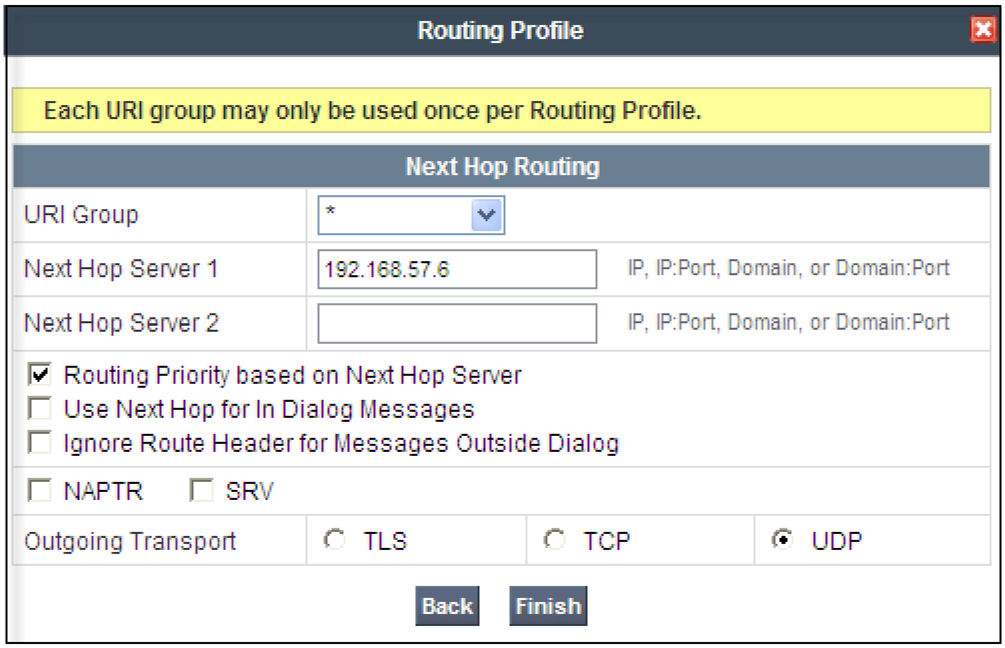
On the next screen, complete the following:

- Set the **URI Group** to the wild card ***** to match on any URI
- **Next Hop Server 1: 192.168.10.32** (Session Manager IP address)
- Check **Routing Priority Based on Next Hop Server**
- **Outgoing Transport: TCP**
- Click **Finish**



Back at the **Routing** tab, repeat the process to create the outbound route:

- Select **Add Profile**
- Enter Profile Name: **Route to SP**
- Click **Next**
- Set the **URI Group** to the wild card * to match on any URI
- **Next Hop Server 1: 192.168.57.6** (service provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server**
- **Outgoing Transport: UDP**
- Click **Finish**



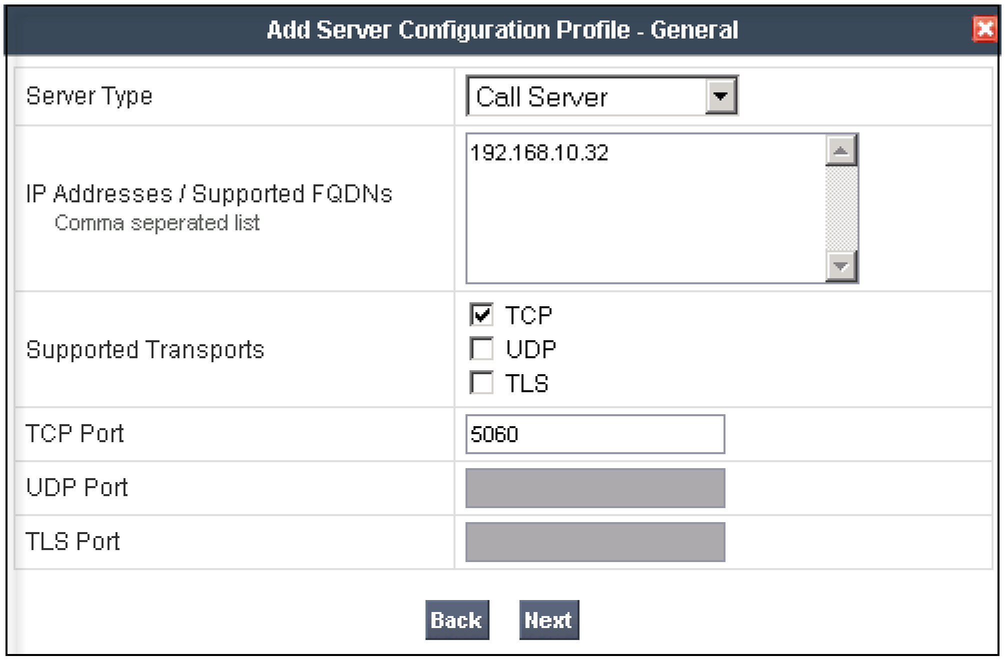
7.3.3. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE two peers: the Call Server (Session Manager) and the Trunk Server or SIP Proxy at the service provider's network. During the compliance test, the Trunk Server profile was configured to provide the registration and authentication parameters for the SIP trunk, as required by Axtel.

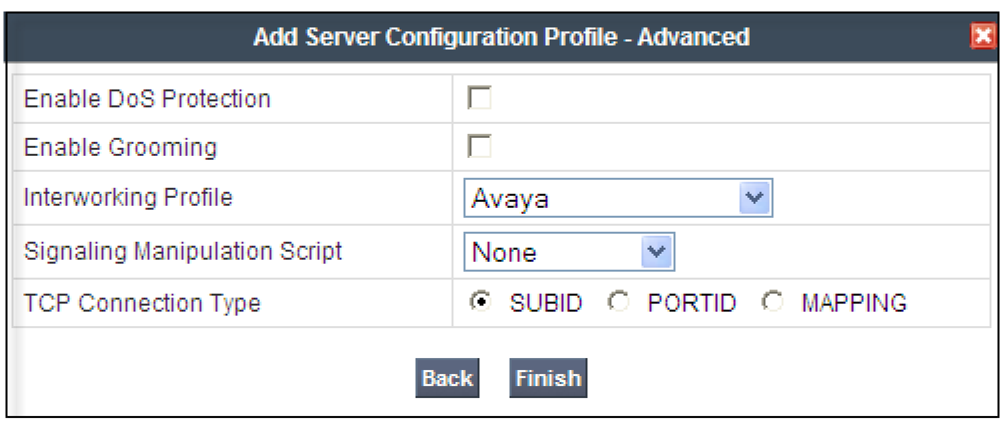
To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add Profile** and enter the profile name. **Session Manager** was the profile name used in the sample configuration.

On the **Add Server Configuration Profile, General** Tab:

- **Server Type:** Select **Call Server**
- **IP Address: 192.168.10.32** (IP Address of Session Manager Security Module)
- **Supported Transports**: Check **TCP**
- **TCP Port: 5060.** Click **Next**.



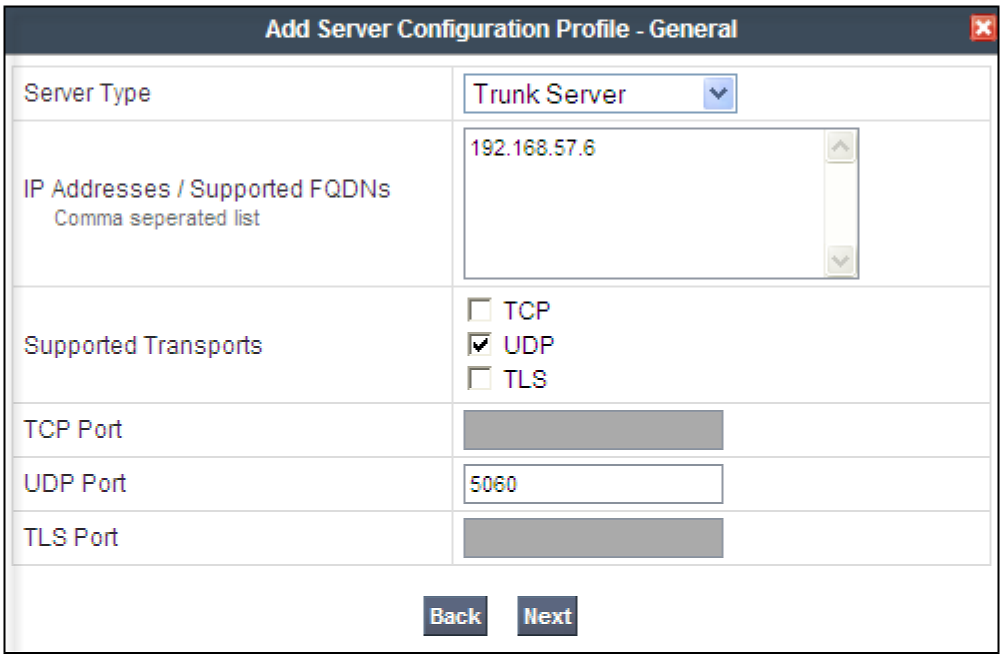
- Click **Next** on the **Authentication** tab
- Click **Next** on the **Heartbeat** tab
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu
- Click **Finish**



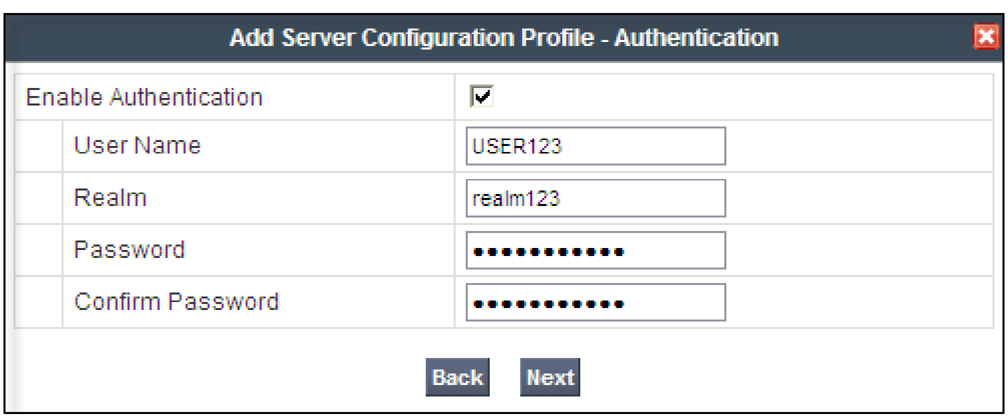
To add the profile for the Trunk Server, on the **Server Configuration** screen, click **Add Profile** and enter the profile name. **Service Provider** was the profile name used in the sample configuration.

On the **Add Server Configuration Profile, General** Tab:

- **Server Type:** Select **Trunk Server**
- **IP Address: 192.168.57.6** (service provider's SIP Proxy IP address)
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060.** Click **Next**

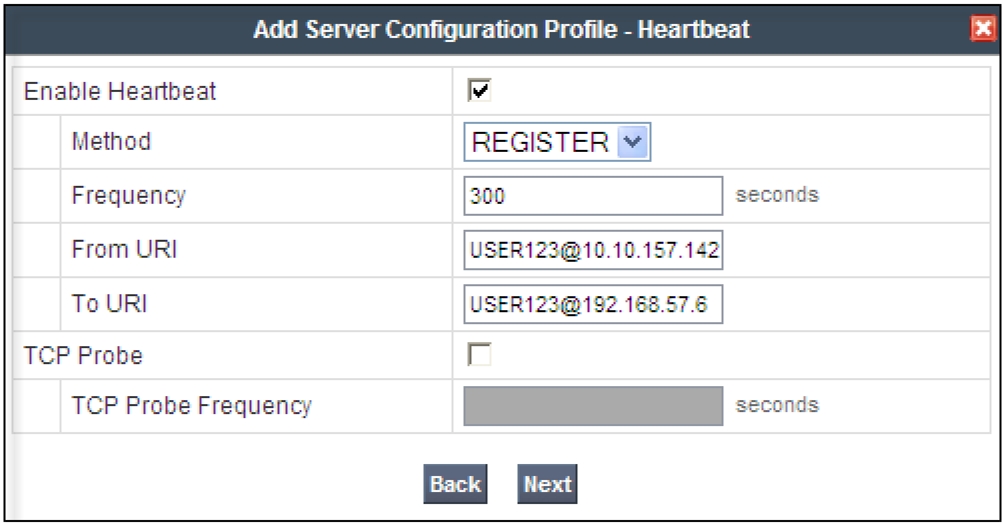


On the **Authentication** tab, check the **Enable Authentication** box. Enter the **User Name**, **Realm** and **Password** credential information supplied by the service provider for the authentication of the SIP trunk. Click **Next**.



On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency:** Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Axtel proxy server in order to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **300** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the **User Name** entered in the **Authentication** screen, and the external IP addresses of the Avaya SBCE (From URI) and the proxy server at Axtel (To URI) **,** like shown on the screen below.
- Click **Next**.



On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave other fields with their default values. Click **Finish.**

7.3.4. Topology Hiding

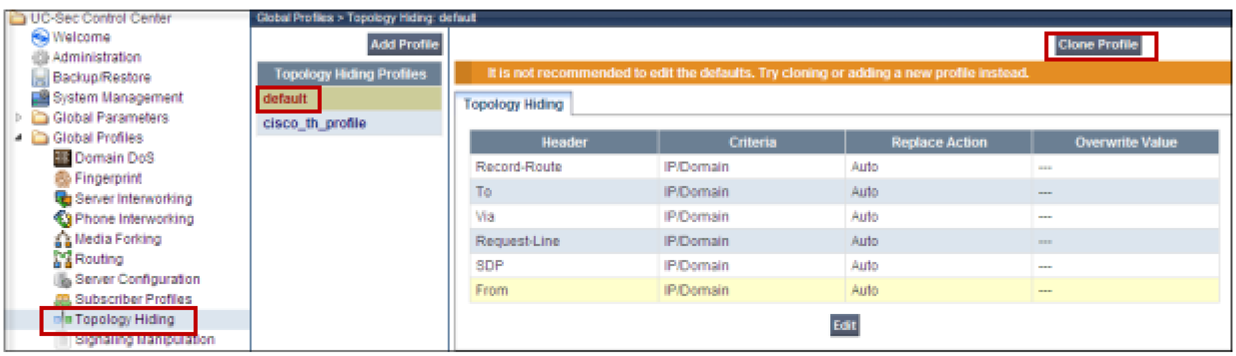
Topology Hiding is a security feature which allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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.

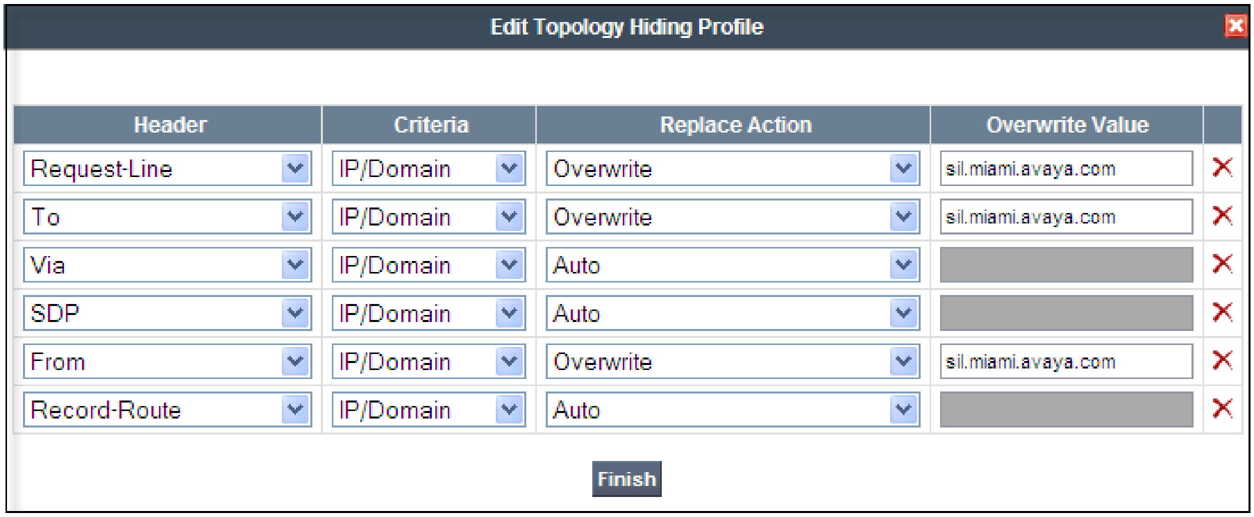
In the sample configuration, Topology Hiding Profiles were created in both the enterprise and service provider directions. They were configured to replace the host portion of the Request-Line, To and From headers with the domain expected by Session Manager and Axtel, respectively. In the examples below, the profiles were created by duplicating or "cloning" the default profile, and then making the required modifications.

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** column.



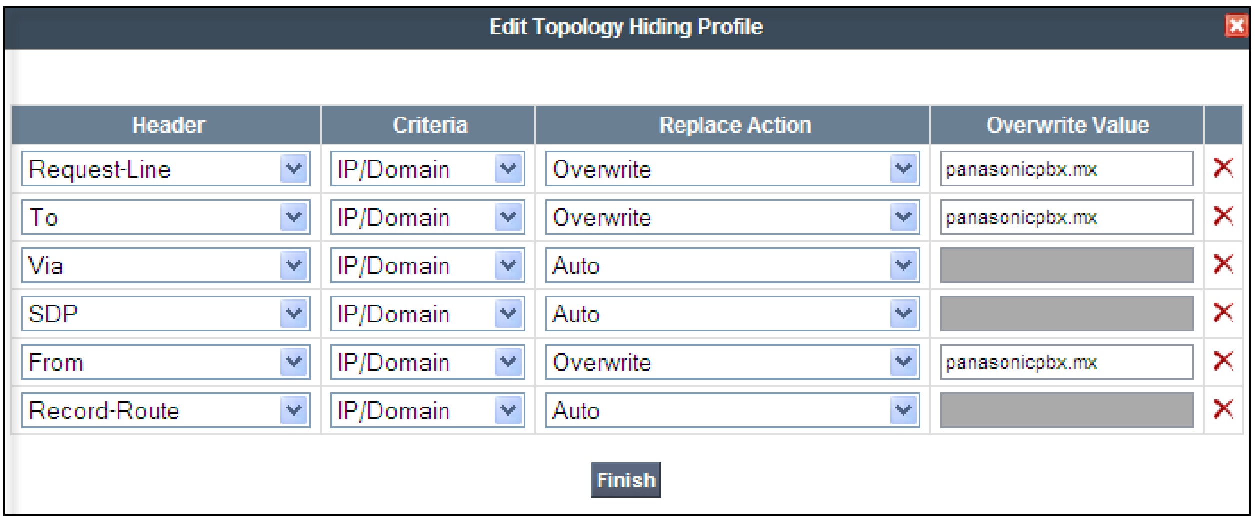
- Click **Clone Profile**
- Enter the **Profile Name**: **Session Manager** (not shown)
- Click **Finish**

- Click **Edit** on the **Topology Hiding** tab.
- For the **Request-Line, To** and **From** headers, select **Overwrite** in the **Replace Action** column.
- In the **Overwrite Value** column, enter **sil.miami.avaya.com**, the SIP domain of the enterprise.
- Click **Finish**



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

- Select **default** from the **Topology Hiding Profiles** column.
- Click **Clone Profile**.
- Enter the **Profile Name**: **Service Provider**. Click **Finish**.
- Click **Edit** on the **Topology Hiding** tab.
- For the **Request-Line, To** and **From** headers, select **Overwrite** in the **Replace Action** column.
- In the **Overwrite Value** column, enter **panasonicpbx.mx**, the Axtel SIP domain used for the compliance test.
- Click **Finish**



7.4. 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 to the enterprise.

7.4.1. Signaling Rules

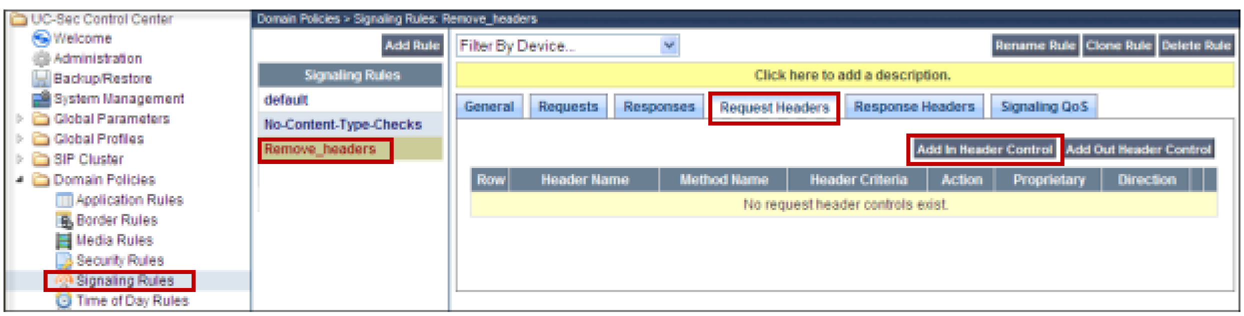
Signaling Rules define the actions to be taken (*Allow*, *Block*, *Block with Response*, etc.) for each type of SIP-specific signaling request and response message. They can also allow the control of the Quality of Service of the signaling packets.

A Signaling Rule was created in the sample configuration to remove (block) the Alert-Info, P-Location and P-Charging-Vector headers, which are sent in SIP messages from the Session Manager to the Avaya SBCE. They contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries.

In the **Domain Policies** menu on the left-hand side, select **Signaling Rules**, then **Add Rule**. Complete the entries in the pop-up windows (not shown).

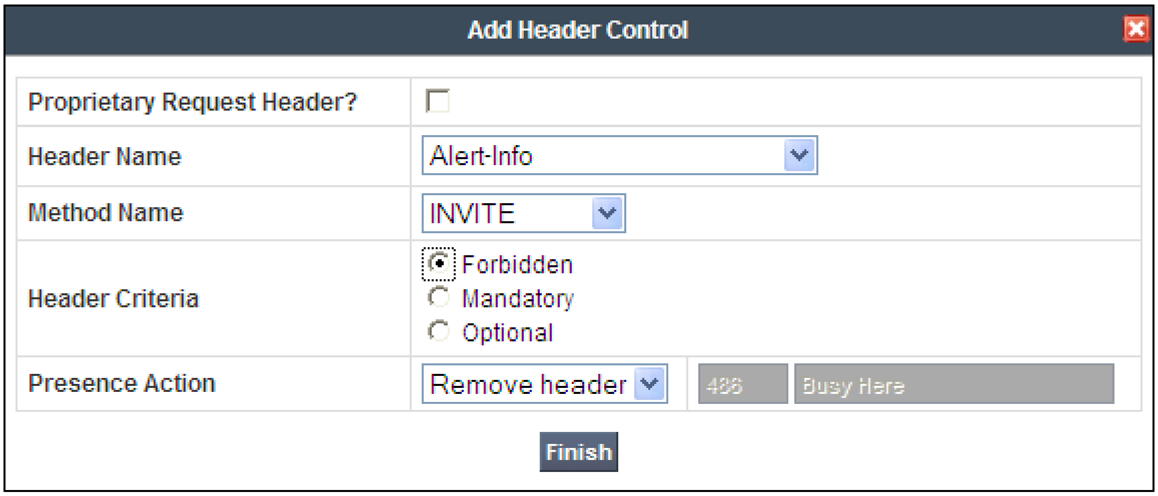
- Enter a name: **Remove_headers**. Click **Next**.
- On the next page, leave sections **Inbound**, **Outbound** and **Content-Type Policies** with their default values. Click **Next**.
- On the **Signaling QoS** tab**,** default values were used**.** Click **Finish**.

On the newly created Signaling Rule, select the **Request Headers** tab. Select **Add In Header Control**.

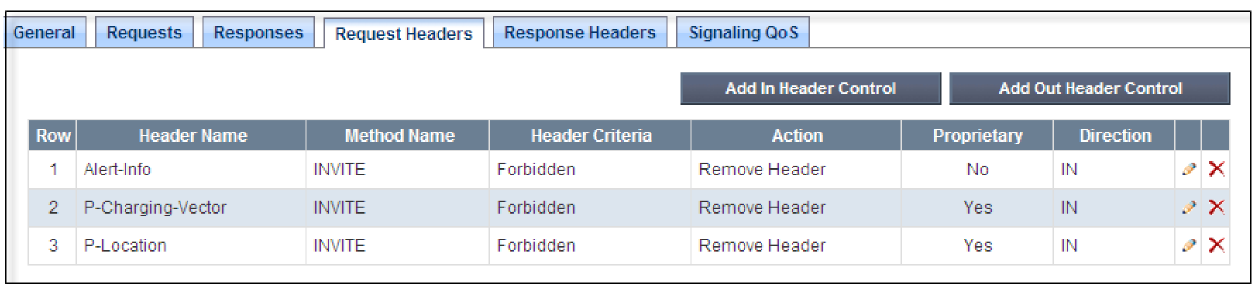


Enter the following:

- **Header Name: Alert-Info**
- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**



Similarly, configure the header control rules for the P-Location and P-Charging-Vector headers. For these two headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Request Headers** tab should look like the following screen:

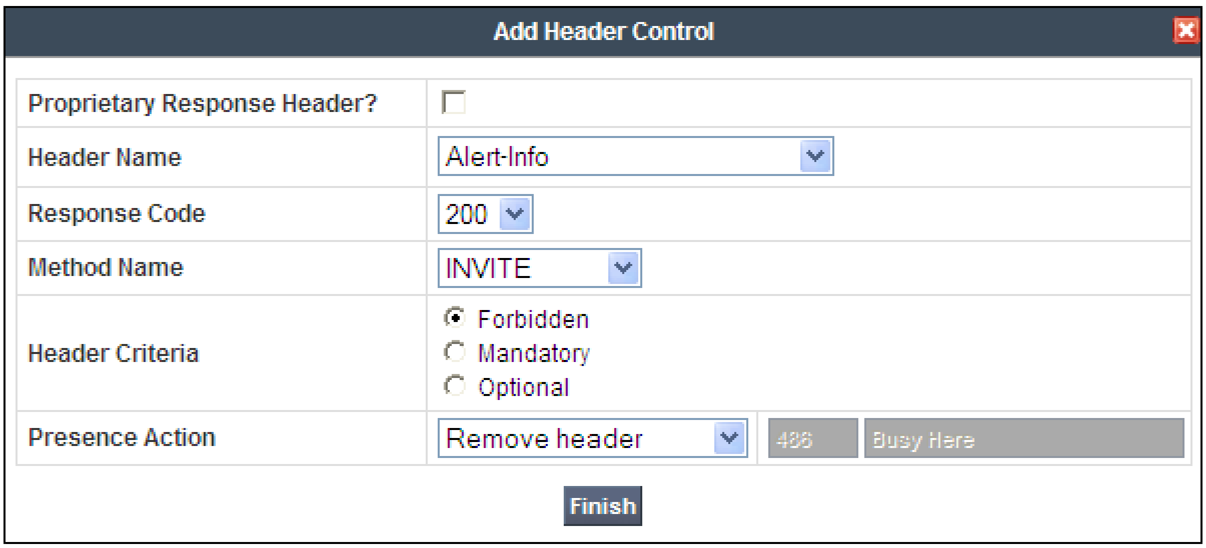


Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	INVITE	Forbidden	Remove Header	No	IN		
2	P-Charging-Vector	INVITE	Forbidden	Remove Header	Yes	IN		
3	P-Location	INVITE	Forbidden	Remove Header	Yes	IN		

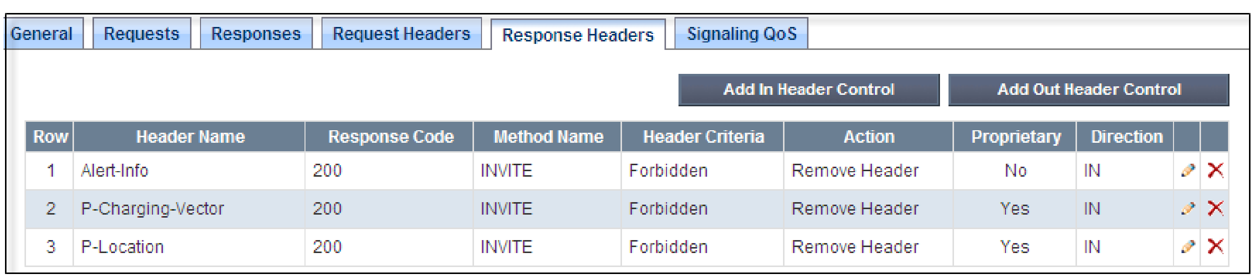
Select the **Response Headers** tab. Select **Add In Header Control** (not shown).

Enter the following:

- **Header Name: Alert-Info**
- **Response Code: 200**
- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**



Similarly, configure the header control rules for the P-Location and P-Charging-Vector headers. For these two headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. Once completed, the **Response Headers** tab should look like the screen below.



Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	200	INVITE	Forbidden	Remove Header	No	IN		
2	P-Charging-Vector	200	INVITE	Forbidden	Remove Header	Yes	IN		
3	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN		

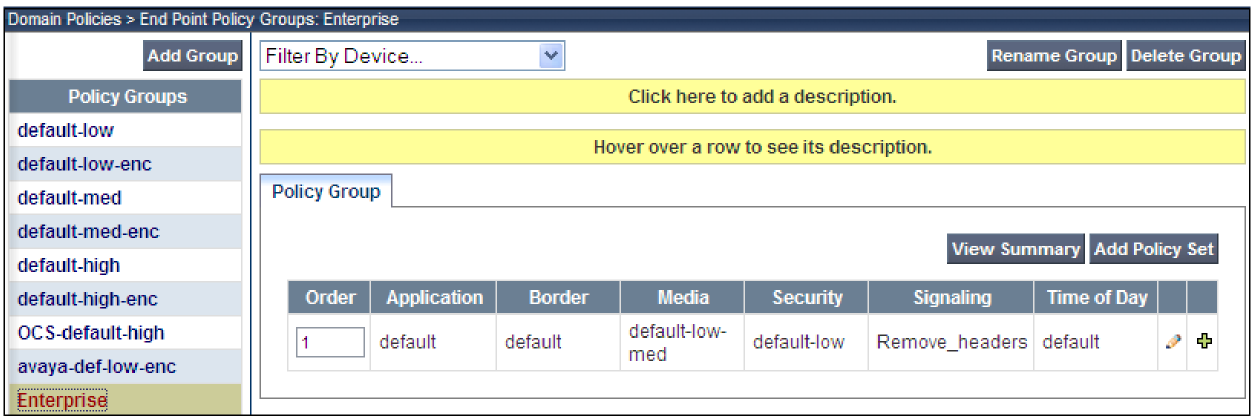
7.4.2. End Point Policy Groups

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.

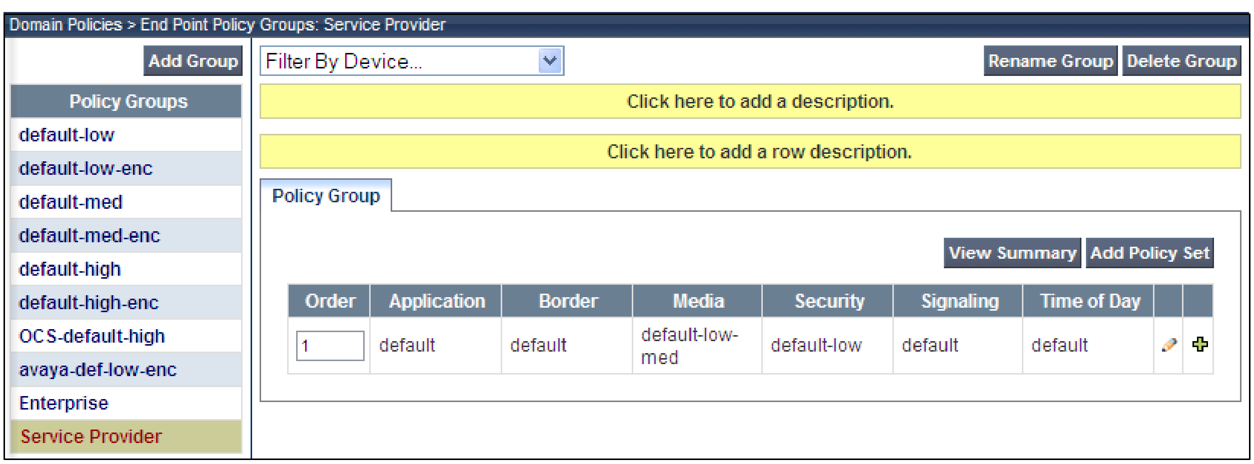
To create an End Point Policy Group for the enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add Group** (not shown).

- **Group Name: Enterprise**. Click **Next**
- **Signaling Rule:** Select **Remove_headers,** the signaling rule created on the previous section.
- Default values were used in all other fields. Click **Finish**

The screen below shows the **Enterprise** End Point Policy Group created.



For the compliance test, a second End Point Policy Group was created for the service provider. Default values were used for each of the rules which comprise this group. The screen below shows the **Service Provider** End Point Policy Group created.



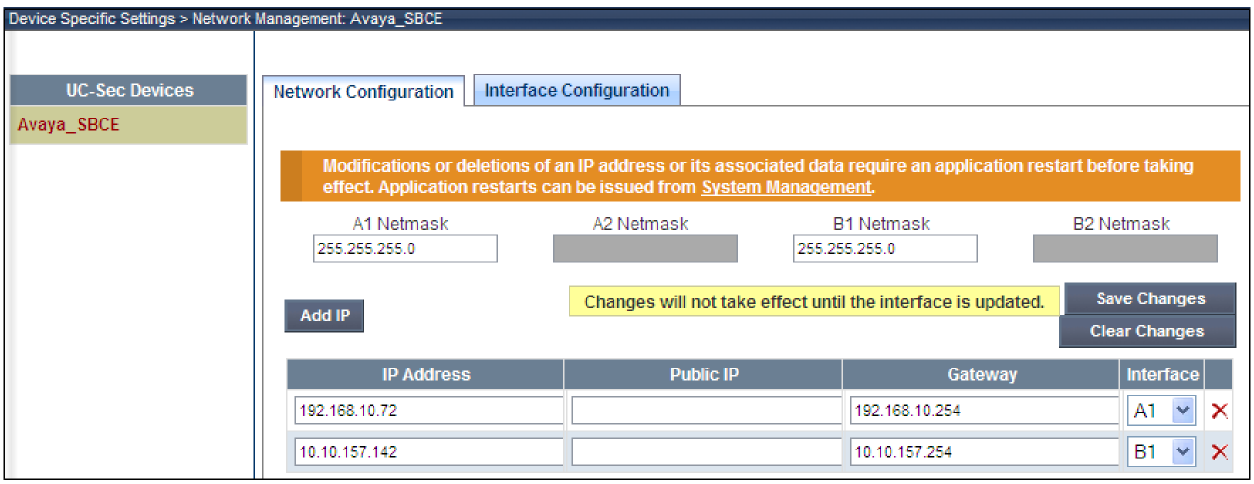
7.5. Device Specific Settings

The **Device Specific Settings** 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.

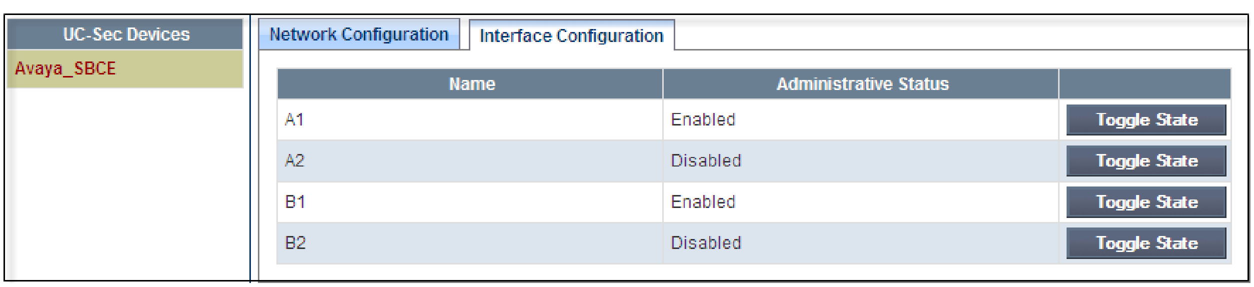
7.5.1. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **UC-Sec Devices**, select the device being managed, **Avaya_SBCE** in the sample configuration. Verify the network information previously assigned. Note that the **A1** interface is used for the internal side and **B1** is used for the external side of the Avaya SBCE.



On the **Interface Configuration** tab, click the **Toggle State** 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 very important to perform this step, or the SBC will not be able to communicate on any of its interfaces.



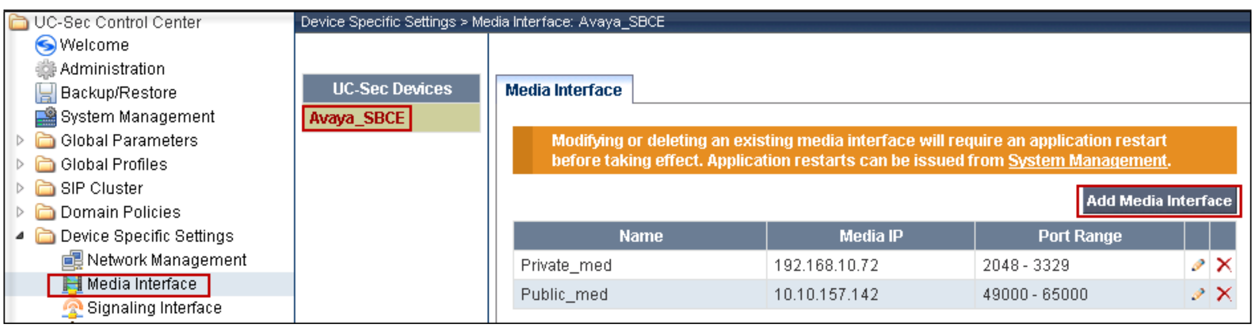
7.5.2. Media Interface

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address and one of the ports in this range as the listening IP address and port in which it will accept media from the Call or Trunk Server. The Private interface was made to match the range specified in the IP-Network-Region in Communication Manager of 2048 to 3349, and the Public interface was set to an arbitrary range of 49000 to 65000.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. In the center pane, select the **Avaya_SBCE** device.

- Select **Add Media Interface**
- **Name: Private_med**
- **IP Address: 192.168.10.72** (inside IP Address of the Avaya SBCE)
- **Port Range: 2048-3329**
- Click **Finish**
- Select **Add Media Interface**
- **Name: Public_med**
- **IP Address: 10.10.157.142** (outside IP Address of the SBC)
- **Port Range: 49000-65000**
- Click **Finish.**

The screen below shows the two Media Interfaces created in the sample configuration.



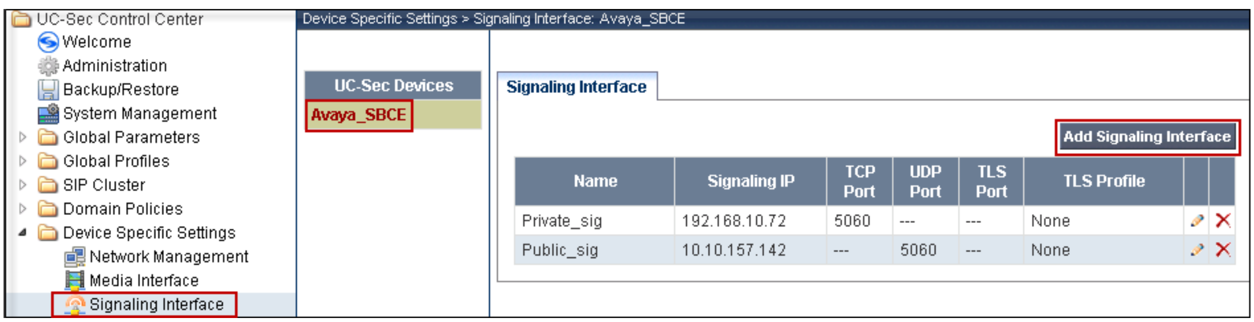
7.5.3. Signaling Interface

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in both the inside and outside networks.

From the **Device Specific Settings** menu on the left-hand side, select **Signaling Interface**. In the center pane, select the **Avaya_SBCE** device.

- Select **Add Signaling Interface**
- **Name: Private_sig**
- **IP Address: 192.168.10.72**
- **TCP Port: 5060**
- Click **Finish**
- Select **Add Signaling Interface**
- **Name: Public_sig**
- **IP Address: 10.10.157.142**
- **UDP Port: 5060**
- Click **Finish**

The screen below shows the two Signaling Interfaces created in the sample configuration.

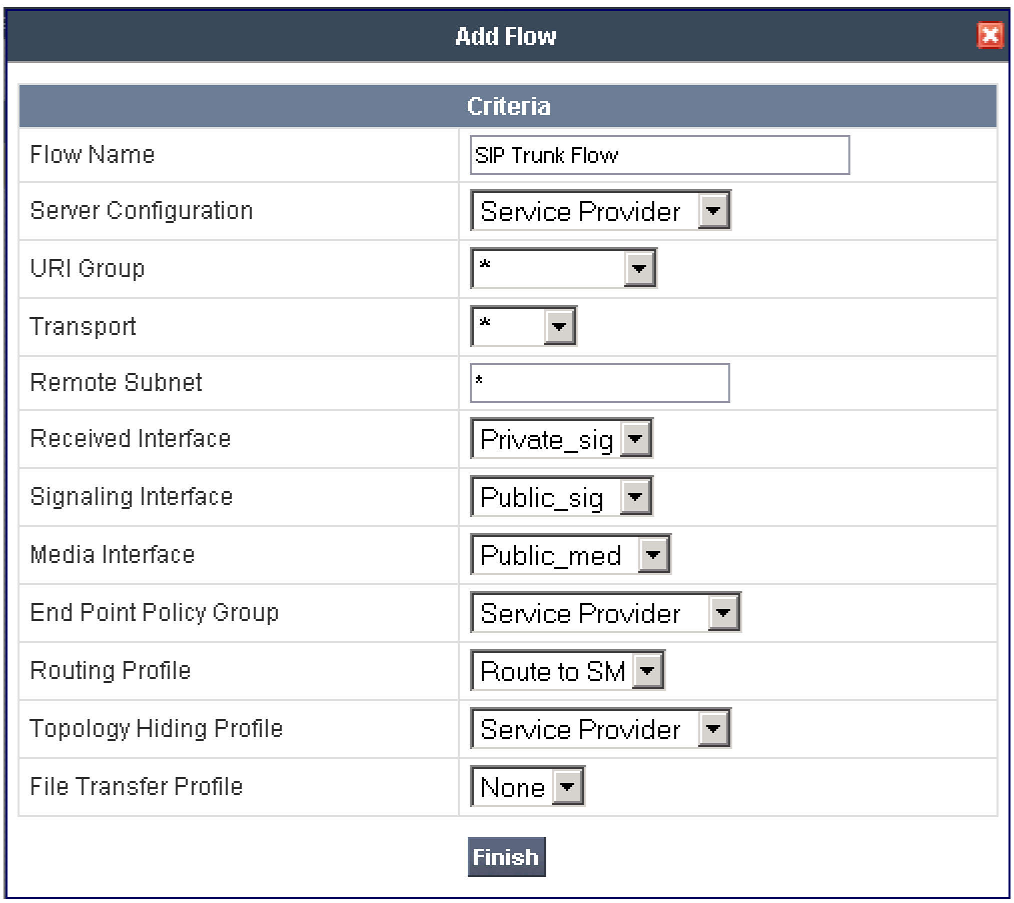


7.5.4. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

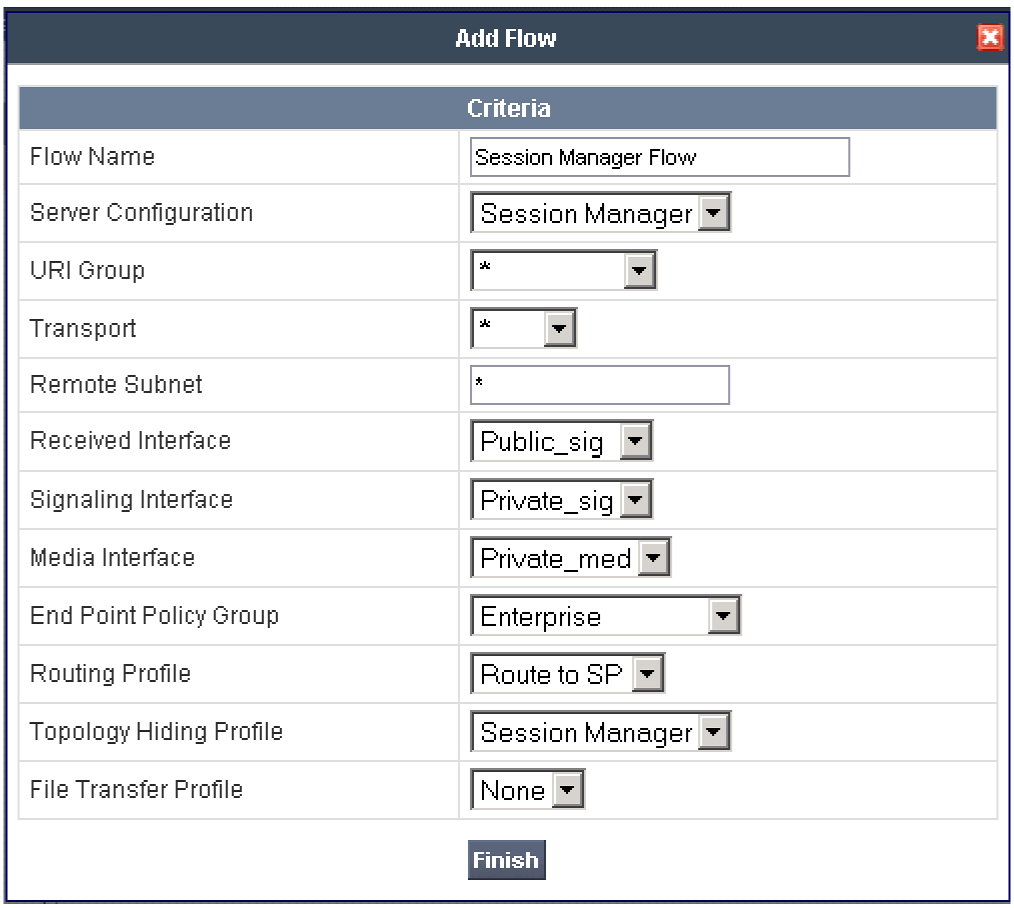
To create the call flow toward the Axtel SIP trunk, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add Flow**.

- **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.**

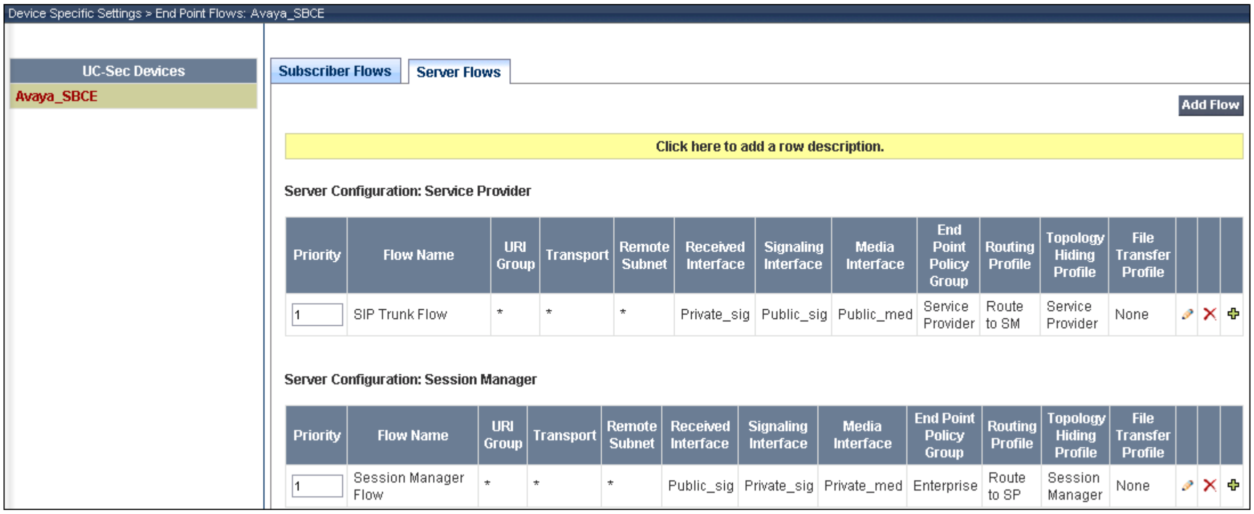


To create the call flow toward Session Manager, click **Add Flow**.

- **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 two Server Flows created in the sample configuration are summarized on the screen below:



8. Axtel SIP Trunking Service Configuration

Axtel is responsible for the configuration of the Axtel SIP Trunking Service in their network. To establish service, the customer will need to provide Axtel with the public IP address used to reach the Avaya SBCE at the enterprise. Axtel will provide the customer with the necessary information to configure the SIP connection from the enterprise site to the Axtel network, including:

- IP address of the Axtel SIP proxy.
- Credentials for SIP trunk registration (username, realm, password)
- Axtel SIP domain.
- Supported codecs.
- DID numbers
- Port numbers used for signaling and media.

This information is used to complete the configuration of Communication Manager, Session Manager and the Avaya SBCE discussed in the previous sections.

9. Verification and Troubleshooting

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

Verification Steps:

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

Troubleshooting:

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

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

3. 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, policies violations, etc.
   - **Diagnostics.** This screen provides a variety of tools to aid in troubleshooting the SBC network connectivity and its operation.

Other useful tools can also be found on the **Troubleshooting Menu,** on the left hand side of the UC-Sec Control Center page.

- **Packet Capture**. Allows to capture the packets in any of the SBC interfaces, and save them as *pcap* files. From the menu on the left hand side, click **Troubleshooting → Trace Settings → Packet Capture** tab.

10. Conclusion

Servicio Troncal SIP de Axtel is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises in Mexico. It provides businesses with a flexible, cost-saving alternative to traditional hardwired telephony trunks.

These Application Notes describe the configuration necessary to connect the service above to Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise R4.0.5.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the exception of the observations/limitations described in **Section 2.2.**

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.1, July 2012.

[2] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, July 2012, Document Number 03-300509.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.2, July 2012, Document Number 555-245-205.

[5] *Upgrading Avaya Aura® System Manager.* Release 6.2, July 2012, Document Number 03-603518

[6] *Implementing Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number 03-603473.

[7] *Administering Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number 03-603324.

[8] *Sipera Systems E-SBC 1U Installation Guide. Release 4.0.5.*November 2011.

[9] *Sipera Systems E-SBC Administration Guide. Release 4.0.5.* November 2011.

[10] *Administering Avaya one-X® Communicator,* October 2011.

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

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

[13] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, http://www.ietf.org/

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.