Avaya Solution & Interoperability Test Lab

Application Notes for Configuring TELUS SIP Trunking with Avaya Aura® Communication Manager Evolution Server 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller For Enterprise – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TELUS SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, Avaya Session Border Controller For Enterprise and various Avaya endpoints. TELUS is a member of the Avaya DevConnect Service Provider program.

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.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TELUS SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, Avaya Session Border Controller For Enterprise (Avaya SBCE) and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with TELUS SIP Trunking 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 ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the TELUS SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and Avaya SBCE.

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:

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator can place calls from the local computer or control a remote phone. Both of these modes were tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP.
- Inbound and outbound calls to/from TELUS Derived Voice endpoints
  Inbound and outbound calls to/from TELUS Mobility endpoints
- Various call types including: local, long distance, international, outbound toll-free, operator services and local directory assistance (411).

- Codecs G.711MU and G.729A
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- Voicemail Message Waiting Indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and enterprise mobility (extension to cellular)
- Network Call Redirection using the SIP REFER method

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested.
- Call redirection requested by a 302 response is not supported by TELUS.
- Establishment of a T.38 fax from a G.729 call could not be tested due to a limitation of the lab environment.

2.2. Test Results

Interoperability testing of TELUS SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **OPTIONS Max-Forwards Value**: TELUS requires that SIP OPTIONS messages sent from the enterprise contain a Max-Forwards value of zero. These messages originate from Session Manager with a non-zero Max-Forwards value when link monitoring is enabled. Thus, the Avaya SBCE was used to modify this value when the Avaya SBCE sent the OPTIONS message to the network. (See **Section 7.6.1)**
- **Use of SA8965**: TELUS requires re-INVITEs to contain Session Description Protocol (SDP) information. Thus, the Communication Manager special application SA8965 must be enabled on the service provider trunk and the internal enterprise trunk used for intra-site SIP traffic. (See **Section 5.2**) Even with SA8965 enabled, some call scenarios involving enterprise SIP endpoints still resulted in some re-INVITEs without SDP. These calls still completed with no impact to the user. These scenarios included inbound calls that were attended transferred back to the service provider by a SIP endpoint and conferencing of multiple PSTN calls by a SIP endpoint.
- **Codecs and Transcoding**: Depending on the codec settings on Communication Manager, some call scenarios that are redirected back to the service provider may result in one call leg using one codec and the second call leg using another. This situation would require the Avaya SBCE to perform transcoding between the two call legs which it currently does not support. As a result, these calls result in poor or no audio. To avoid this situation, the codec set configured on Communication Manager should use the same preferred codec and priority list recommended by TELUS (See **Section 5.5**). G.711MU is the preferred/default codec used by TELUS. G.729 is supported but is not available on all media gateways in the TELUS network.

- **Call Fowarding and EC500**: Inbound PSTN calls that are call forwarded back to the PSTN or ring to an EC500 (enterprise mobility) endpoint, will display the forwarding party/EC500 host at the destination instead of the original PSTN caller. This is the result of differences in the interpretation/implementation of the SIP Diversion header between TELUS and Communication Manager. A SIP header manipulation was created on the Avaya SBCE to modify the P-Asserted-ID header with information contained in the Diversion header. (See **Section 7.6.1)** This allows the call to complete but results in the incorrect calling party displayed at the destination as described above.
- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. Communication Manager provides the new connected party information by updating the Contact header in a re-INVITE message. TELUS does not use the updated Contact header for displaying calling party information.
- **Coverage to Voicemail for TELUS Mobility Users**: Calls from the enterprise to TELUS mobility users that cover to voicemail could result in one-way audio. If this occurs, the caller will not be able to hear the voicemail announcements and menus. A software change was made on Communication Manager to address this issue and was built on top of Release 6.0.1 Service Pack 7. The change was tested and passed compliance testing using an early development release. The change will be available in a future service pack release. Customers who encounter this problem should use the standard escalation process to request a patch from Avaya Global Services.
- **Use of REFER**: Enabling of the Network Call Redirection feature on the Communication Manager SIP trunk activates the use of the SIP REFER method for various inbound PSTN calls redirected back to the PSTN. The use of the REFER method resulted in dropped calls for blind transfer and vector redirection scenarios. Enabling of Network Call Redirection is not recommended.
- **T.38 Fax – Network Coverage**: Not all media gateways in the TELUS network support T.38 fax. Communication Manager does not support fallback to G.711 pass-through fax from T.38 fax. Thus, if a T.38 fax call encounters a media gateway in the TELUS network that does not support T.38 then the call will terminate.
- **Transitioning to T.38 for Outbound Calls**: In general, the answering side of a fax call will send a re-INVITE to transition to T.38. For outbound fax calls to the PSTN, this means the network would typically send the re-INVITE to transition to T.38. However, TELUS requires Communication Manager to transition to T.38 for both inbound and outbound fax calls. Relying on Communication Manager to transition to T.38 on an outbound call may have the following impact:
  - On an outbound call, sending of the T.38 INVITE happens on detection of the V.21 preamble of the originating fax machine's Digital Command Signal (DCS) message. This is part of the T.30 exchange. This request to transition to T.38 may happen too late for some terminating gateways to accommodate the switch to T.38.
  - If the initial call is using the G.729 codec, the compression of the V.21 preamble may cause its detection to be less reliable then if the call was initially using G.711.

- The ability to transition to T.38 in the middle of the T.30 exchange is supported on the following Avaya media platforms (G430/G450/TN2602). Older platforms (G350/G700/TN2302) may have different behavior.

  Compliance testing was conducted with the TN2602 media platform (part of the G650 media gateway) using codec G.711MU to initially establish the call. Outbound T.38 fax calls in this environment were successful.
- **G.711 Pass-through Fax**: Communication Manager does not support G.711 pass-through fax over SIP trunks. These calls are treated like any other voice call by Communication Manager. If a customer chooses to use G.711 pass-through fax, success is not guaranteed.
- **Avaya one-X® Communicator SIP and "Other Phone" Mode**: When Communication Manager places the call to the "Other Phone" on the PSTN, the call is rejected with a 500 Server Error from the TELUS network. It is rejected because the initial INVITE from Communication Manager includes a PAI header containing the enterprise extension instead of the DID number for that station. As a result, Avaya one-X@ Communicator SIP should not be used in "Other Phone" mode with this solution.

2.3. Support

For technical support on the TELUS system, please contact your TELUS Account Executive or visit http://telus.com.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Selecting the **Support Contact Options** link followed by **Maintenance Support** provides the worldwide support directory for Avaya Global Services. Specific numbers are provided for both customers and partners based on the specific type of support or consultation services needed. Some services may require specific Avaya service support agreements. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to TELUS SIP Trunking. This is the configuration used for compliance testing.

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

- Avaya S8300D Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya 1600-Series IP Telephones (H.323)
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya A175 Desktop Video Device
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Avaya SBCE. The Avaya SBCE has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.

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

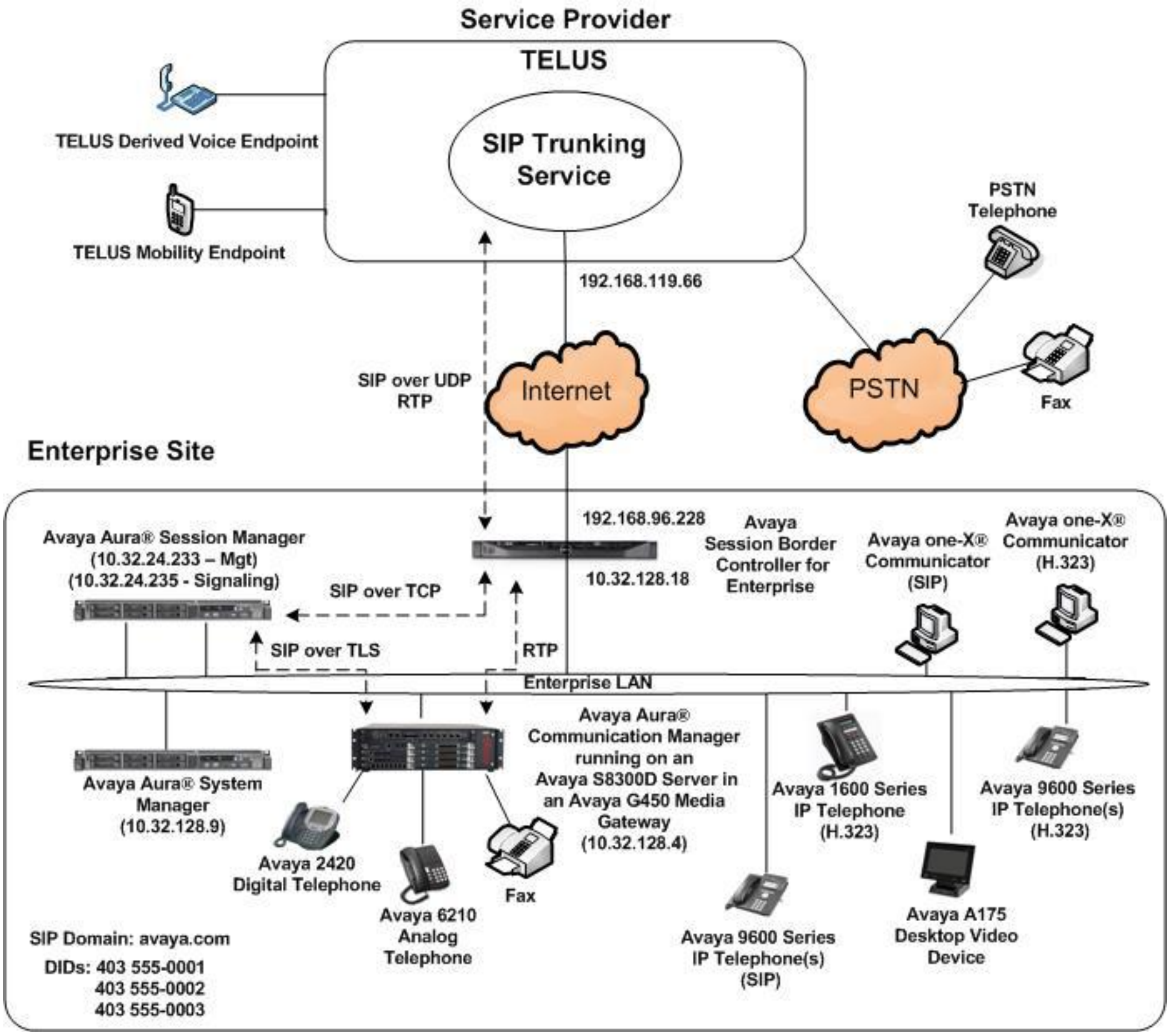


Figure 1: Avaya IP Telephony Network using TELUS SIP Trunking

For inbound calls, the calls flow from the service provider 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 are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the Avaya SBCE. From the Avaya SBCE, the call is sent to TELUS SIP Trunking.

For the compliance test, the enterprise sent 11 digits in the destination headers (e.g., Request-URI and To) and sent 10 digits in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). TELUS sent 10 digits in both the source and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on an Avaya S8300D Server	6.0.1 SP7 + development patch (R016x.00.1.510.1-19686) (System Platform 6.0.3.6.3)
Avaya G450 Media Gateway	31.20.0
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.1 SP5 (Build 6.1.5.0.615006)
Avaya Aura® System Manager running on an Avaya S8800 Server	6.1 SP5 (Build 6.1.0.0.7345-6.1.5.502; SW Update Revision 6.1.6.1.1087) (System Platform 6.0.3.03)
Avaya Session Border Controller For Enterprise	4.0.5Q09
Avaya 1608 IP Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.3 SP1
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1 SP4 (3.1.04S)
Avaya 9630 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6 SP6 (2.6.6)
Avaya 9611 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 6.0 SP3 (6.0.3)
Avaya A175 Desktop Video Device with Avaya Flare® Experience	1.1
Avaya one-X® Communicator (H.323 or SIP)	6.1 SP3 Patch 3 (Build 6.1.3.09-SP3-Patch3-35953)
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
TELUS SIP Trunking Solution Components	
Equipment/Software	Release/Version
Acme Packet 4520 Net-Net Session Border Controller	6.1m7p5
Nokia Siemens Networks HiQ 4200	Version 14.0

Table 1: Equipment and Software Tested

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 TELUS SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from TELUS. It is assumed 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. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 SIP trunks are available and 25 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  36
           Maximum Concurrently Registered IP Stations: 2400  3
             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  0
                       Maximum Administered SIP Trunks: 4000  25
  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    0
           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
```

5.2. Special Application SA8965

TELUS requires that all INVITE messages contain SDP information, including re-INVITEs. In general, when Communication Manager sends a re-INVITE to perform a media shuffling operation (redirect media directly between two endpoints) the re-INVITE will not include SDP information. In order to change this behavior, special application SA8965 must be enabled. This is done via the **change system-parameters special-applications** command. Navigate to **Page 7** and enter a **y** next to the special application titled **SA8965 - SIP Shuffling with SDP** in the list below. By enabling this feature, a new protocol variation parameter will appear on **Page 3** of the trunk form (See **Section 5.8**).

```
change system-parameters special-applications                     Page   7 of   9
                             SPECIAL APPLICATIONS

                       (SA8888) - Per Station Music On Hold? n
     (SA8889) - Verizon VoiceGenie SIP MIME Message Bodies? n
                  (SA8891) - Verizon VoiceGenie SIP Headers? n
                                (SA8893) - Blast Conference? n
                       (SA8896) - IP Softphone Lamp Control? n
                  (SA8900) - Support for NTT Call Screening? n
               (SA8904) - Location Based Call Type Analysis? n
                   (SA8911) - Expanded Public Unknown Table? n
       (SA8917) - LSP Redirect using special coverage point? n
                          (SA8927) - Increase Paging Groups? n
     (SA8928) - Display Names on Bridged Appearance Labels? n
             (SA8931) - Send IE with EC500 Extension Number? n
           (SA8942) - Multiple Unicode Message File Support? n
           (SA8944) - Multiple Logins for Single IP Address? n
                             (SA8946) - Site Data Expansion? n
  (SA8958) - Increase BSR Polling/Interflow Pairs to 40000? n
                          (SA8965) - SIP Shuffling with SDP? y
  (SA8967) - Mask CLI and Station Name for QSIG/ISDN Calls? y
```

5.3. 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
```

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:

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.4. 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 (**sessionMgr**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
cmm                 10.32.128.4
default             0.0.0.0
procr               10.32.128.4
procr6              ::
sessionMgr          10.32.24.235
```

5.5. 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. The list should include the codecs and preferred order defined by TELUS. G.711MU is the preferred/default codec used by TELUS. Thus, G.711MU should be entered as the first entry in the list. Additional codecs are optional. For the compliance test, ip-codec-set 3 was used. Part of the testing was done with G.711MU only as shown below and part was done with a codec list of G.711MU and G.729A. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. 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.711MU          n          2        20
 2:
 3:
```

On **Page 2**, to enable T.38 fax, set the **Fax Mode** to **t.38-standard**. Otherwise, set the **Fax Mode** to **off**.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
```

5.6. 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 3 was chosen for the service provider trunk. 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 **avaya.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 5.5**.
- 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: avaya.com
    Name: SP Region
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. 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 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 3 will automatically create a complementary table entry on the IP network region 1 form for destination region 3. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).

```
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
```

5.7. 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 **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, part of 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.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and can not be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a 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 5.4**.
- Set the **Far-end Node Name** to **sessionMgr**. This node name maps to the IP address of Session Manager as defined in **Section 5.4**.
- 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 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a

SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.8**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5062**.

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**.
- 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 SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **15**. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

```
add signaling-group 3                                               Page   1 of   1
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                  Far-end Node Name: sessionMgr
 Near-end Listen Port: 5062                 Far-end Listen Port: 5062
                                         Far-end Network Region: 3

Far-end Domain: avaya.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? n                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 15
```

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**. 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 **Member Assignment Method** to **auto**.
- 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.

```
add trunk-group 3                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 3                   Group Type: sip           CDR Reports: y
  Group Name: SP Trunk                   COR: 1        TN: 1        TAC: 1003
   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: 5
```

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.7**.

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 **900** seconds was used.

```
add trunk-group 3                                               Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 15000

            SCCAN? n                                Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900

                                     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 (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. To remove the + sign, 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 5.3**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 3                                               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 the **Network Call Redirection** field to **n**. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been re-directed. These settings are needed by TELUS to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**, the value preferred by TELUS.

Set the **Shuffling with SDP** field to **y**. This will instruct Communication Manager to send SDP information in shuffling re-INVITEs on calls that use this trunk. This parameter only appears if special application SA8965 is enabled. See **Section 5.2** for full details.

```
add 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? n
                      Send Diversion Header? y
                    Support Request History? n
               Telephone Event Payload Type: 101
                         Shuffling with SDP? y

          Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
```

Calls between the enterprise SIP endpoints and TELUS traverse two SIP trunks: the internal SIP trunk for intra-enterprise traffic (trunk 1 in the test configuration) and the service provider SIP trunk to TELUS (trunk 3 described above). In order for SA8965 to be properly applied to these calls, **Shuffling with SDP** must also be enabled on the internal SIP trunk used for SIP endpoints in addition to the trunk to TELUS shown above. Use the **change trunk-group** command to enable **Shuffling with SDP** on the internal enterprise SIP trunk 1 as shown below.

```
change trunk-group 1                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                        Mark Users as Phone? n
              Prepend '+' to Calling Number? n
        Send Transferring Party Information? n
                   Network Call Redirection? n
                      Send Diversion Header? y
                    Support Request History? n
               Telephone Event Payload Type:
                         Shuffling with SDP? y

          Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
```

5.9. 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 5.8**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 40003, 40005 and 40015. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change private-numbering 0                                        Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private       Total
Len Code             Grp(s)     Prefix         Len
                                                     Total Administered: 4
 5  4                                          5        Maximum Entries: 240
 5  40003           3         4035550001      10
 5  40005           3         4035550002      10
 5  40015           3         4035550003      10
```

In a real customer environment, normally the DID number is 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 5-digit extension beginning with 4 will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 0                                        Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private       Total
Len Code             Grp(s)     Prefix         Len
                                                     Total Administered: 1
 5  4               3         40355            10      Maximum Entries: 240
```

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   dac
   4           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

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:
                       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: *01    All: *02    Deactivation: *03
```

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 0                                                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
    0                    1    1      2        op            n
    0                    11   11     2        op            n
    011                  10   18     2        intl          n
    1800                 11   11     2        fpna          n
    1877                 11   11     2        fpna          n
    1908                 11   11     2        fpna          n
    411                  3    3      2        svcl          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 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 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.
- **Pfx Mrk**: **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers.
- **Numbering Format**: **unk-unk** All 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 5.8**.
- **LAR**: **next**

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2   Pattern Name: SP route
                             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       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
```

6. Configure Avaya Aura® Session Manager

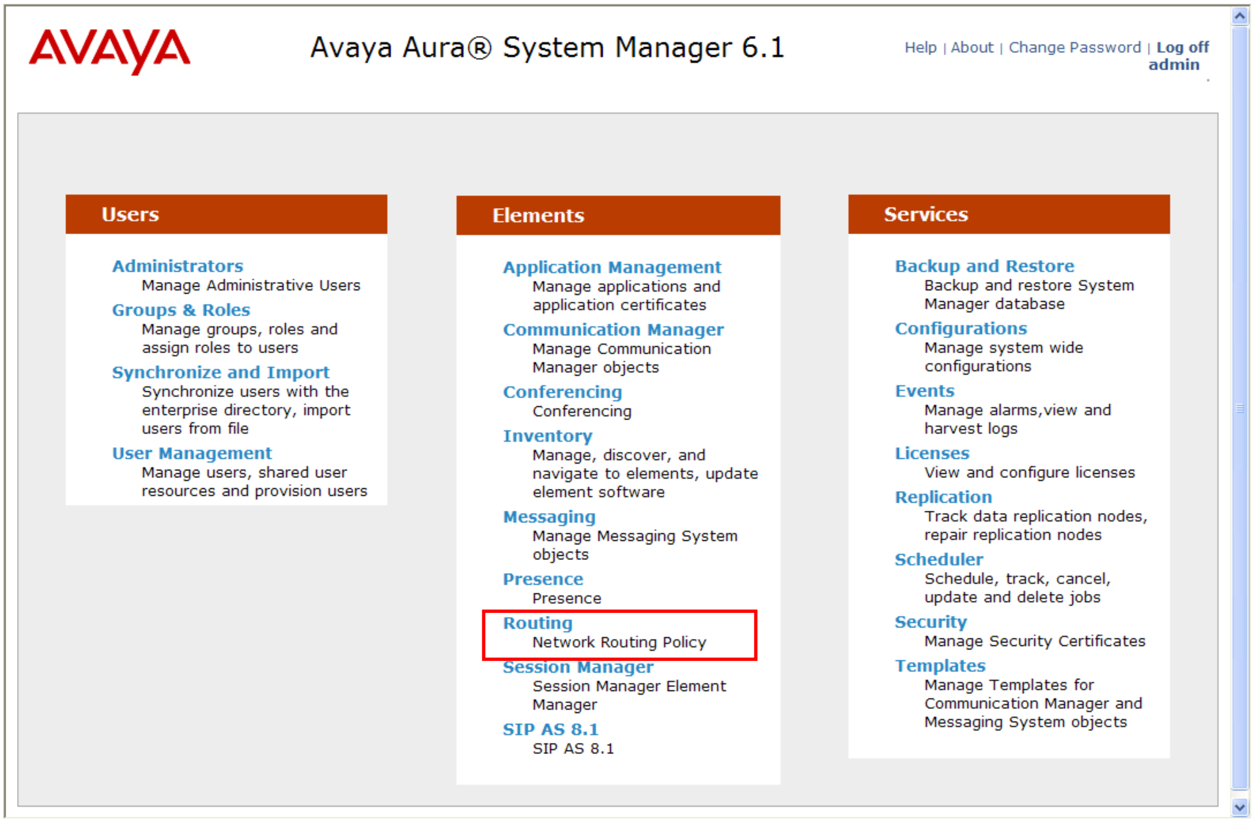
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- 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 governs which Routing Policy is used to service a call.
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

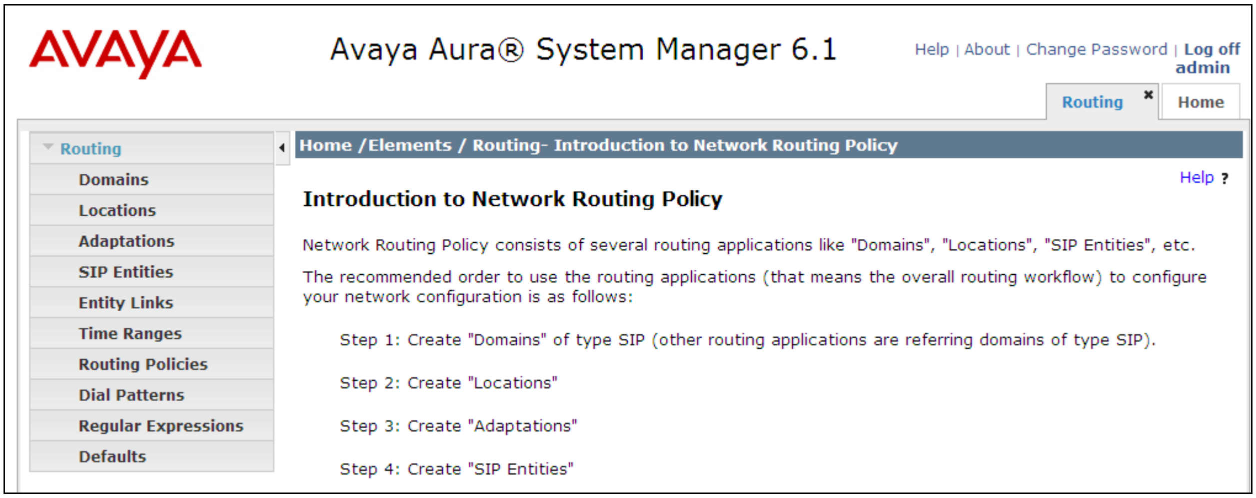
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Avaya Aura® 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 **Login** (not shown). The **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements → Routing** link highlighted below.



Clicking the **Elements → Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.

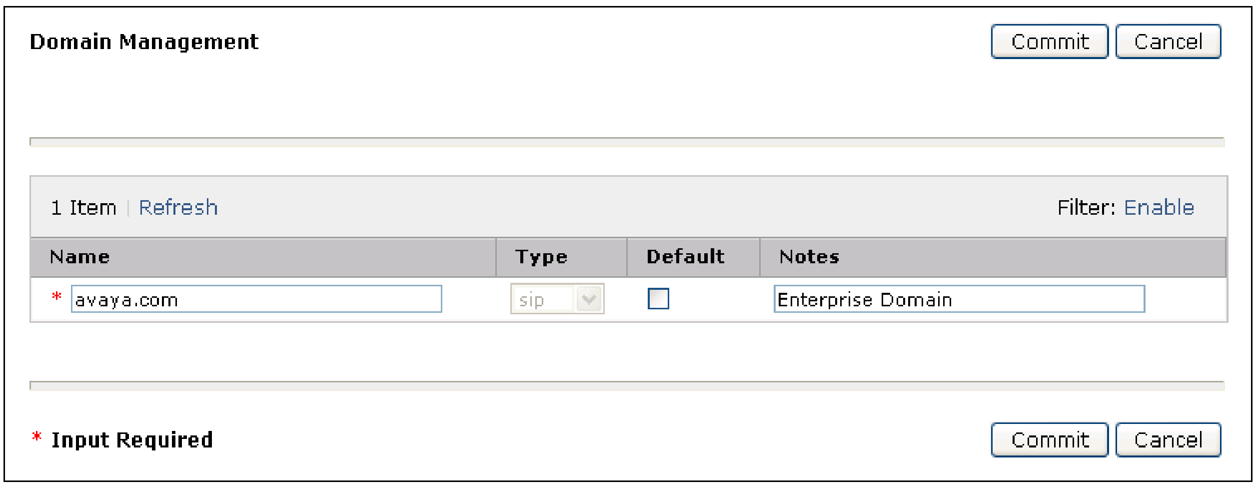


6.2. Specify SIP Domain

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 includes the enterprise domain (**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.



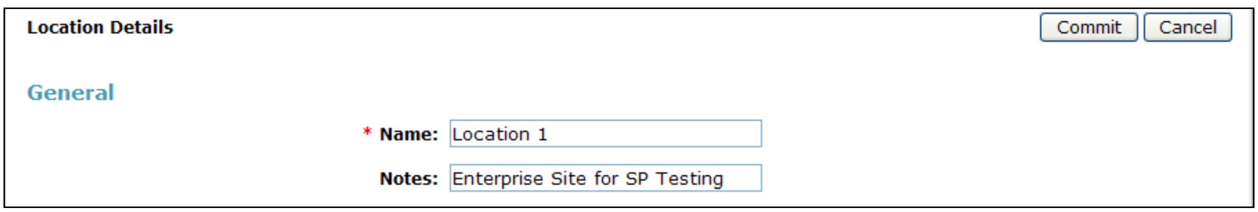
6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the location named **Location 1**, which includes all equipment on the enterprise including Communication Manager, Session Manager and the Avaya SBCE.

To add a location, navigate to **Routing →Locations** 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:

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

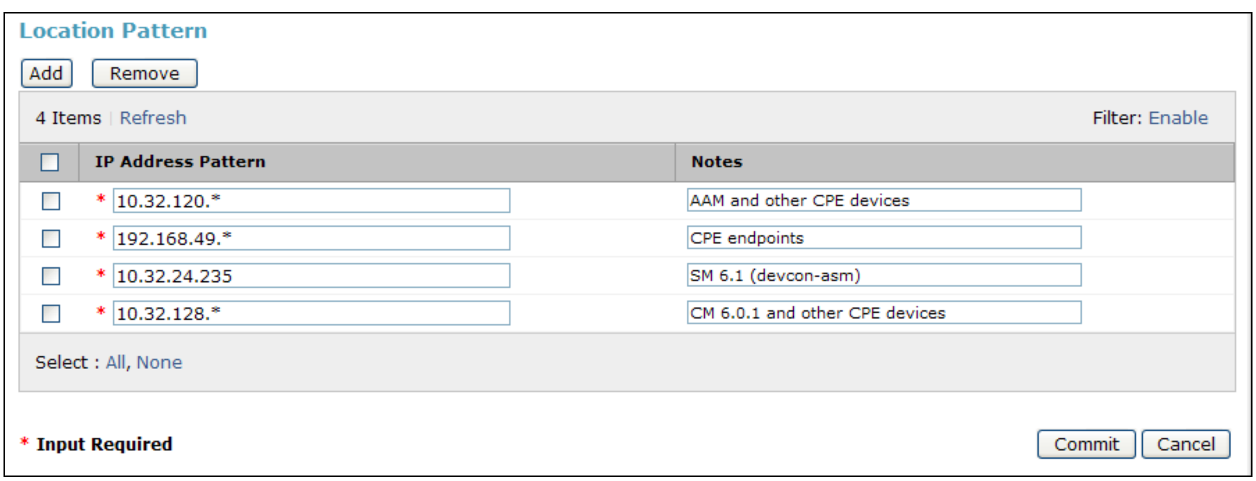
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).



Scroll down to 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).

Click **Commit** to save.



6.4. Add Adaptation Module

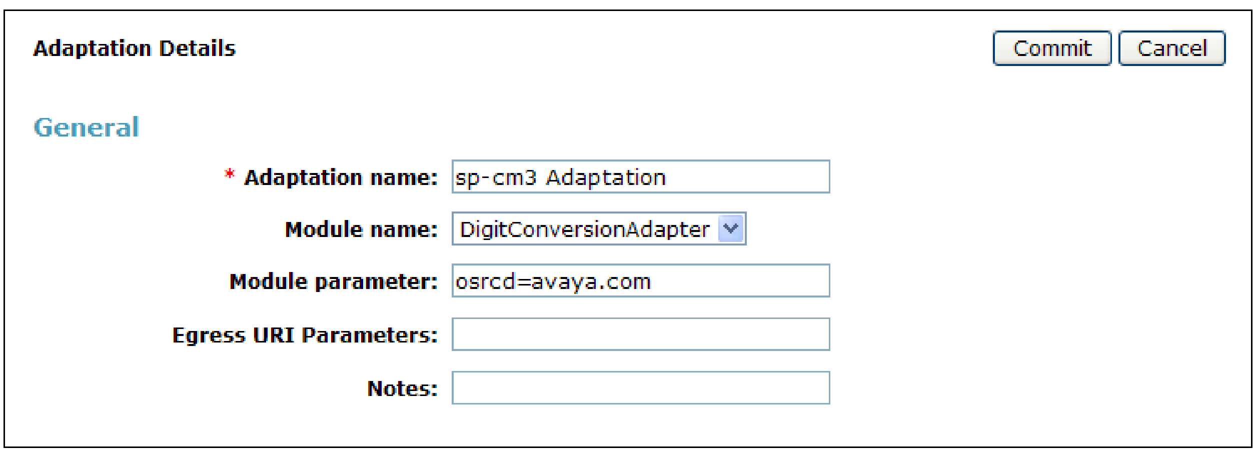
Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products.

For the compliance test, an adaptation was applied to the Communication Manager SIP entity and converted the domain part of the inbound PAI header to the enterprise domain (**avaya.com**). In addition, this adaptation mapped inbound DID numbers from TELUS to local Communication Manager extensions.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

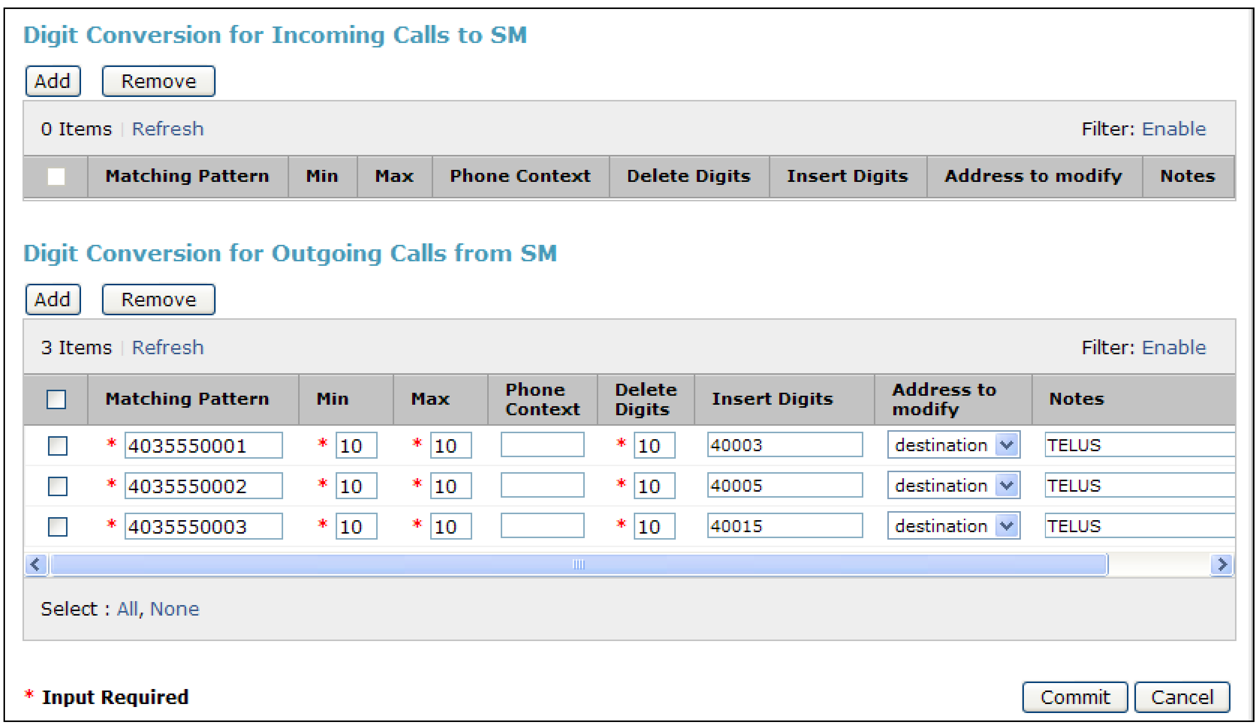
- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter **DigitConversionAdapter**.
- **Module parameter:** Enter **osrcd=avaya.com**. This is the OverrideSourceDomain parameter. This parameter replaces the domain in the inbound PAI header with the given value. This parameter must match the value used for the **Far-end Domain** setting on the Communication Manager signaling group form in **Section 5.7**.



To map inbound DID numbers from TELUS to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select **destination** since this digit conversion only applies to the destination number.

Click **Commit** to save.



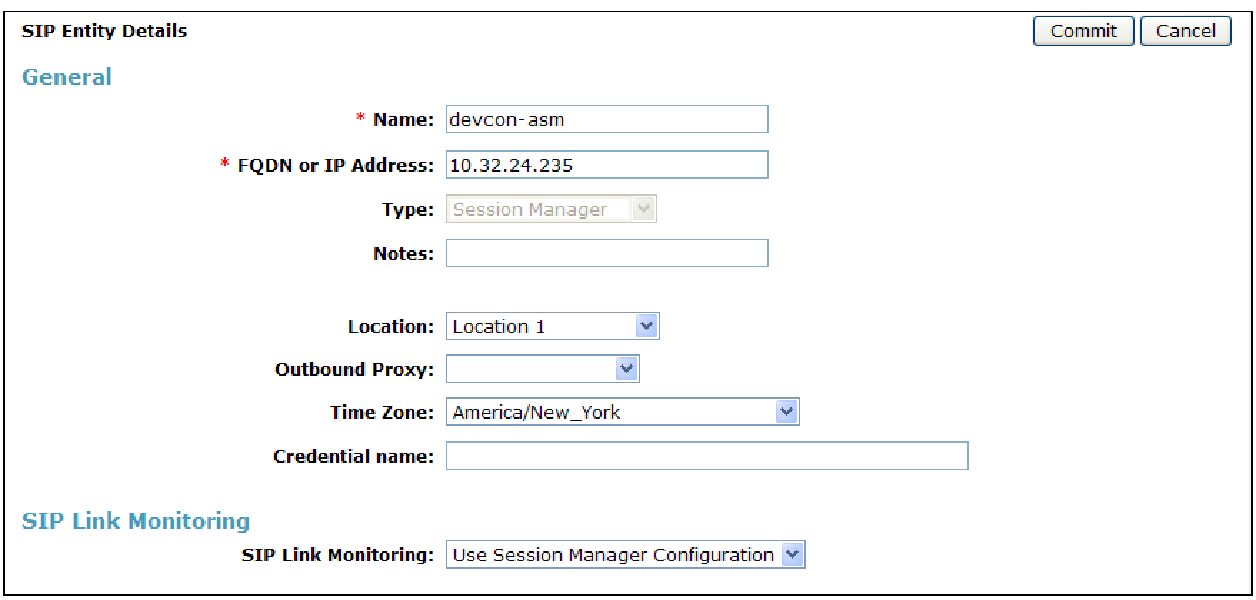
6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation name** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all components were located in location **Location 1**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.



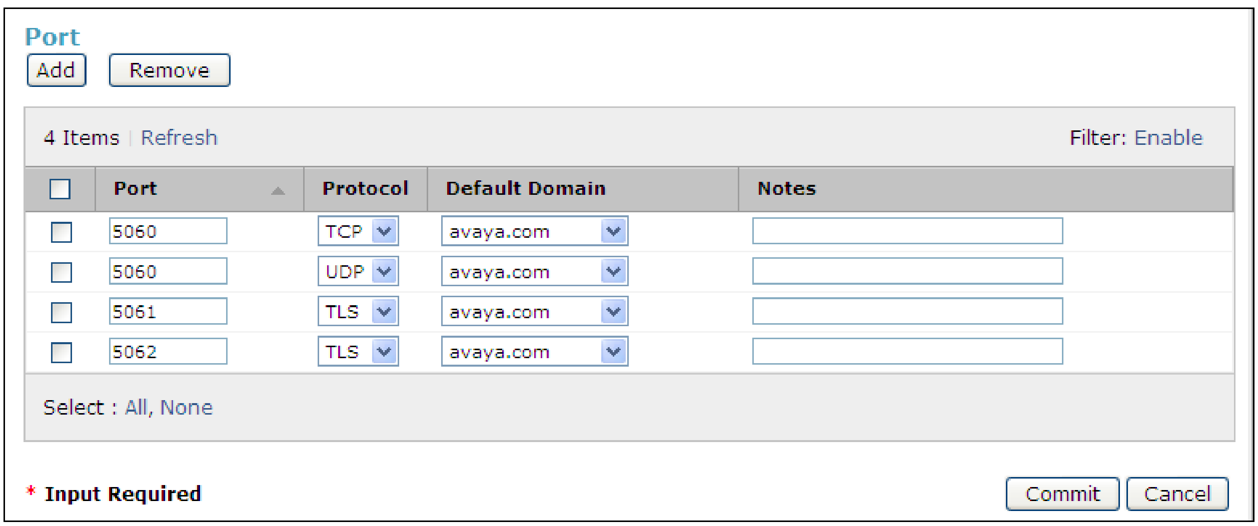
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

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

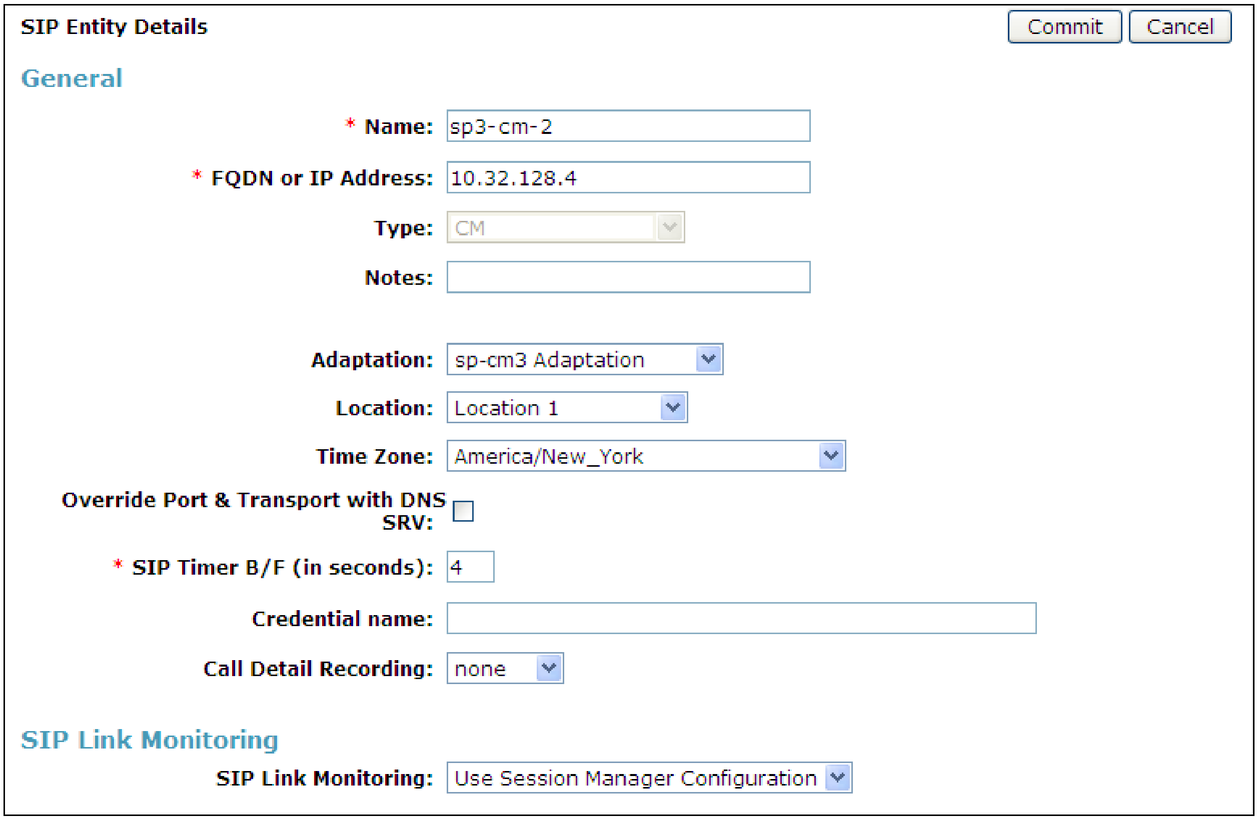
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.

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

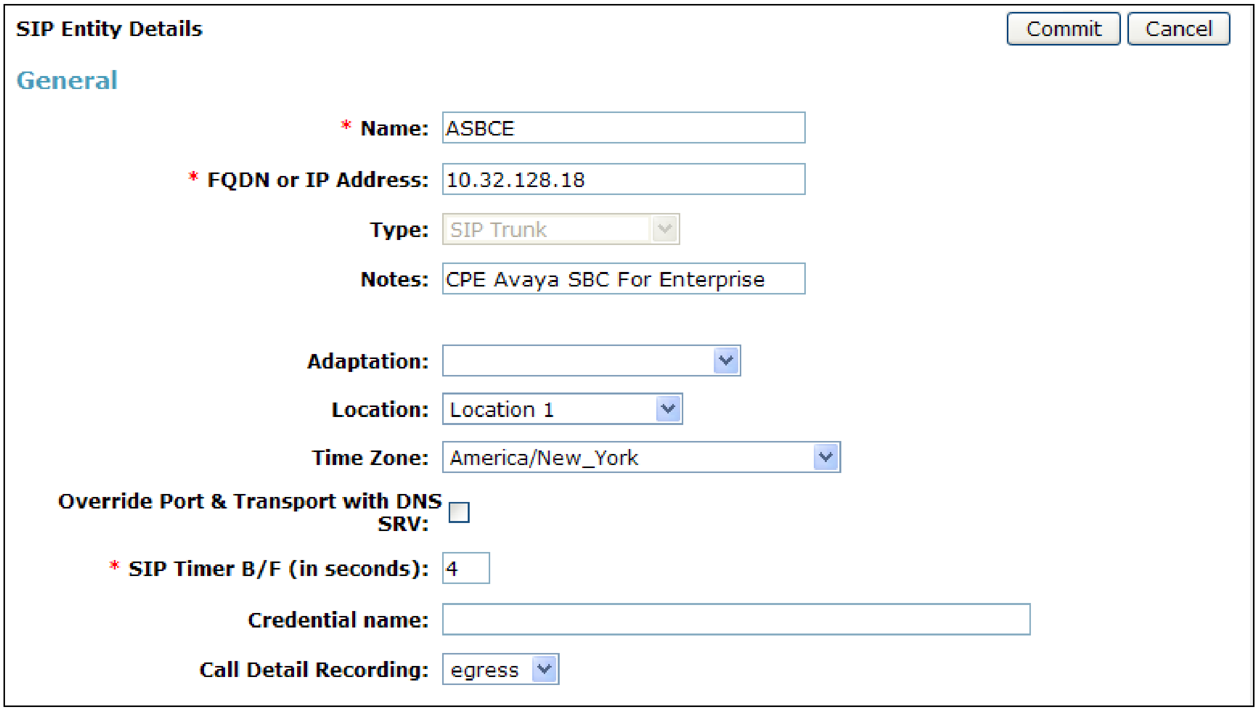
For the compliance test, four port entries were used. The first three are the standard ports used for SIP traffic: port 5060 for UDP/TCP and port 5061 for TLS. In addition, port 5062 defined in **Section 5.7** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.



The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, this requires the creation of a separate SIP entity for Communication Manager other than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the Avaya Server running Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 6.4**. The **Location** field is set to **Location 1** which is the location defined for the subnet where Communication Manager resides.



The following screen shows the addition of the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The **Location** field is set to **Location 1** which is the location defined for the subnet where the Avaya SBCE resides.

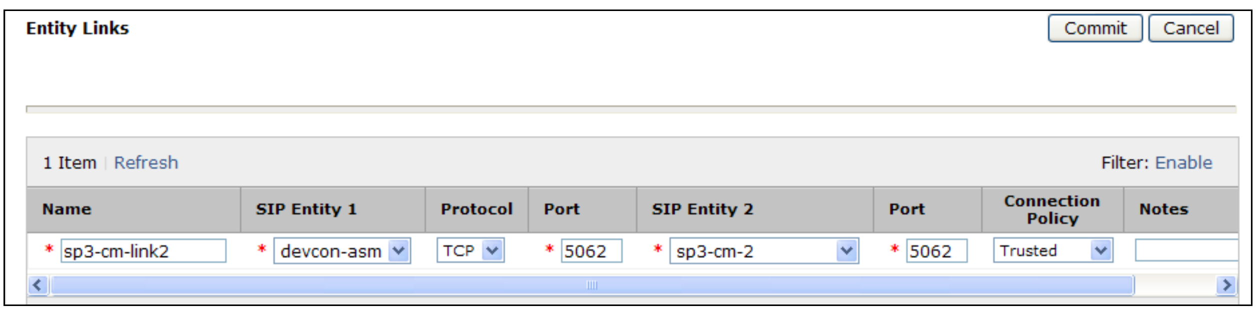


6.6. Add Entity Links

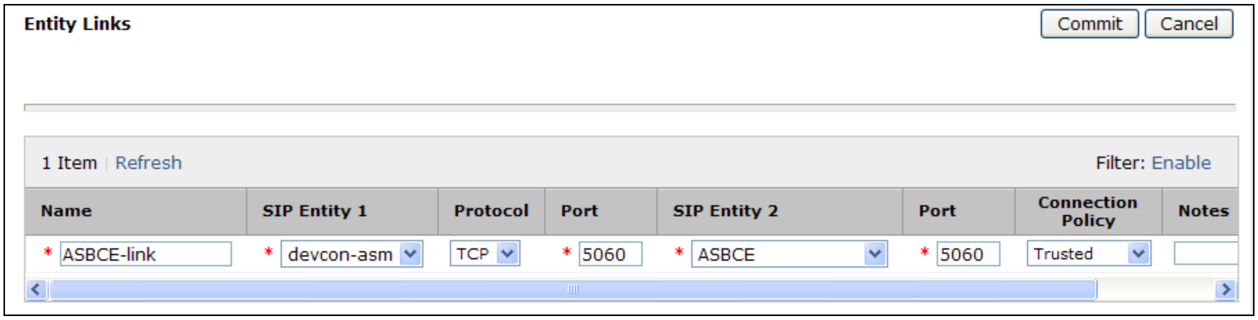
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **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 the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **Connection Policy:** Select **Trusted** from pull-down menu.

Click **Commit** to save. The following screen illustrates 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 5.7**.



The following screen illustrates the Entity Link to the Avaya SBCE.



6.7. Add Routing Policies

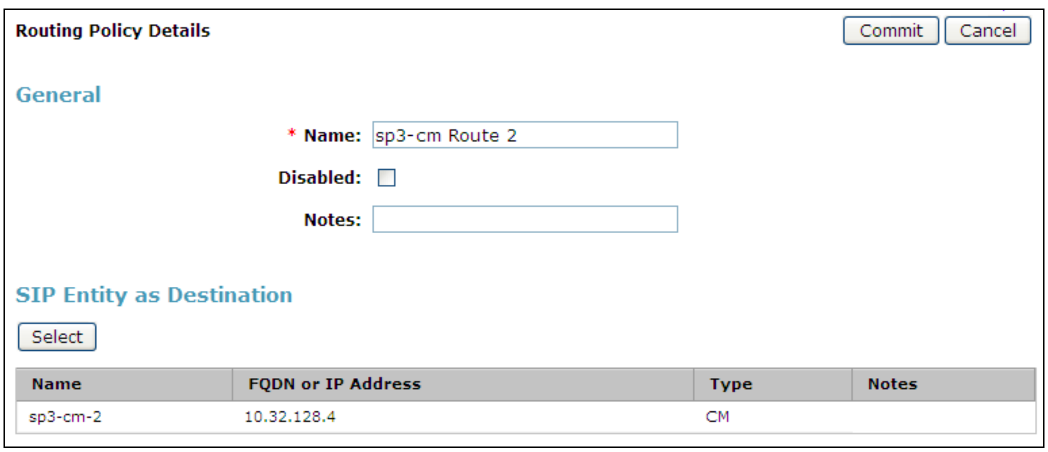
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

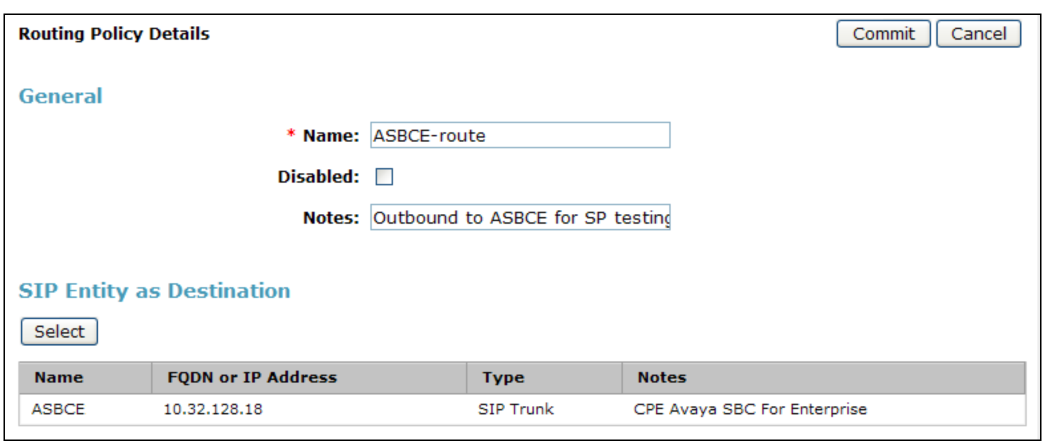
In the **General** section, enter the following values. Use default values for all remaining fields.

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

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

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





6.8. Add 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 TELUS 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 (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

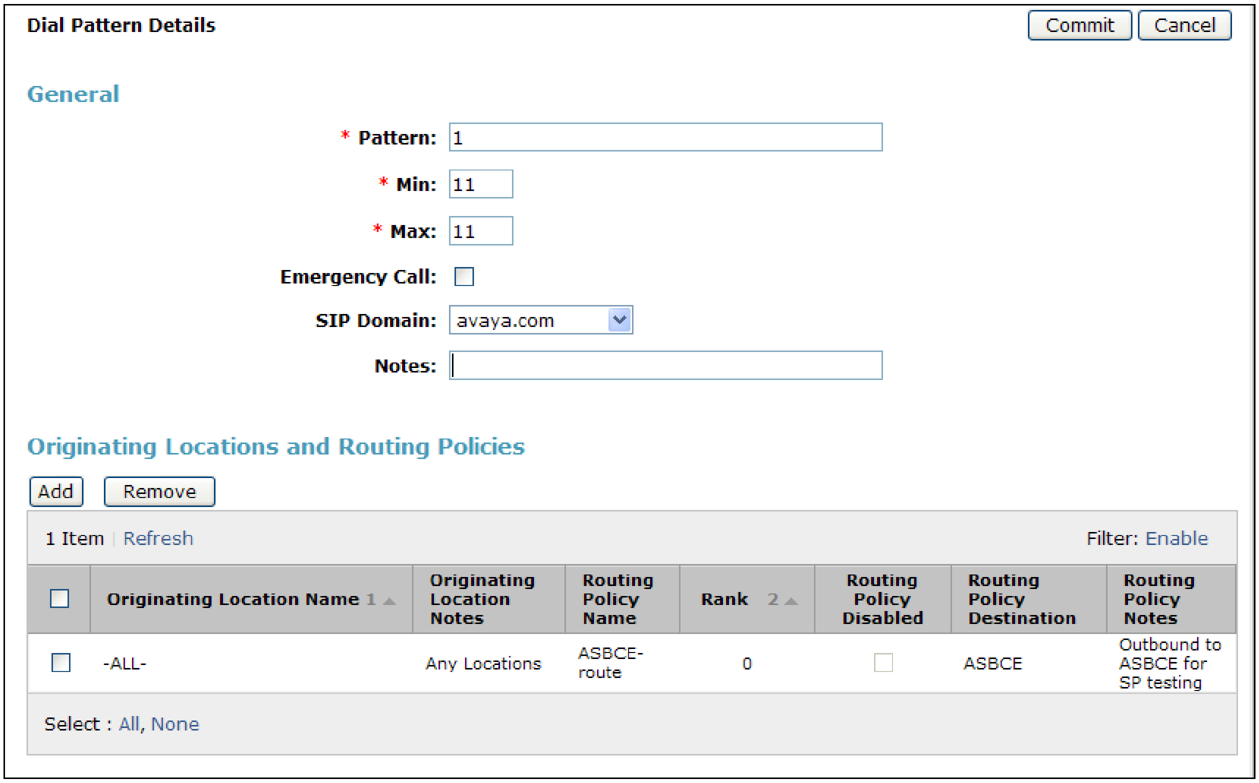
In the **General** section, enter the following values. Use default values for all remaining fields.

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

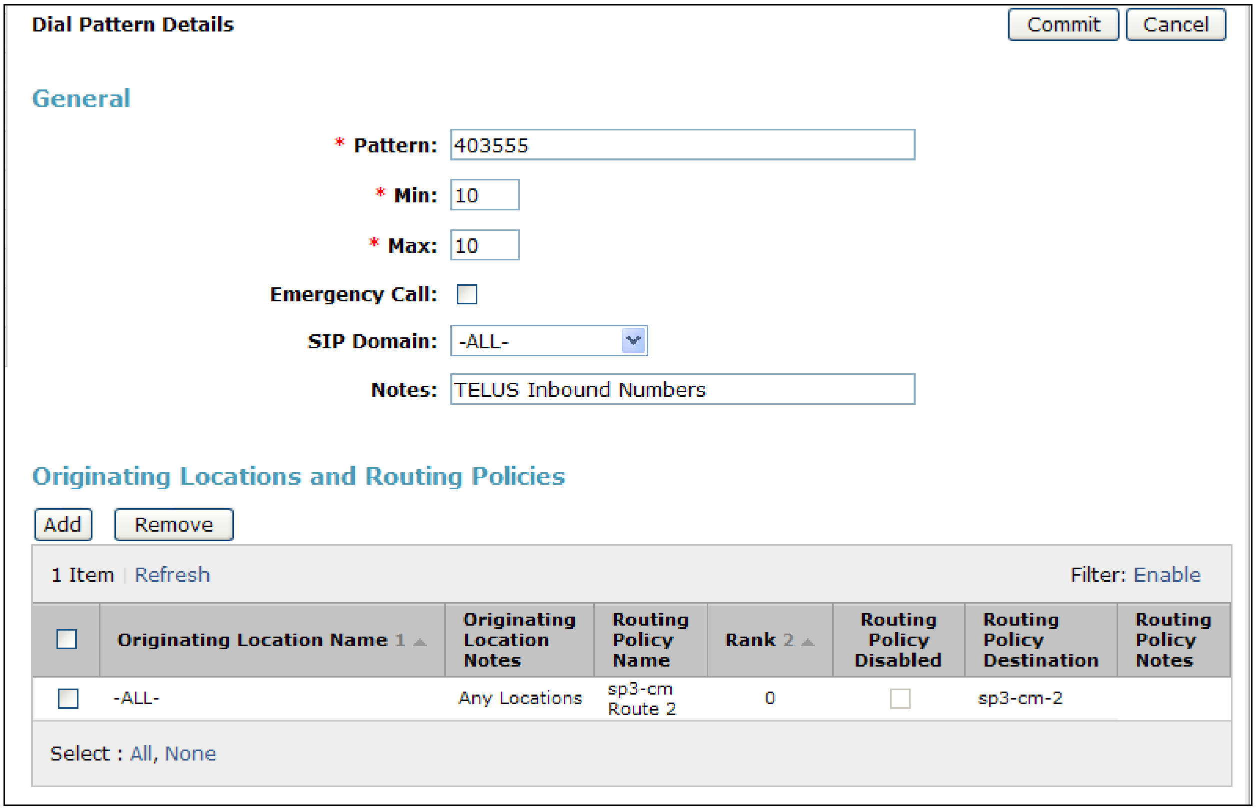
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that 11 digit numbers that begin with a 1 and have a destination domain of **avaya.com** from **ALL** locations uses route policy **ASBCE-Route**.



The second example shows that 10 digit numbers that start with **403555** to any domain and originating from **ALL** locations uses route policy **sp3-cm Route 2**. These are the DID numbers assigned to the enterprise from TELUS.



Dial Pattern Details

Commit | Cancel

General

* Pattern: 403555

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: TELUS Inbound Numbers

Originating Locations and Routing Policies

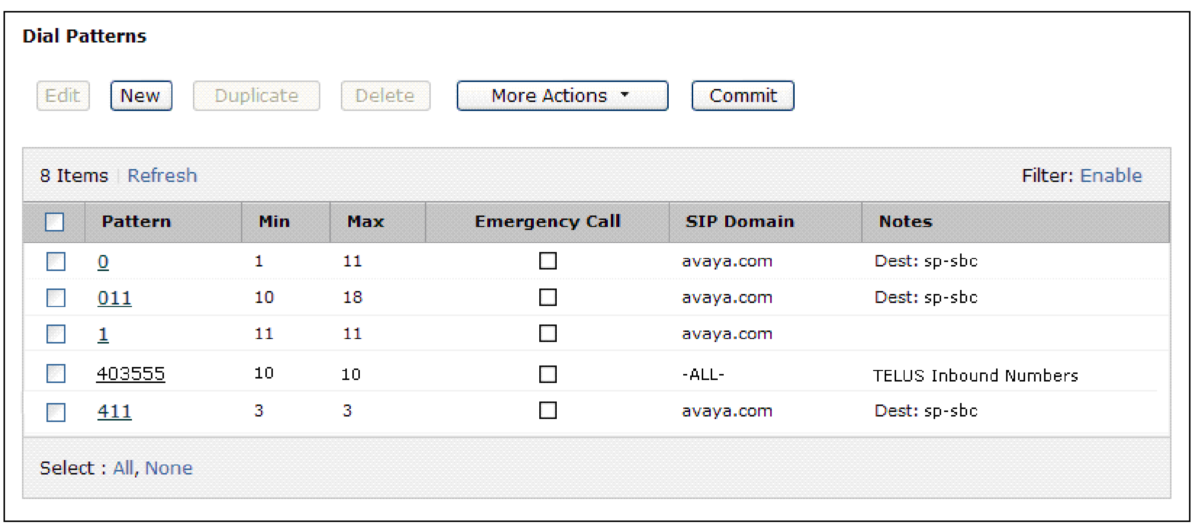
Add | Remove

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
☐	-ALL-	Any Locations	sp3-cm Route 2	0	☐	sp3-cm-2	

Select : All, None

The complete list of dial patterns defined for the compliance test is shown below.



Dial Patterns

Edit | New | Duplicate | Delete | More Actions | Commit

8 Items | Refresh — Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
☐	0	1	11	☐	avaya.com	Dest: sp-sbc
☐	011	10	18	☐	avaya.com	Dest: sp-sbc
☐	1	11	11	☐	avaya.com	
☐	403555	10	10	☐	-ALL-	TELUS Inbound Numbers
☐	411	3	3	☐	avaya.com	Dest: sp-sbc

Select : All, None

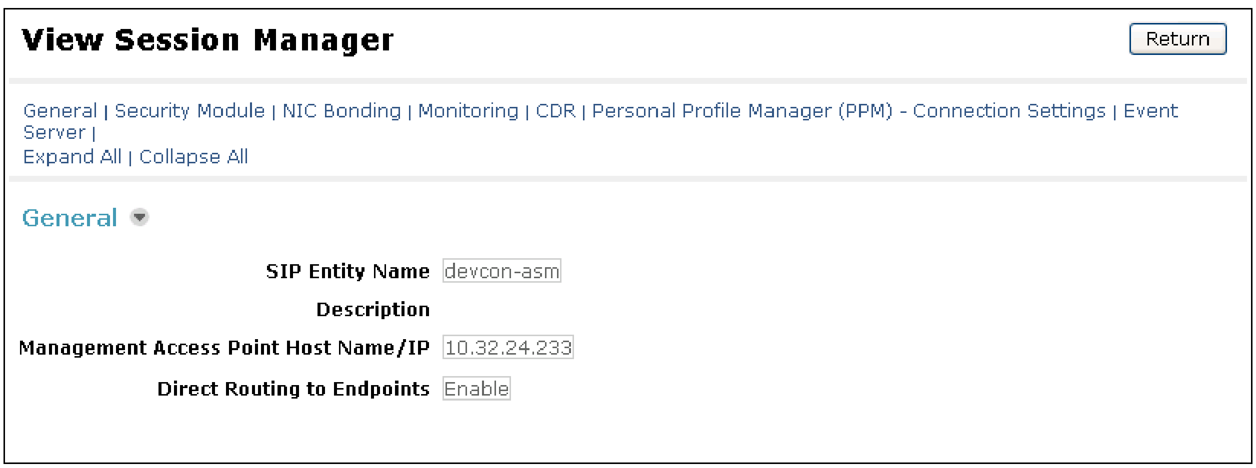
6.9. Add/View Session Manager

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 a Session Manager, from the **Home** page, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and 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.

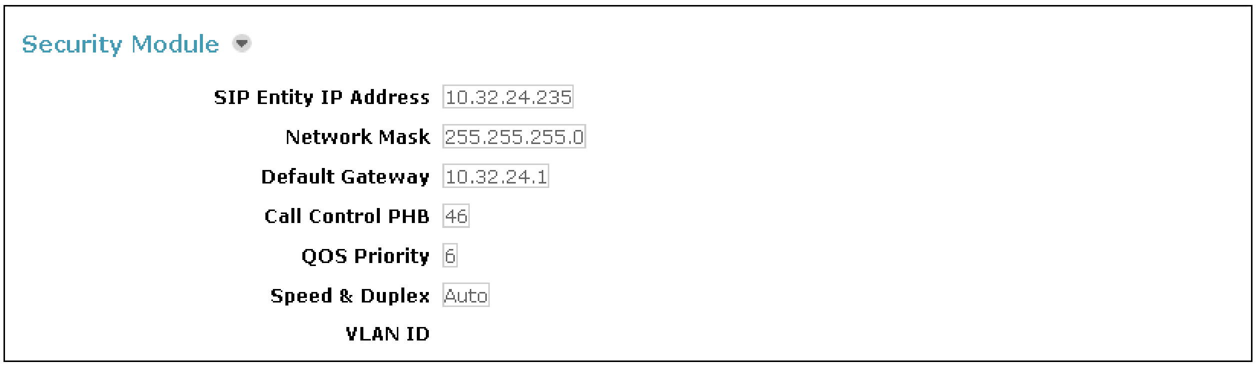
The screen below shows the Session Manager values used for the compliance test.



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 the remaining Session Manager values used for the compliance test.

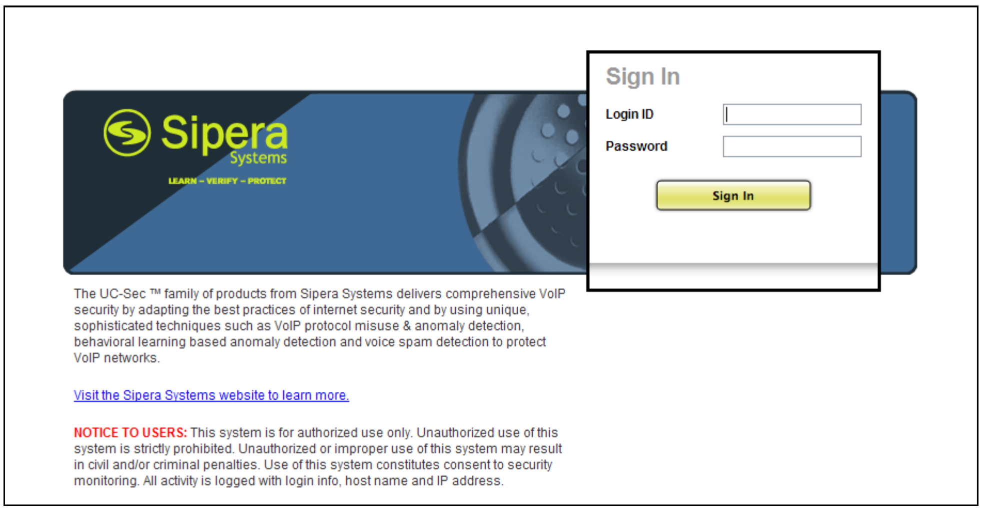


7. Configure Avaya Session Border Controller For Enterprise

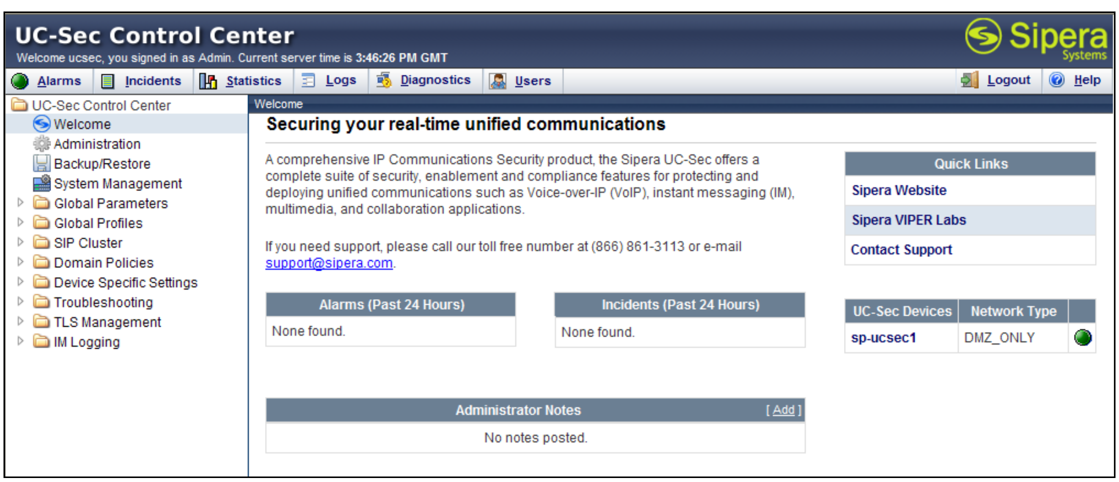
This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

7.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. A screen will appear (not shown) requesting the user to **Choose a destination**. Select **UC-Sec Control Center** and the Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.

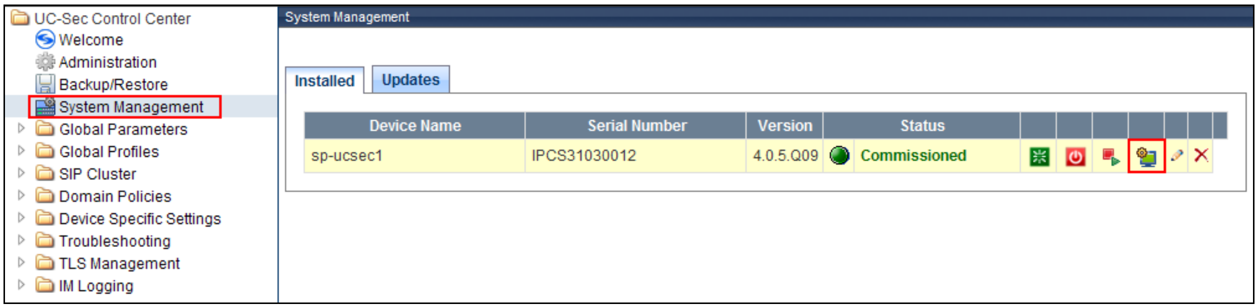


After logging in, the Welcome screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

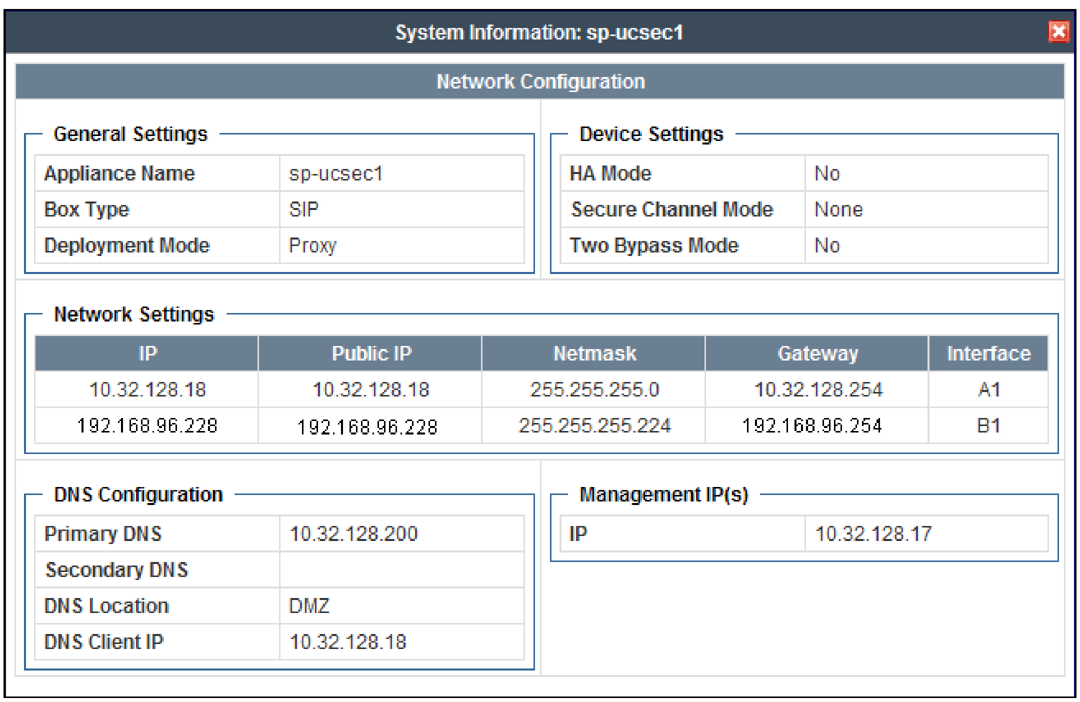


7.2. Verify Network Configuration and Enable Interfaces

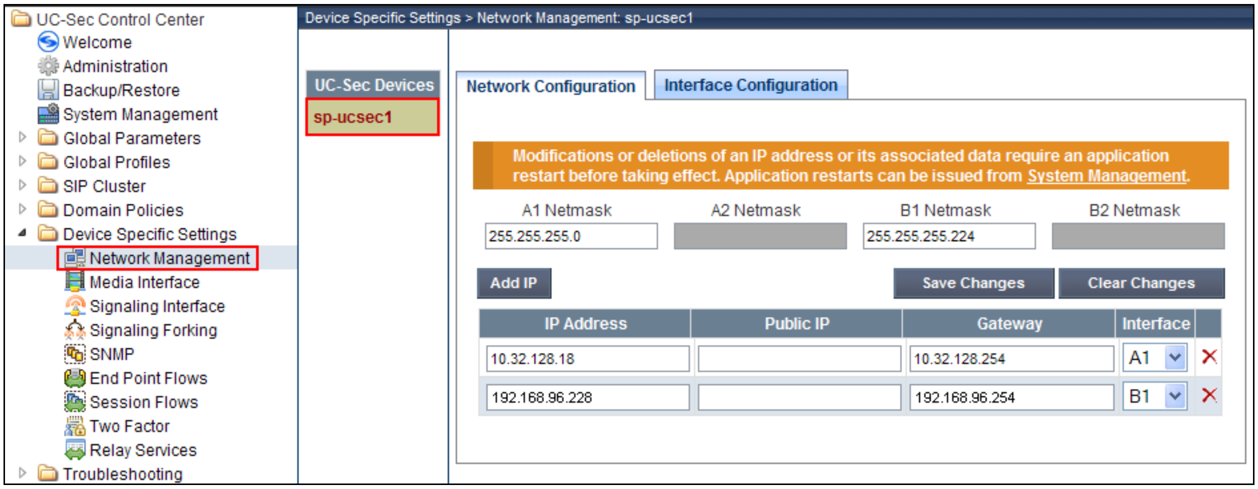
To view the network information provided during installation, navigate to **System Management**. In the right pane, click the **View Config** icon highlighted below.



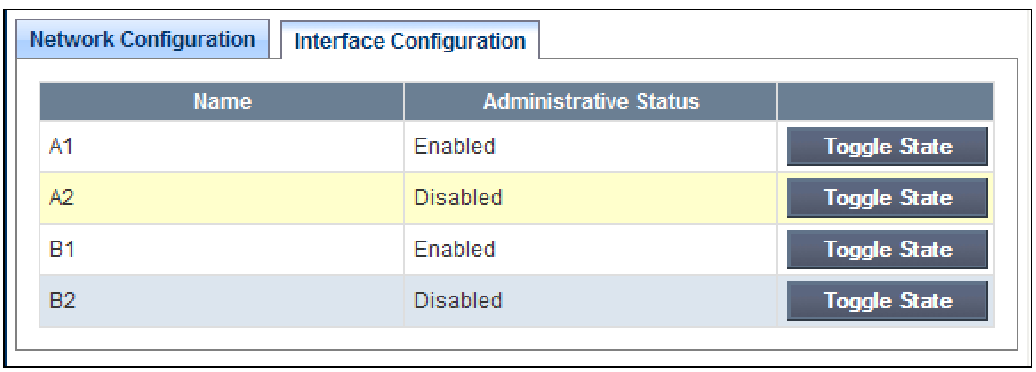
A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE. Each of these interfaces must be enabled after installation. For the compliance test, the private interface and management interface were configured on the same sub-net. However, for security reasons, the management interface should be configured on a separate sub-net.



To enable the interfaces, first navigate to **Device Specific Settings → Network Management** in the left pane and select the device being managed in the center pane. The right pane will show the same **A1** and **B1** interfaces displayed in the previous screen. Click on the **Interface Configuration** tab.



On the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the **Toggle State** button to enable the interface.



7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

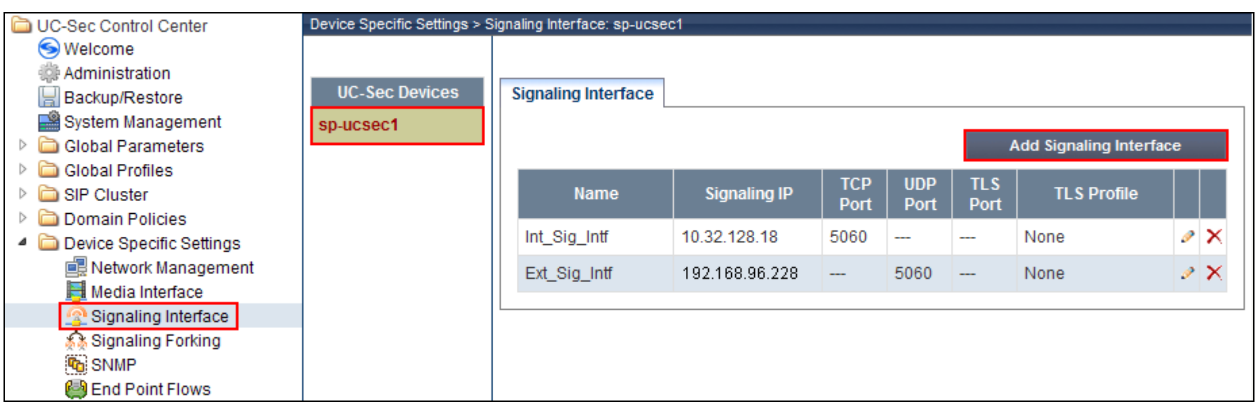
To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Signaling Interface**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**.
- Set **TCP port** to the port the Avaya SBCE will listen on for SIP requests from Session Manager.

Signaling interface **Ent_Sig_Intf** was created for the Avaya SBCE external interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **UDP port** to the port the Avaya SBCE will listen on for SIP requests from TELUS.



7.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

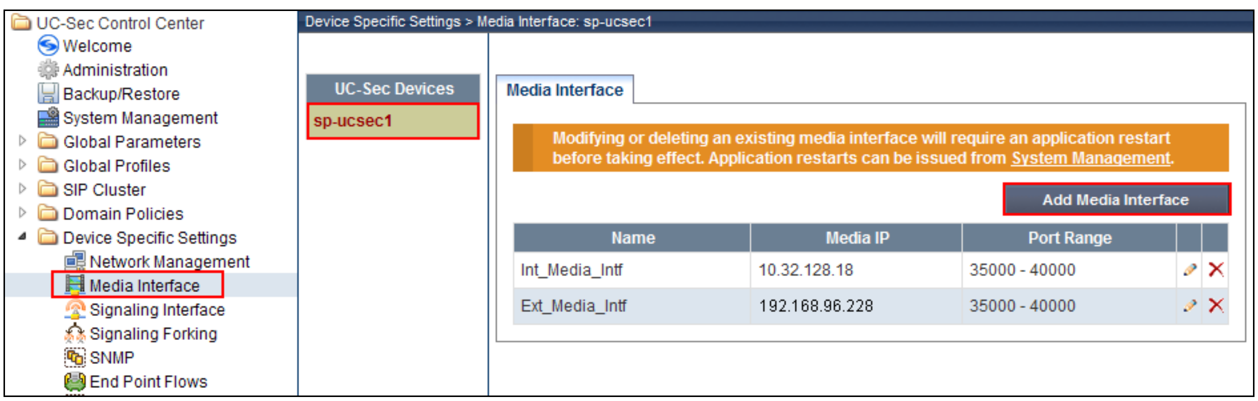
To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add Media Interface**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Media_Intf** was created for the Avaya SBCE internal interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and Session Manager. For the compliance test, the port range used was selected arbitrarily.

Signaling interface **Ent_Media_Intf** was created for the Avaya SBCE external interface. When configuring the interface, configure the parameters as follows:

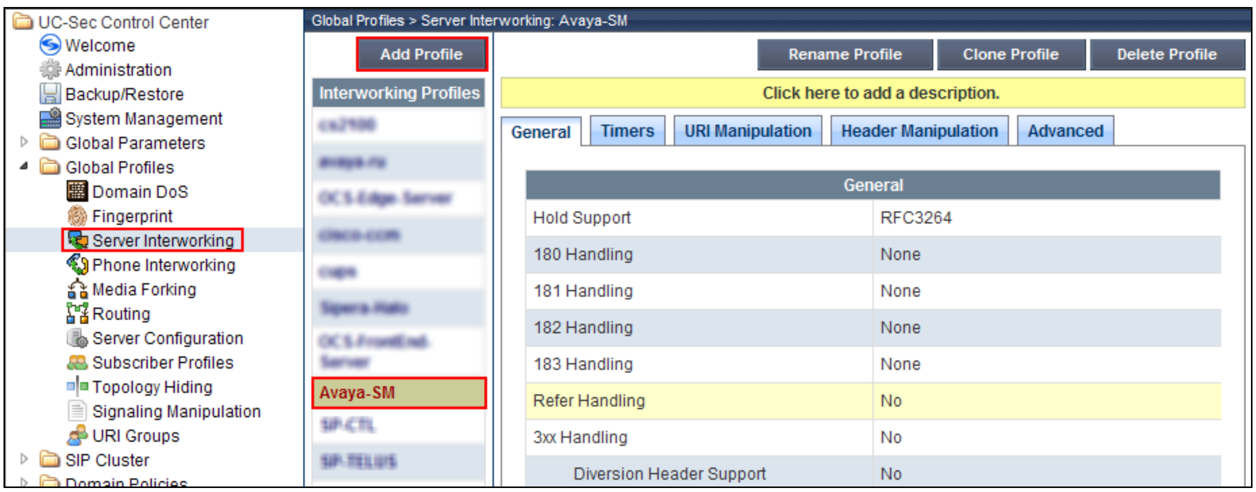
- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and TELUS. For the compliance test, the port range used was selected arbitrarily.



7.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create a server interworking profile for the Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Section 7.7.1** and **7.7.2**.

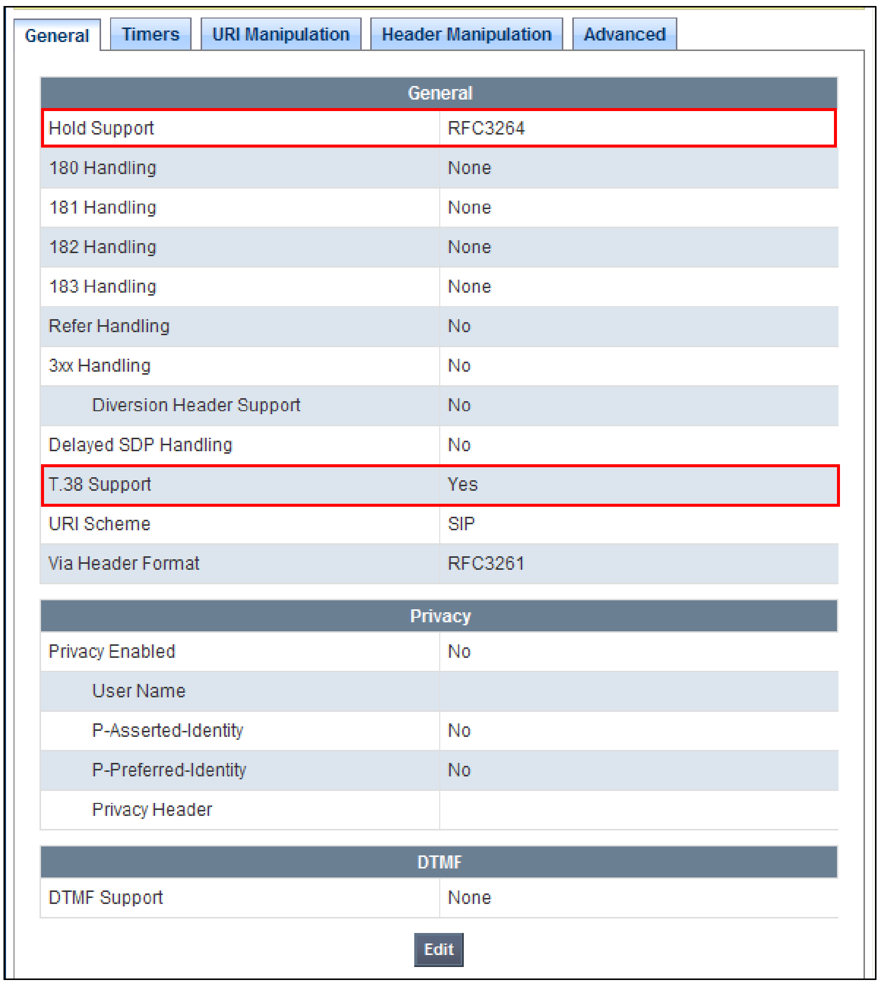
To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane. The example below shows the selection of profile **Avaya-SM**.



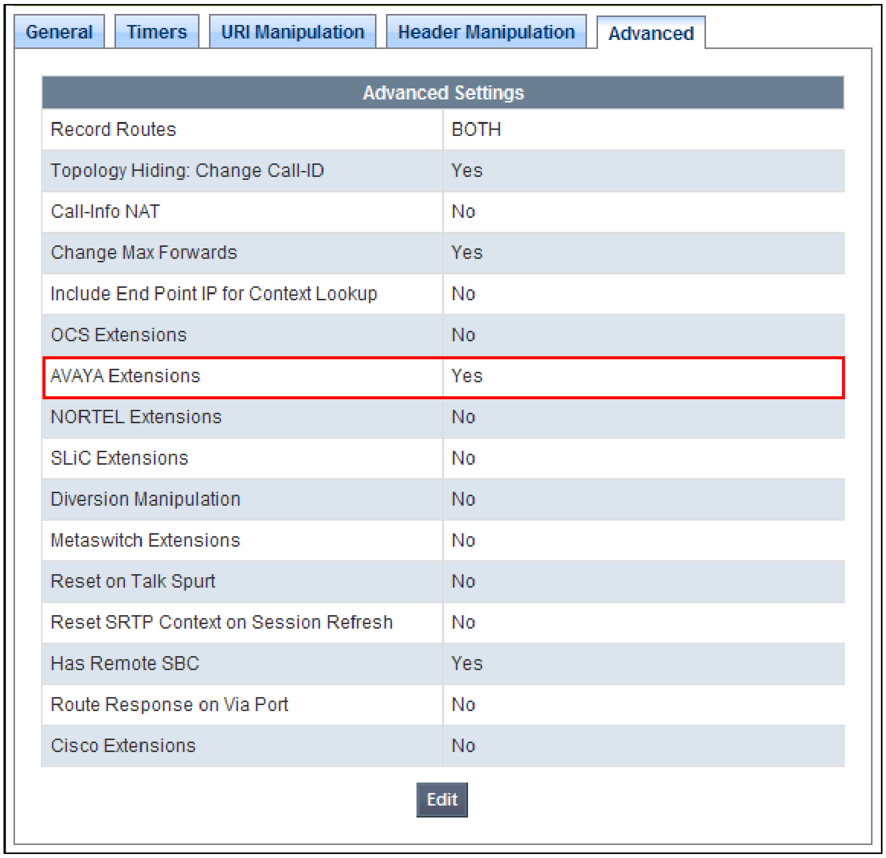
7.5.1. Server Interworking – Session Manager

For the compliance test, server interworking profile **Avaya-SM** was created for Session Manager. When creating the profile, configure the General tab parameters as follows:

- Set **Hold Support** to **RFC3264.**
- Enable **T.38 Support**.



On the Advanced tab, enable the **Avaya Extensions**.


General | Timers | URI Manipulation | Header Manipulation | Advanced

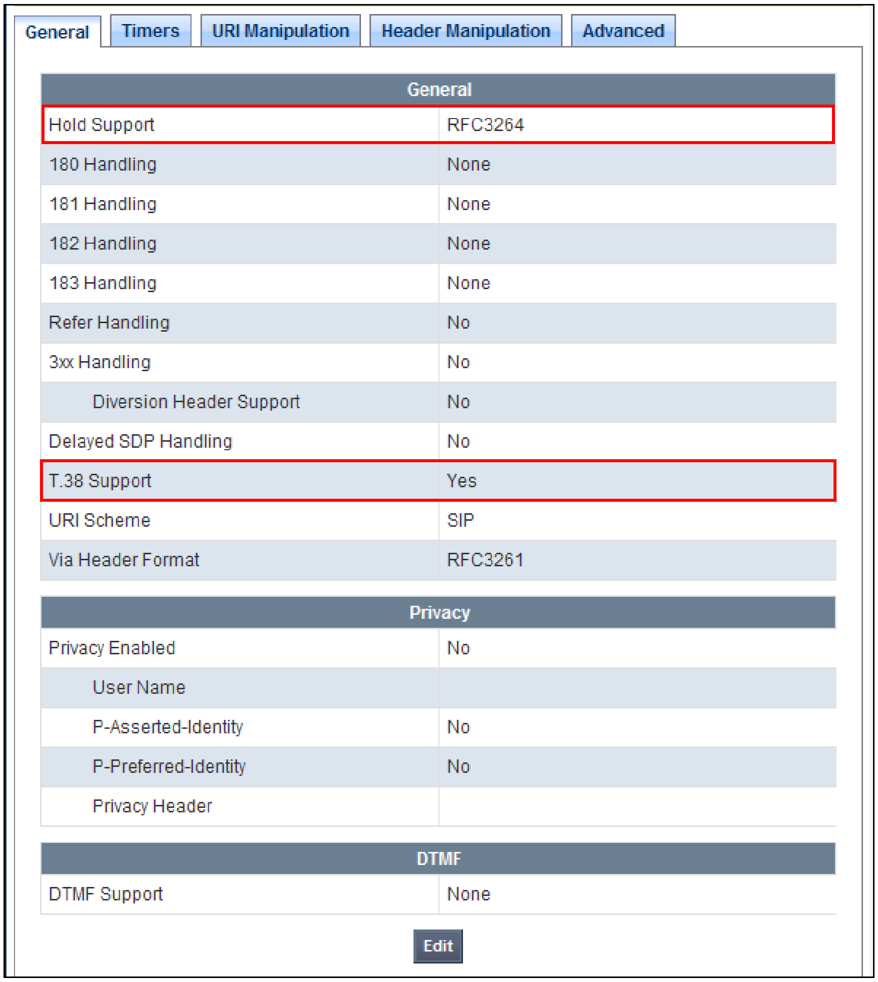
Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

Edit

7.5.2. Server Interworking – TELUS

For the compliance test, server interworking profile **SP-TELUS** was created for the TELUS SIP server. When creating the profile, configure the General tab parameters as follows:

- Set **Hold Support** to **RFC3264.**
- Enable **T.38 Support**.



General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	
DTMF	
DTMF Support	None

Edit

On the Advanced tab, disable the **Avaya Extensions**.

General | Timers | URI Manipulation | Header Manipulation | Advanced

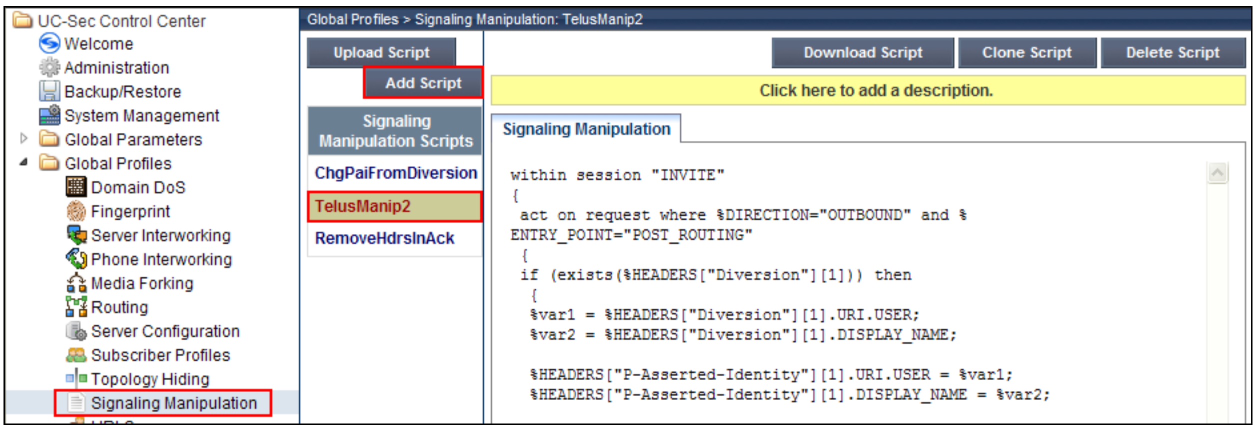
Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

Edit

7.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which can not be done by other configuration within the Avaya SBCE. SIP interworking with TELUS required the signaling manipulation script defined in **Section 7.6.1**. It is applied to the TELUS server in **Section 7.7.2**.

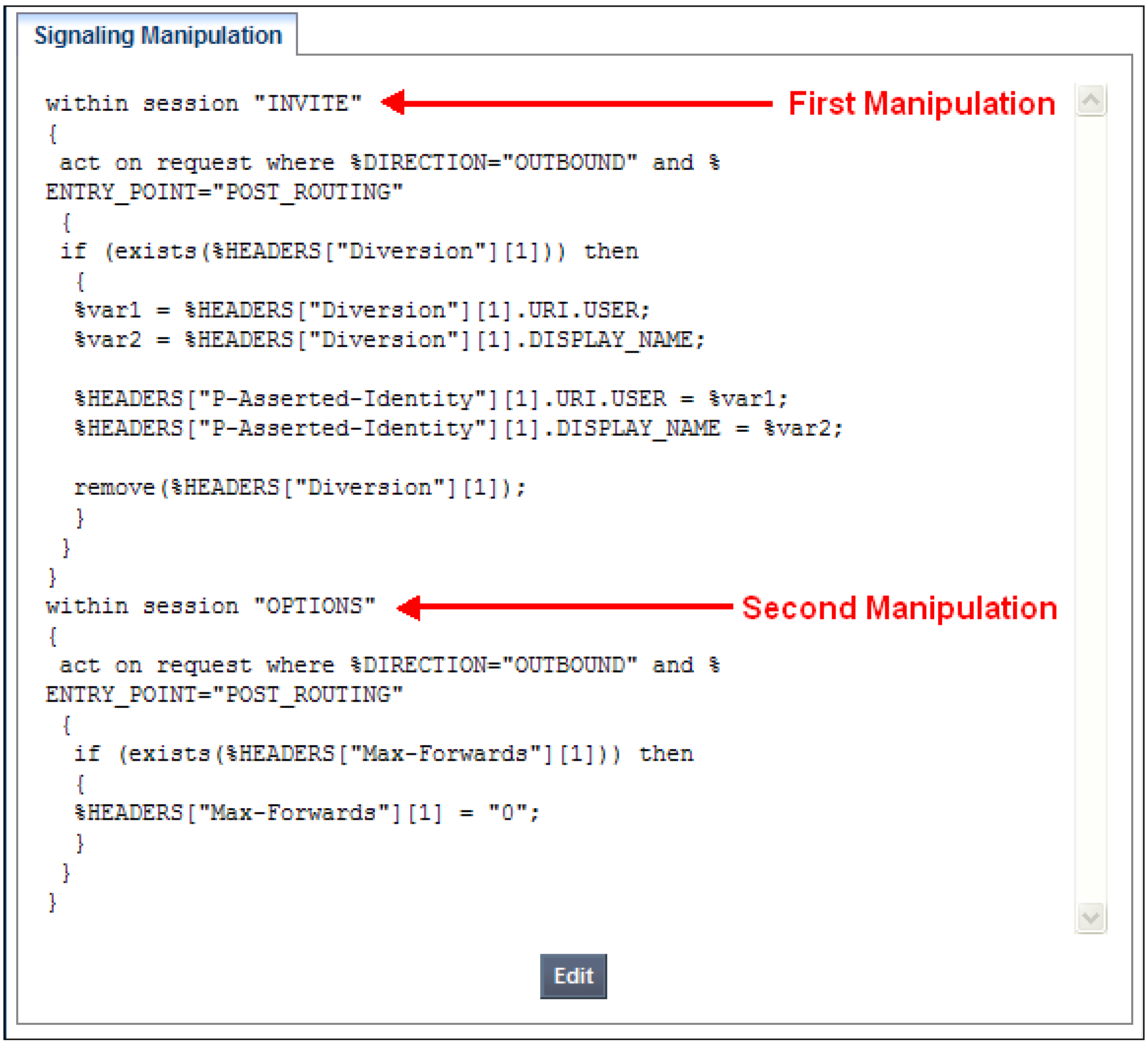
To create a script, navigate to **Global Profiles → Signaling Manipulation** in the left pane. In the center pane, select **Add Script**. A script editor window (not shown) will appear in which the script can be entered line by line. The **Title** box at the top of the editor window (not shown) is where the name of the script is entered. Once complete, the script is shown in the far right pane. To view an existing script, select the script from the center pane. The settings will appear in the right pane. The example below shows the selection of script **TelusManip2**.



7.6.1. Signaling Manipulation – TELUS

For the compliance test, signaling manipulation script **TelusManip2** was created for TELUS. The script performs two manipulations. The first manipulation highlighted below checks if a Diversion header is present in the outbound INVITE message and if it exists then modifies the user and display name of the PAI header with information from the Diversion header. It then removes the Diversion header. This is necessary to complete inbound calls that are redirected back to the service provider.

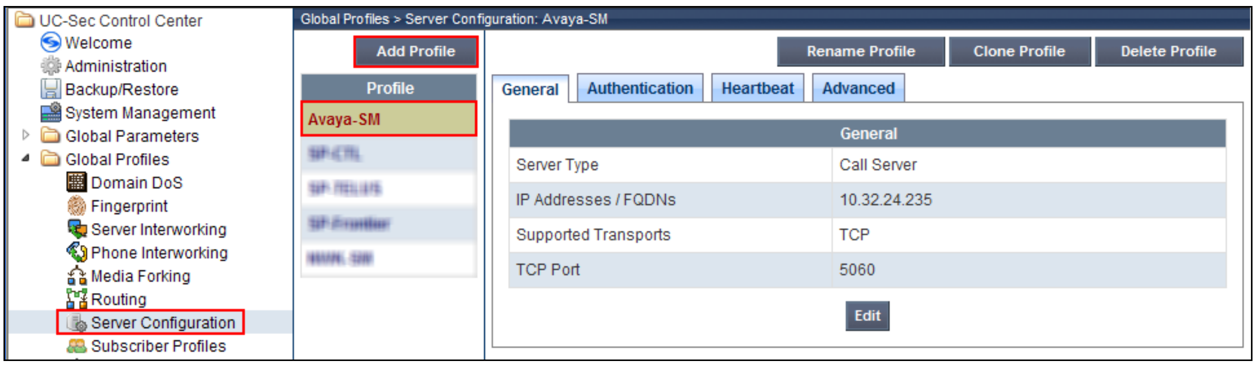
The second manipulation sets the value of the Max-Forwards header to 0 in the outbound OPTIONS message. This is a TELUS requirement.



7.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a server configuration profile for the Session Manager and the service provider SIP server.

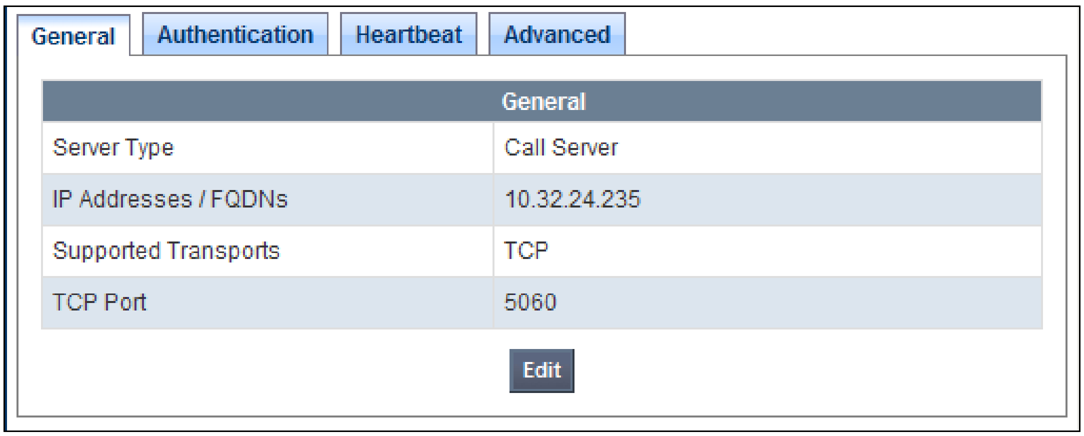
To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane. The example below shows the selection of profile **Avaya-SM**.



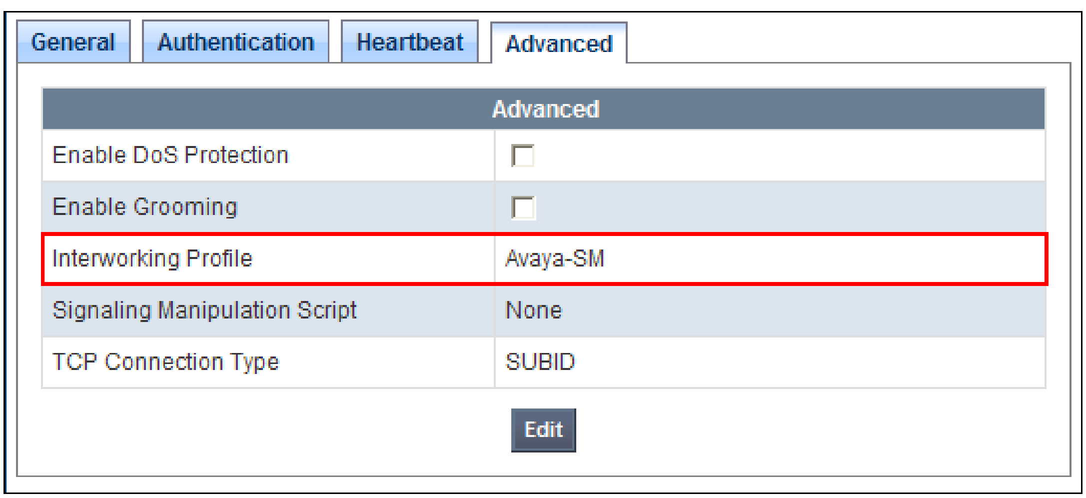
7.7.1. Server Configuration – Session Manager

For the compliance test, server configuration profile **Avaya-SM** was created for Session Manager. When creating the profile, configure the General tab parameters as follows:

- Set **Server Type** to **Call Server.**
- Set **IP Addresses / FQDNs** to the IP address of Session Manager signaling interface.
- Set **Supported Transports** to the transport protocol used for SIP signaling between the Session Manager and the Avaya SBCE.
- Set the **TCP Port** to the port the Session Manager will listen on for SIP requests from the Avaya SBCE.



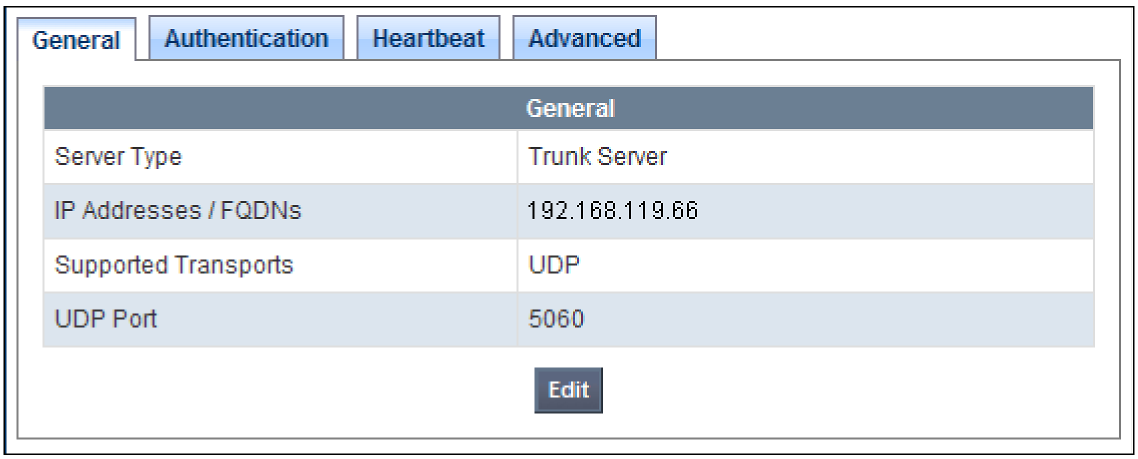
On the Advanced tab, set the **Interworking Profile** field to the interworking profile for the Session Manager defined in **Section 7.5.1**.



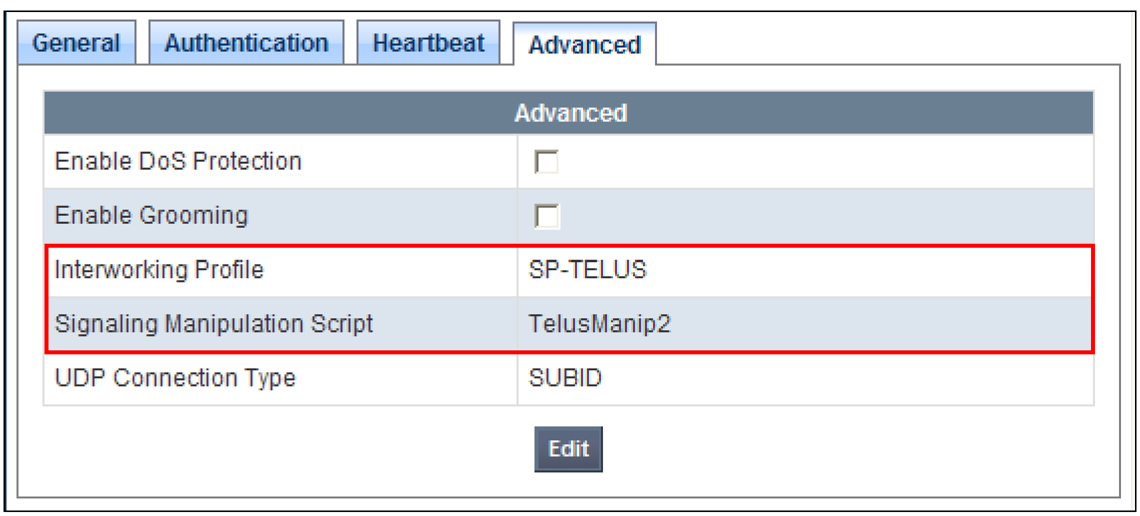
7.7.2. Server Configuration – TELUS

For the compliance test, server configuration profile **SP-TELUS** was created for TELUS. When creating the profile, configure the General tab parameters as follows:

- Set **Server Type** to **Trunk Server.**
- Set **IP Addresses / FQDNs** to the IP address of the TELUS SIP server.
- Set **Supported Transports** to the transport protocol used for SIP signaling between TELUS and the Avaya SBCE.
- Set the **UDP Port** to the port TELUS will listen on for SIP requests from the Avaya SBCE.



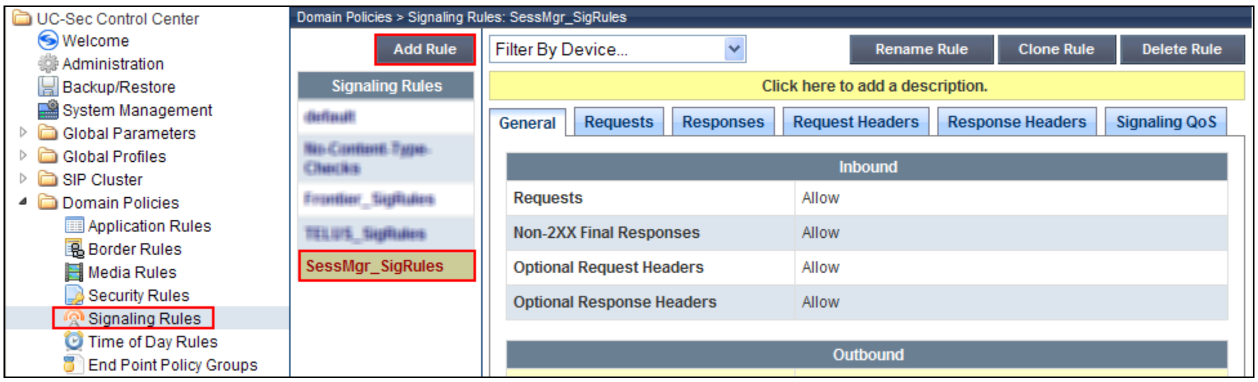
On the Advanced tab, set the **Interworking Profile** field to the interworking profile for TELUS defined in **Section 7.5.2**. Set the **Signaling Manipulation Script** field to the signaling manipulation script for TELUS defined in **Section 7.6.1**.



7.8. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.10**. A specific signaling rule was created for Session Manager. The TELUS SIP server used the **default** rule.

To create a new rule, navigate to **Domain Profiles → Signaling Rules** in the left pane. In the center pane, select **Add Rule**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane. The example below shows the selection of rule **SessMgr_SigRules**.



7.8.1. Signaling Rules – Session Manager

For the compliance test, signaling rule **SessMgr_SigRules** was created for Session Manager to prevent proprietary headers in the SIP messages sent from the Session Manager from being propagated to TELUS. Select this rule in the center pane, then select the Request Headers tab to view the manipulations performed on request messages such as the initial INVITE or UPDATE message.

An entry is created by clicking the **Add In Header Control** or **Add Out Header Control** button depending on the direction (relative to the Avaya SBCE) of the message to be modified. The entries perform the following actions:

1. Removes the **P-Charging Vector** header from the **INVITE** message in the **IN** direction (Session Manager to Avaya SBCE).
2. Removes the **P-Charging Vector** header from the **UPDATE** message in the **IN** direction.
3. Removes the **P-Location** header from the **INVITE** message in the **IN** direction.

General | Requests | Responses | **Request Headers** | Response Headers | Signaling QoS

Add In Header Control | Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-Charging-Vector	INVITE	Forbidden	Remove Header	Yes	IN		
2	P-Charging-Vector	UPDATE	Forbidden	Remove Header	Yes	IN		
3	P-Location	INVITE	Forbidden	Remove Header	Yes	IN		

Similarly, manipulations can be performed on SIP response messages. These can be viewed by selecting the Response Header tab as shown below. Entries were created in the same manner as was done on the Request Headers tab. The entries shown perform the following actions:

1. Removes the **P-Charging Vector** header from the **200** response to an **INVITE** message in the **IN** direction (Session Manager to Avaya SBCE).
2. Removes the **P-Charging Vector** header from the **200** response to an **UPDATE** message in the **IN** direction.
3. Removes the **P-Location** header from the **181** response to an **INVITE** message in the **IN** direction.
4. Removes the **P-Location** header from the **183** response to an **INVITE** message in the **IN** direction.
5. Removes the **P-Location** header from the **200** response to an **INVITE** message in the **IN** direction.

General | Requests | Responses | Request Headers | **Response Headers** | Signaling QoS

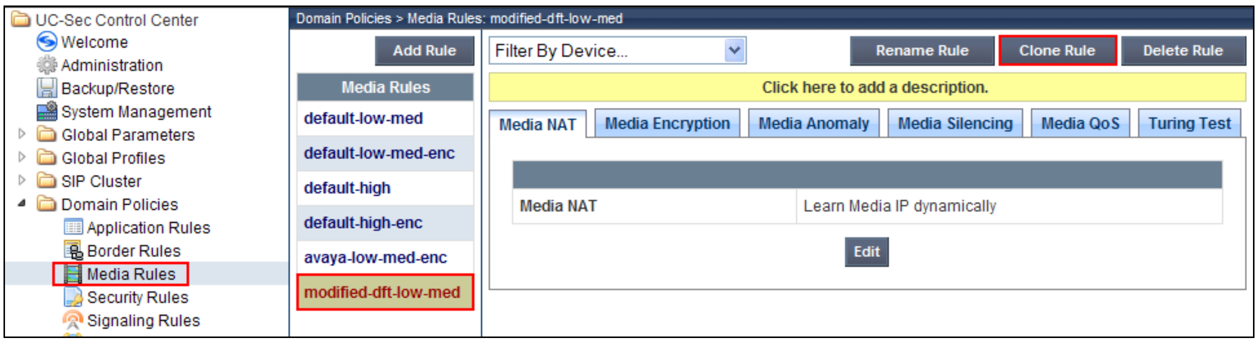
Add In Header Control | Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-Charging-Vector	200	INVITE	Forbidden	Remove Header	Yes	IN		
2	P-Charging-Vector	200	UPDATE	Forbidden	Remove Header	Yes	IN		
3	P-Location	181	INVITE	Forbidden	Remove Header	Yes	IN		
4	P-Location	183	INVITE	Forbidden	Remove Header	Yes	IN		
5	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN		

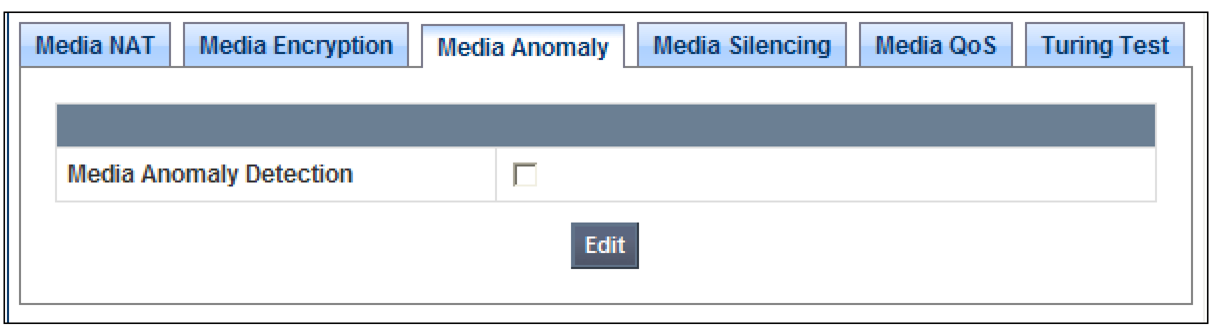
7.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.10**.

To create a new rule, navigate to **Domain Profiles → Media Rules** in the left pane. In the center pane, select **Add Rule**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new rule may be created by selecting an existing rule in the center pane and clicking the **Clone Rule** button in the right pane. This will create a copy of the selected rule which can then be edited as needed. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane. The example below shows the selection of rule **modified-dft-low-med**.



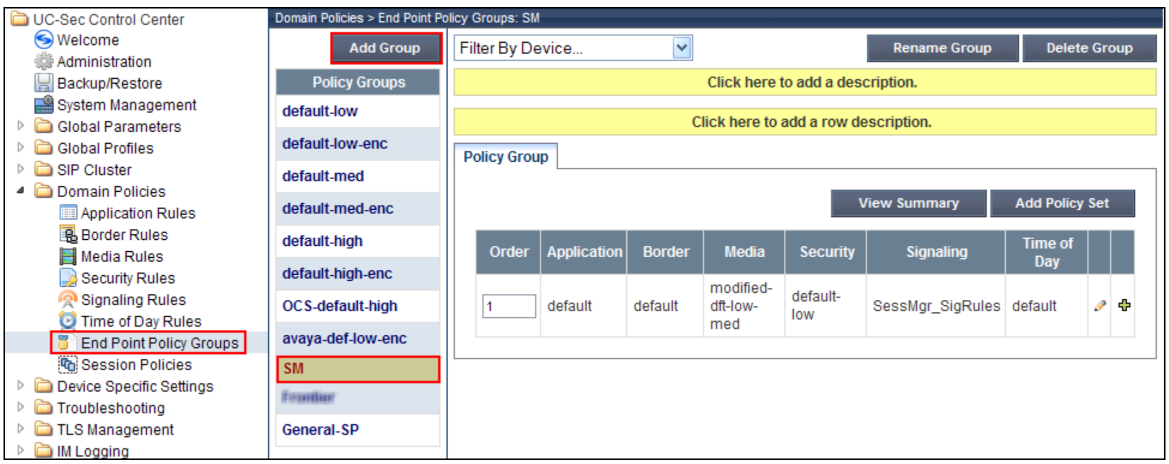
For the compliance test, a single media rule **modified-dft-low-med** was created that was used for both the Session Manager and the TELUS SIP server. It was created by cloning the existing rule **default-low-med** which uses unencrypted media and then disabling **Media Anomaly Detection** on the Media Anomaly tab. This was done to prevent some false media errors from impacting the RTP media stream.



7.10. Endpoint Policy Groups

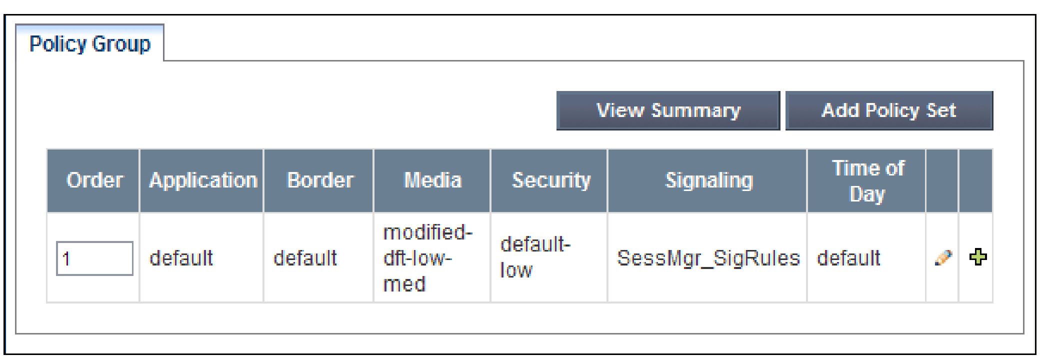
An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.13**.

To create a new group, navigate to **Domain Profiles → End Point Policy Groups** in the left pane. In the center pane, select **Add Group**. A pop-up window (not shown) will appear requesting the name of the new group, followed by series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane. The example below shows the selection of group **SM**.



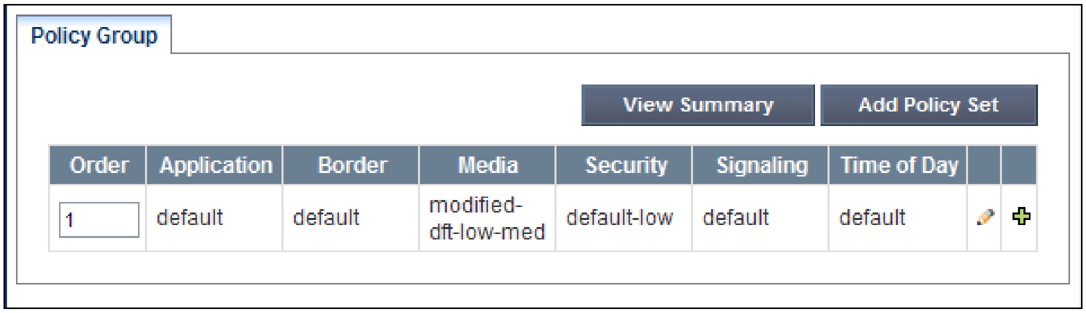
7.10.1. Endpoint Policy Group – Session Manager

For the compliance test, endpoint policy group **SM** was created for Session Manager. Default values were used for each of the rules which comprise the group with the exception of **Media** and **Signaling**. For **Media**, select the media rule created in **Section 7.9**. For **Signaling**, select the signaling rule created for the Session Manager in **Section 7.8.1**.



7.10.2. Endpoint Policy Group – TELUS

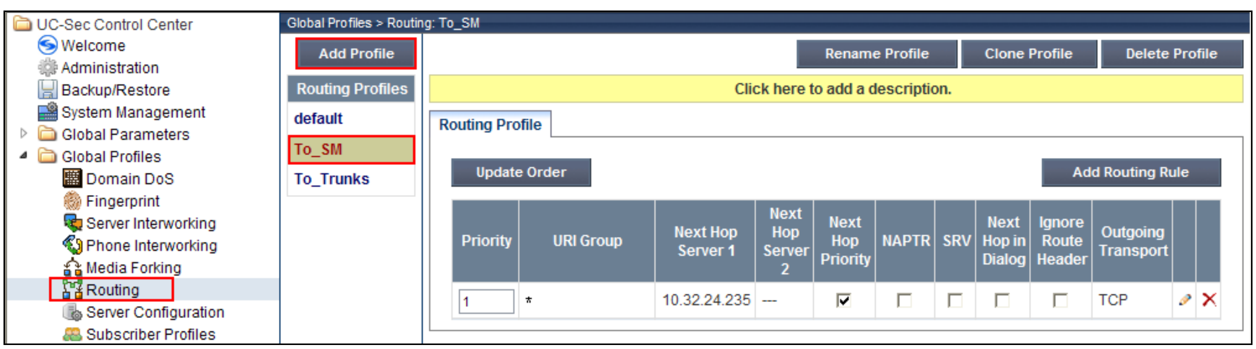
For the compliance test, endpoint policy group **General-SP** was created for the TELUS SIP server. Default values were used for each of the rules which comprise the group with the exception of **Media**. For **Media**, select the media rule created in **Section 7.9**.



7.11. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only have the traffic has matched an endpoint server flow defined in **Section 7.13**. Create a routing profile for the Session Manager and the service provider SIP server.

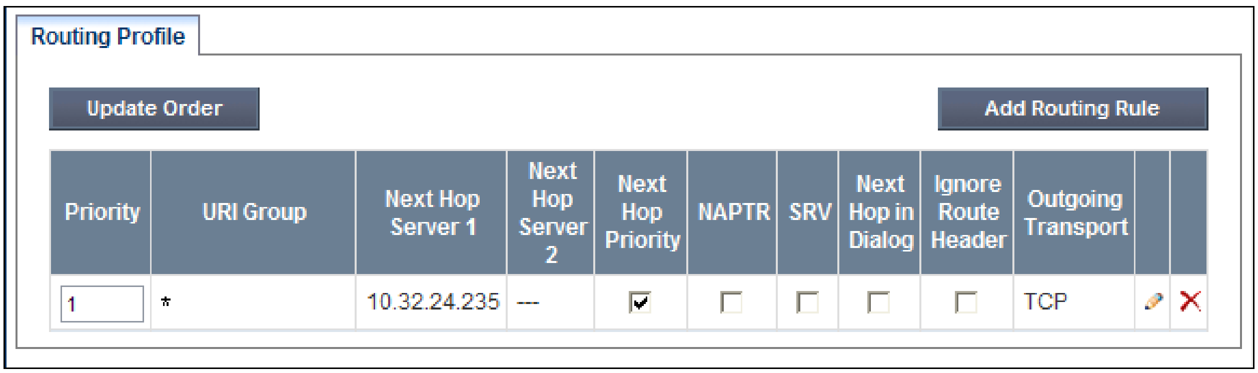
To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane. The example below shows the selection of profile **To_SM**.



7.11.1. Routing – Session Manager

For the compliance test, routing profile **To_SM** was created for Session Manager. When creating the profile, configure the parameters as follows:

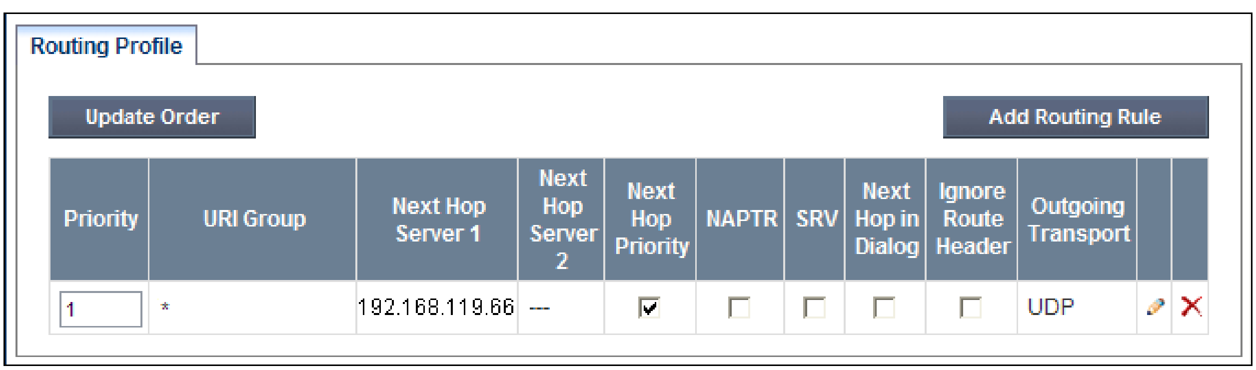
- Set the **URI Group** to the wild card ***** to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the Session Manager signaling interface.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **TCP**.



7.11.2. Routing – TELUS

For the compliance test, routing profile **To_Trunks** was created for TELUS. When creating the profile, configure the parameters as follows:

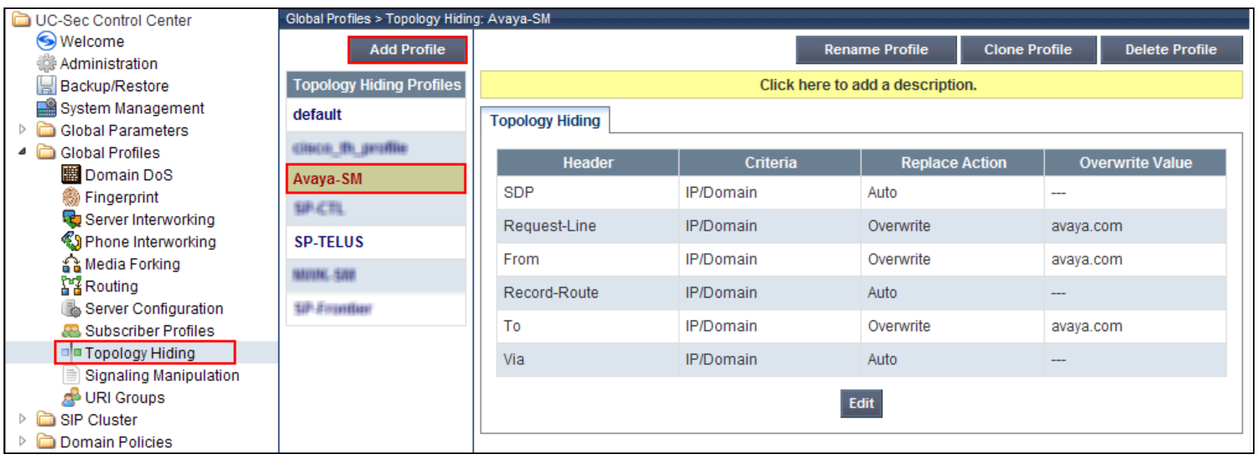
- Set the **URI Group** to the wild card ***** to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the TELUS SIP server.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP**.



7.12. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.13**.

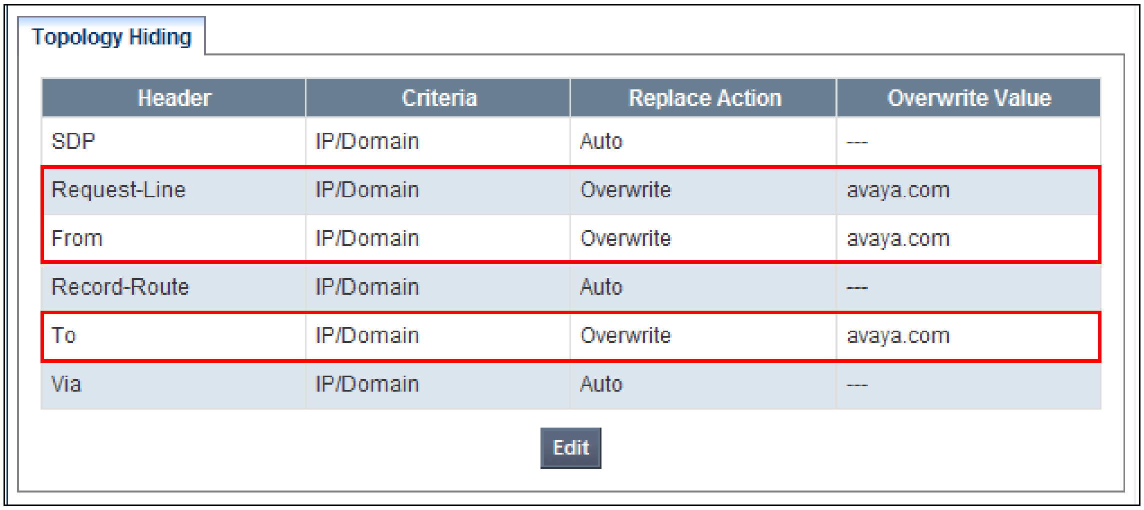
To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add Profile**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a pop-up window in which a header can be selected and configured. Additional headers can be added in this window. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane. The example below shows the selection of profile **Avaya_SM**.



7.12.1. Topology Hiding – Session Manager

For the compliance test, topology hiding profile **Avaya_SM** was created for Session Manager. This profile will be applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**avaya.com**).



Topology Hiding

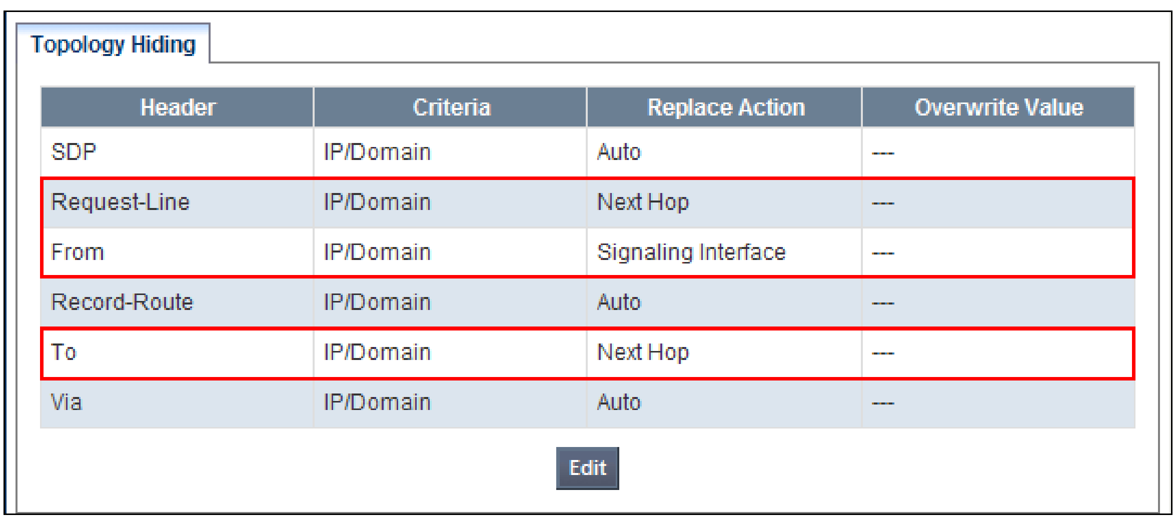
Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya.com
From	IP/Domain	Overwrite	avaya.com
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya.com
Via	IP/Domain	Auto	---

Edit

7.12.2. Topology Hiding – TELUS

For the compliance test, topology hiding profile **SP-TELUS** was created for TELUS. This profile will be applied to traffic from the Avaya SBCE to TELUS. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To**. Set the **Replace Action** for the **Request-Line** and **To** headers to **Next Hop** which is the IP address of the TELUS SIP server. Set the **Replace Action** for the **From** header to **Signaling Interface** which is the IP address of the public interface of the Avaya SBCE.



Topology Hiding

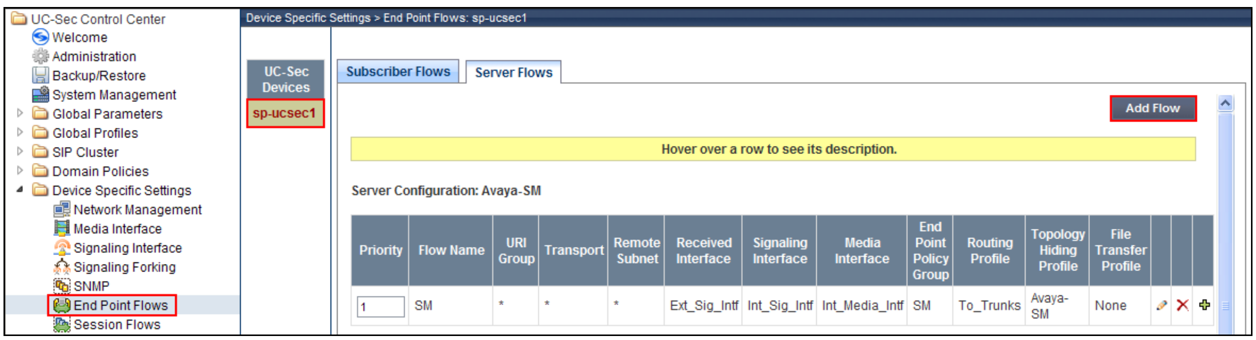
Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Next Hop	---
From	IP/Domain	Signaling Interface	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Next Hop	---
Via	IP/Domain	Auto	---

Edit

7.13. End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of SIP trunking, the signaling endpoints are the Session Manager and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select the Server Flows tab and click the **Add Flow** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.



7.13.1. End Point Flow – Session Manager

For the compliance test, endpoint flow **SM** was created for the Session Manager. All traffic from the Session Manager will match this flow as the source flow and use the specified **Routing Profile To_Trunks** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the external signaling interface.
- Set the **Signaling Interface** to the internal signaling interface.
- Set the **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Session Manager in **Section 7.10.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.11.1** used to direct traffic to the TELUS SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.12.1**.

Subscriber Flows | Server Flows

Add Flow

Hover over a row to see its description.

Server Configuration: Avaya-SM

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	SM	*	*	*	Ext_Sig_Intf	Int_Sig_Intf	Int_Media_Intf	SM	To_Trunks	Avaya-SM	None			

7.13.2. End Point Flow – TELUS

For the compliance test, endpoint flow **TELUS** was created for the TELUS SIP server. All traffic from TELUS will match this flow as the source flow and use the specified **Routing Profile To_SM** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the TELUS SIP server created in **Section 7.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the internal signaling interface.
- Set the **Signaling Interface** to the external signaling interface.
- Set the **Media Interface** to the external media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for TELUS in **Section 7.10.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.11.2** used to direct traffic to the Session Manager.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for TELUS in **Section 7.12.2**.

Server Configuration: SP-TELUS

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	TELUS	*	*	*	Int_Sig_Intf	Ext_Sig_Intf	Ext_Media_Intf	General-SP	To_SM	SP-TELUS	None			

8. TELUS SIP Trunking Configuration

TELUS is responsible for the network configuration of the TELUS SIP Trunking service. TELUS will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise. TELUS will provide the IP address of the TELUS SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager, and the Avaya SBCE configuration discussed in the previous sections.

The configuration between TELUS and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the TELUS network.

9. Verification Steps

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> - Traces calls over a specific trunk group.
    - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
    - **status trunk** <trunk access code number> - Displays trunk group information.
    - **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.

2. Session Manager:
    - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Session Border Controller For Enterprise to TELUS SIP Trunking. TELUS SIP Trunking passed compliance testing. Please refer to **Section 2.2** for any exceptions or workarounds.

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 6.0.3, March 2012.
[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
[3] *Administering Avaya Aura® Communication Manager*, Issue 6.0, June 2010, Document Number 03-300509.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 8.0, June 2010, Document Number 555-245-205.
[5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
[6] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010.
[7] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Document Number 03-603473.
[8] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Document Number 03-603324.
[9] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, April 2010, Document Number 16-601443.
[10] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Issue 8, March 2012, Document Number 16-300698.
[11] *Avaya one-X® Deskphone Edition SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
[12] *Avaya one-X® Deskphone SIP 9608, 9611G, 9621G, 9641G Administrator Guide*, Release 6.0.1, May 2011, Document Number 16-603813.
[13] *Administering Avaya one-X® Communicator*, October 2011.
[14] *Implementing and Administering the Avaya A175 Desktop Video Device with the Avaya Flare® Experience*, Release 1.1, March 2012, Document Number 16-603739.
[15] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/
[16] 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.