Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 to support Telesur SIP Trunking – Issue 1.0

Abstract

These Application Notes describe the procedures required for configuring Session Initiation Protocol (SIP) trunking between Telesur SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.

Telesur is a member of the Avaya DevConnect Service Provider program. The Telesur SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the Telesur network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Telesur SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2 and various Avaya endpoints.

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

2. General Test Approach and Test Results

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

For the compliance test, Telesur required all signaling traffic on the SIP trunk to be routed over a VPN IPsec tunnel, established between the simulated enterprise site and the Telesur network over the public Internet. RTP traffic was routed directly over the Internet.

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:

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using “This Computer” and “Other Phone” modes. (H.332, SIP).
- Inbound and outbound PSTN calls to/from Avaya Flare® Experience for Windows softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 deskphones, Avaya one-X® Communicator and Flare® Experience for Windows .
- Various call types, including: local, long distance and international.
- Codecs G.711A and G.729A and proper codec negotiation.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- T.38 Fax.

The following items are not supported and were not tested:

- Network Call Redirection using the REFER or 302 Moved Temporarily methods is not currently supported by Telesur.
- Emergency calls are supported but were not tested as part of the compliance test

2.2. Test Results

Interoperability testing of the Telesur SIP Trunking service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **Response to OPTIONS**: Telesur was not configured to send OPTIONS messages to the SIP trunk during the compliance test, but responded to the OPTIONS sent by the enterprise with a “200 OK” message.
- **Caller ID on international outbound calls to the U.S.**: Calls originating from the enterprise to PSTN telephones based in the U.S. did not display Caller ID information on the PSTN telephone display. This seems to be the expected behavior for type of calls, which is ultimately controlled by the PSTN providers. This behavior is not necessarily indicative of a limitation of the combined Avaya/Telesur solution.
- **Telephone number on enterprise extensions displays**: On outbound calls originating from the enterprise, once the call was answered by the PSTN endpoint the display on the enterprise telephone changed from the dialed PSTN number to the string “**sgc.c@sil.miami....**”, which was the result of Communication Manager updating the displays, based on the information received in the Contact header arriving in responses from Telesur. To avoid this issue and to keep the original dialed number on the enterprise telephones displays, a script file was created on the Avaya SBCE to manipulate the Contact header on responses arriving from the service provider. See **Section 7.7** later in this document.
- **Codec on international outbound calls to the U.S.**: Calls originating from the enterprise to PSTN telephones based in the U.S. connected using codec G.729A, regardless of the priority order of this codec in the SDP of the outbound INVITE. On incoming calls from the U.S. and on local calls (inbound and outbound) in Suriname, the codec order on the SDP was followed and the calls connect at codec G711A as the first option. Since this behavior on international calls is controlled by the PSTN providers, it is not necessarily an indication of a limitation of the combined Avaya/Telesur solution.
- **PSTN numbering plans**: In the configuration used during the compliance test, the DID numbers accessible from the PSTN that were used for testing had to be redirected in the Telesur softswitch to a different set of DID numbers, that were the actual numbers assigned in the softswitch configuration to the test SIP trunk to the enterprise. The reason to do this was that this second group of DIDs numbers was not accessible from the PSTN. This type of setup is not expected to be present in an actual customer implementation.
- **Call Transfer to the PSTN**: Since Network Call Redirection (NCR) using the REFER or 302 Moved Temporarily methods is not currently supported by Telesur, NCR needs to be disabled on the Trunk Group form in Avaya Communication Manager. Inbound/ outbound calls that are transferred back to the PSTN are still allowed to complete, but Communication Manager is not released after the call is transferred, and two trunks remain busy for the complete duration of the call.

- **T.38 Fax Version**: On inbound fax calls, a “488 Not Acceptable Here” error message was received message from Telesur in response to the re-INVITE with T.38 parameters sent by the enterprise. A script file was created on the Avaya SBCE to replace the “T38FaxVersion:1” parameter contained on the SDP of T.38 re-INVITES sent by Communication Manager, to the “T38FaxVersion:0” acceptable by the Telesur softswitch. Fax calls successfully negotiated the T.38 Fax Version 0 protocol once the script was applied. See **Section 7.7** later in this document.
- **Remote workers/shuffling**: Shuffling (direct IP-IP connections) must be disabled in Communication Manager on the IP-Network-Region assigned to the Remote Workers, to avoid issues of DTMF payload type interoperability and intermittent one way audio that were observed when calls were made from these endpoints. See **Section 5.5**.
- **SIP header optimization**: There are multiple SIP headers used by Communication Manager and Session Manager that at the time of the compliance test had no particular use in the service provider’s network. These headers were removed in order to block private IP addresses and other enterprise information from being propagated outside of the enterprise boundaries, and also to reduce the packet size entering the Telesur network. The parameters “gsid” and “epv” were removed from outbound Contact headers using a Sigma Script in the Avaya SBCE. See **Section 7.7**. Additionally, the following outbound headers were blocked by the Avaya SBCE using Signaling Rules: AV-Correlation-ID, AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location (**Section 7.11**).

2.3. Support

For technical support and contact information on the Telesur SIP Trunking service offer, visit http://www.telesur.sr/

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Telesur SIP Trunking.

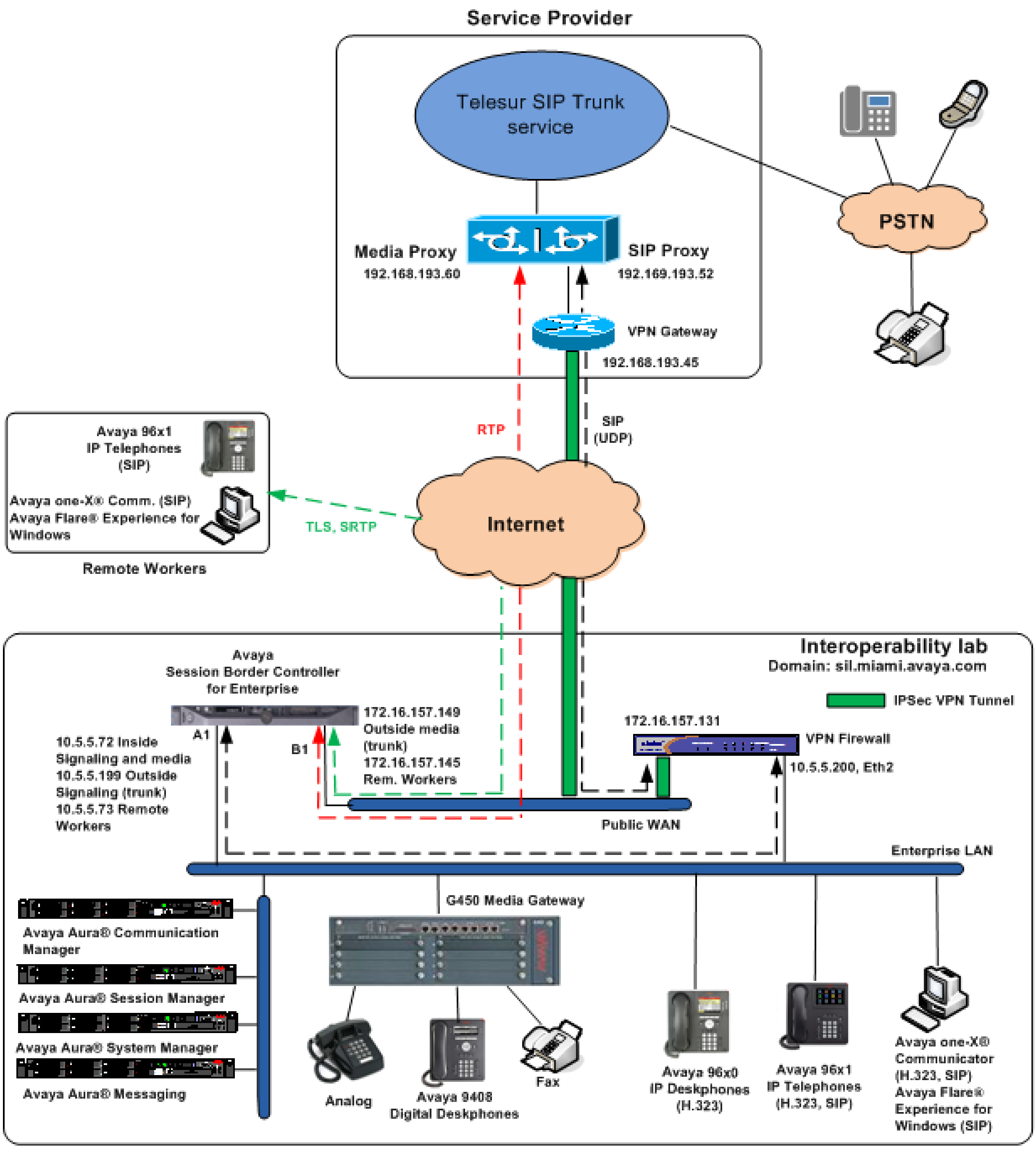


Figure 1: Avaya SIP Enterprise Solution connected to Telesur SIP Trunking.

For security purposes, references to any public IP addresses used during the compliance test have been replaced in these Application Notes with private addresses. Also, PSTN routable phone numbers used in the test have been changed to non-routable numbers.

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya G450 Media Gateway.
- Avaya 96x0 and 96x1 Series IP Telephones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Flare® Experience for Windows softphones.
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the Session Manager at the enterprise via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint at the enterprise. This functionality was successfully tested using the following endpoints and protocols:

- Avaya 96x1 SIP Deskphones (using TLS and SRTP).
- Avaya Flare® Experience for Windows (using TLS and SRTP).
- Avaya one-X® Communicator SIP (using TLS and RTP).

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [**7**] in the **References** section for additional information on this topic.

Located at the edge of the enterprise, the Avaya SBCE has two physical interfaces. Interface B1 was used to connect to the public network, while interface A1 was used to connect to the private enterprise infrastructure. For the compliance test, Telesur required the use of a VPN tunnel to handle all the signaling traffic between the interoperability lab and the Telesur network, while the RTP traffic was routed directly over the Internet. Note that all signaling and media traffic entering or leaving the enterprise still flows through the Avaya SBCE, in this way protecting the enterprise against any SIP-based attacks. The Avaya SBCE also performs network address translation at both the IP and SIP layers.

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 may be performed.

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

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

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

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager on HP® Proliant DL360 G7 Server	6.3 Service Pack 8 (6.3-03.0.124.0 patch 21588) System Platform 6.3.4.08011.0
Avaya Aura® Session Manager on HP® Proliant DL360 G7 Server	6.3 Service Pack 9 (6.3.9.0.639011)
Avaya Aura® System Manager on HP® Proliant DL360 G7 Server	6.3.9 (Update Revision 6.3.9.1.2482) System Platform 6.3.4.08011.0
Avaya Session Border Controller for Enterprise on a Dell R210 V2 Server	6.2.1.Q18
Avaya Aura® Messaging on a Dell PowerEdge R610 server	6.3.SP0 (MSG-03.0.124.0.315_0007)
Avaya G450 Media Gateway	36.9.0
Avaya 96xx Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 3.2.1
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 6.4.1.25
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 6.4
Avaya one-X Communicator (H.323, SIP)	6.2.4.07_FP4
Avaya Flare Experience for Windows	1.1.4.23
Avaya 9408 Digital Telephone	Rel 12.0
Avaya 6210 Analog Telephone	N/A
Telesur	
Ericsson Telephone Soft Switch	TSS4.0 MP-S09 IP6.0
Ericsson TSS Gateway Controller	TGC4.0 IP6.6 IS2.0 CP19EP2
Ericsson Media Gateway	IS MGW2.0 IP6.8 IS2.0 CP20
Ericsson Session Border Gateway	SBG 14 A (2.1.0.00)

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Servers 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 to work with Telesur SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider.

It is assumed that the general installation of Communication Manager and the Avaya G450 Media Gateway has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **391** 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.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 10
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 2
                   Maximum Video Capable IP Softphones: 18000 6
                       Maximum Administered SIP Trunks: 24000 391
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 100   0

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

5.2. System Features

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

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

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




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

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

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

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

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

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code:
          International Access Code:
```

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and the Session Manager security module (**asm**). These node names will be needed for defining the service provider signaling group in **Section 5.6.**

```
change node-names ip                                            Page   1 of   2
                                IP NODE NAMES
    Name              IP Address
ASBCE_A1            10.5.5.72
Acme_s1p0           192.168.10.52
HG_CM               172.16.5.12
HG_SM               172.16.5.32
LSP                 10.5.5.102
asm                 192.168.10.32
default             0.0.0.0
ip_office           192.168.10.60
procr               192.168.10.12
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Telesur used codecs G711A and G729A, in this order of preference. Enter the corresponding codecs in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

                          IP CODEC SET

    Codec Set: 2

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

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

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

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n


                                                                       Packet
                          Mode                 Redundancy              Size(ms)
    FAX                   t.38-standard         0            ECM: y
    Modem                 off                   0
    TDD/TTY               off                   3
    H.323 Clear-channel   n                     0
    SIP 64K Data          n                     0                      20
```

5.5. IP Network Regions

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

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

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1          Authoritative Domain: sil.miami.avaya.com
    Name: Telesur                       Stub Network Region: n
MEDIA PARAMETERS                        Intra-region IP-IP Direct Audio: yes
      Codec Set: 2                      Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                              IP Audio Hairpinning? n
   UDP Port Max: 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 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

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

 Source Region: 2     Inter Network Region Connection Management     I      M
                                                                     G  A   t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G   c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L   e
 1    2     y    NoLimit                                             n      t
 2    2                                                                 all
 3
 4
```

A separate network region was additionally created and assigned to the remote workers. In this network-region, inter-region direct IP-IP audio connections (shuffling) were disabled. This was necessary as a workaround to the interoperability problems observed on calls originating from these endpoints, as mentioned in **Section 2.2.** In the example below, IP Network Region 5 was used for this purpose.

Use the **change ip-network-region 5** command and enter the following parameters:

- **Authoritative Domain**: ***sil.miami.avaya.com***
- Enter a descriptive name in the **Name** field.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Change the **Inter-region IP-IP Direct Audio** to ***no.*** This will effectively disable shuffling between endpoints in this network-region and the rest of the Enterprise
- Default values can be used for all other fields.

```
change ip-network-region 5                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 5
Location: 1         Authoritative Domain: sil.miami.avaya.com
    Name: Remote Workers           Stub Network Region: n
MEDIA PARAMETERS                   Intra-region IP-IP Direct Audio: yes
      Codec Set: 2                 Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                         IP Audio Hairpinning? n
   UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```

On **Page 4**, specify the IP codec set to be used for traffic between region 5 and region 1 (the rest of the enterprise). Codec set **2** was used for calls between region 5 (the remote workers region) and region 1 (the rest of the enterprise). Note that since shuffling is not allowed, it was not necessary to specify a codec set between network regions 5 and 2.

```
change ip-network-region 5                                      Page   4 of  20

 Source Region: 5     Inter Network Region Connection Management     I        M
                                                                     G  A     t
 dst codec direct   WAN-BW-limits   Video       Intervening      Dyn A  G     c
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC R  L     e
 1    2     y    NoLimit                                             n        t
 2
 3
 4
 5    2                                                                 all
 6
```

Use the **change ip-network-map** to assign the inside IP address of the Avaya SBCE used for remote workers, ***10.5.5.73*** in the reference configuration, to network region 5. Note that the configuration steps required to support remote workers are not covered in these Application Notes. Consult [**7**] in the **References** section for additional information.

```
change ip-network-map                                           Page   1 of  63
                              IP ADDRESS MAPPING

                                                Subnet  Network       Emergency
 IP Address                                     Bits    Region  VLAN  Location Ext
 ---------------------------------------------  ------  ------  ----  -------------
 FROM: 10.5.5.73                                /32     5       n
   TO: 10.5.5.73
 FROM:                                          /               n
   TO:
```

5.6. Signaling Group

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

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, ***tls*** was used.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to ***SM*** once Communication Manager detects its peer is a Session Manager.

Note: Once the **Peer-Server** field is updated to ***SM***, the system changes the default values of the following fields, setting them to display–only:

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to ***y***.
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to ***n***.

- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***asm***. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.

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

 Group Number: 2             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                     Far-end Node Name: asm
 Near-end Listen Port: 5063                    Far-end Listen Port: 5063
                                            Far-end Network Region: 2

Far-end Domain: sil.miami.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
        Enable Layer 3 Test? y                       Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n               Alternate Route Timer(sec): 6
```

- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For the compliance test both the **Near-end Listen Port** and **Far-end Listen Port** were set to ***5063***.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. Note that media shuffling can also be individually enabled or restricted on each IP network regions form.
- Default values may be used for all other fields.

5.7. Trunk Group

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

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group shown in the previous section.
- 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 2                                                   Page   1 of  21
                                TRUNK GROUP

Group Number: 2                   Group Type: sip           CDR Reports: y
  Group Name: Telesur                         COR: 1        TN: 1        TAC: 602
   Direction: two-way         Outgoing Display? n
 Dial Access? n                                       Night Service:
Queue Length: 0
Service Type: public-ntwrk           Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 6
```

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

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

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y
```

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. The private numbering table in **Section 5.8** will be used to map local Communication Manager extension numbers to the DID numbers known to Telesur. Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

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



                    Numbering Format: private
                                                UUI Treatment: service-provider

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

On **Page 4**, set the **Network Call Redirection** field to ***n***. See **Section 2.2** for more details on this setting. Set the **Send Diversion Header** field to ***y***. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to ***n***.

Set the **Telephone Event Payload Type** to ***98***, and **Convert 180 to 183 for Early Media** to ***y***, the values preferred by Telesur. Default values were used for all other fields.

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

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? y
                                   Support Request History? n
                              Telephone Event Payload Type: 98


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

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
```

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected in the trunk form to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs) and they are used to authenticate the caller with the Service Provider. The example below shows four DID numbers assigned by Telesur for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  3001             2          597600095        9     Total Administered: 9
 4  3002             2          597600096        9        Maximum Entries: 540
 4  3003             2          597600097        9
 4  3004             2          597600098        9
```

5.9. Inbound Routing

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

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    6  600095           6   3001
 public-ntwrk    6  600096           6   3002
 public-ntwrk    6  600097           6   3003
 public-ntwrk    6  600098           6   3004
 public-ntwrk
```

5.10. Outbound Routing

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

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

    Dialed    Total  Call       Dialed    Total  Call       Dialed    Total  Call
    String    Length Type       String    Length Type       String    Length Type
   0           1    attd
   1           5    ext
   2           5    ext
   3           4    ext
   4           5    ext
   5           5    ext
   6           3    dac
   7           5    ext
   8           5    ext
   9           1    fac
   *           3    dac
   #           3    dac
```

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

```
change feature-access-codes                                    Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
                 Automatic Callback Activation: *33     Deactivation: #33
Call Forwarding Activation Busy/DA: *30   All: *31     Deactivation: #30
   Call Forwarding Enhanced Status:       Act:         Deactivation:
```

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

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

          Dialed              Total     Route     Call    Node    ANI
          String             Min  Max  Pattern    Type    Num     Reqd
    001                      13   13    2         intl            n
    420                      6    6     2         locl            n
    597                      9    9     2         natl            n
                                                                  n
```

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

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format**: Set to ***unk-unk***. All calls using this route pattern will use the private numbering table.

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2      Pattern Name: Telesur
                             SCCAN? n      Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 2    0                                                               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   none
```

Enter the **save translation** command to save all changes made to the Communication Manager configuration.

6. Configure Avaya Aura® Session Manager

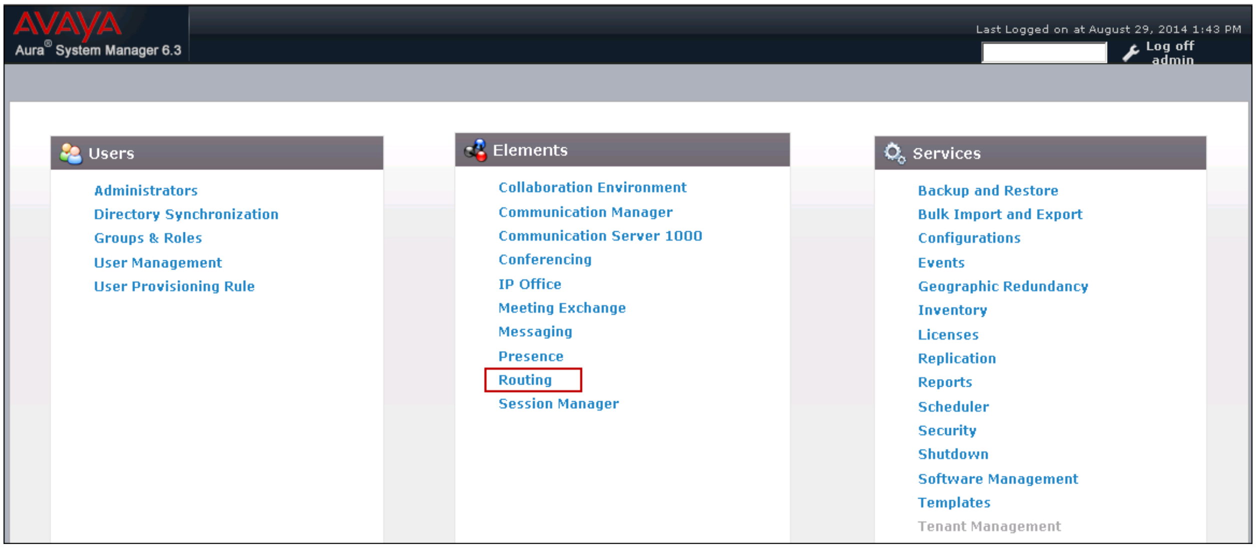
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

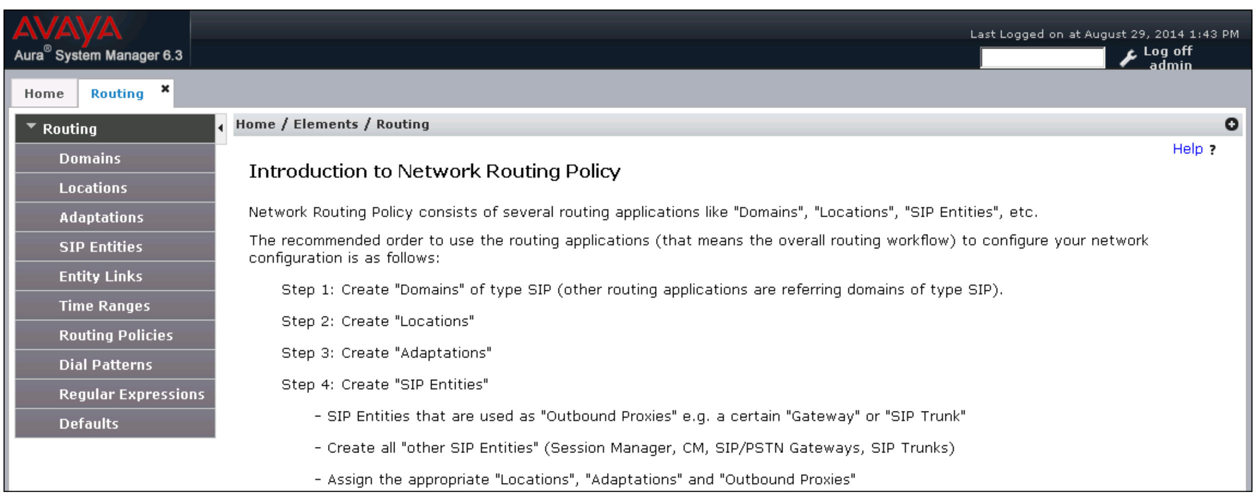
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. System Manager Login and Navigation

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



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

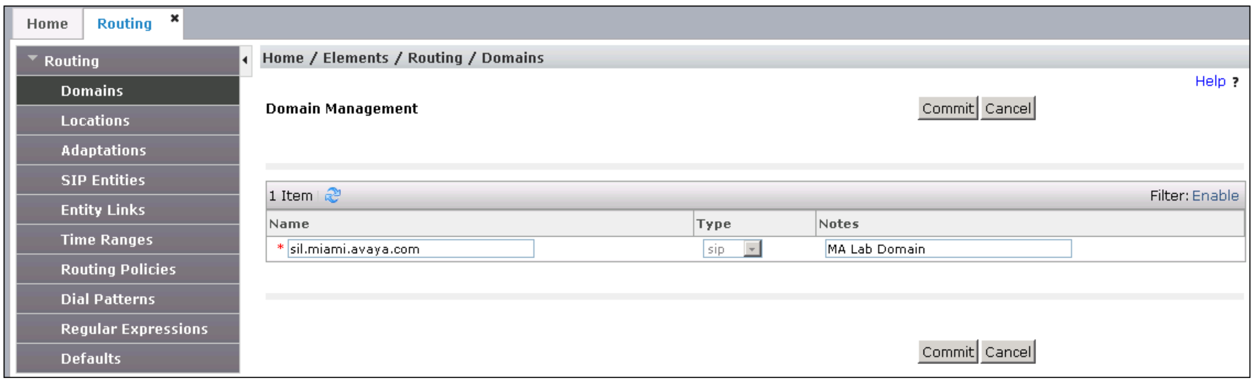


6.2. SIP Domain

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

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

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



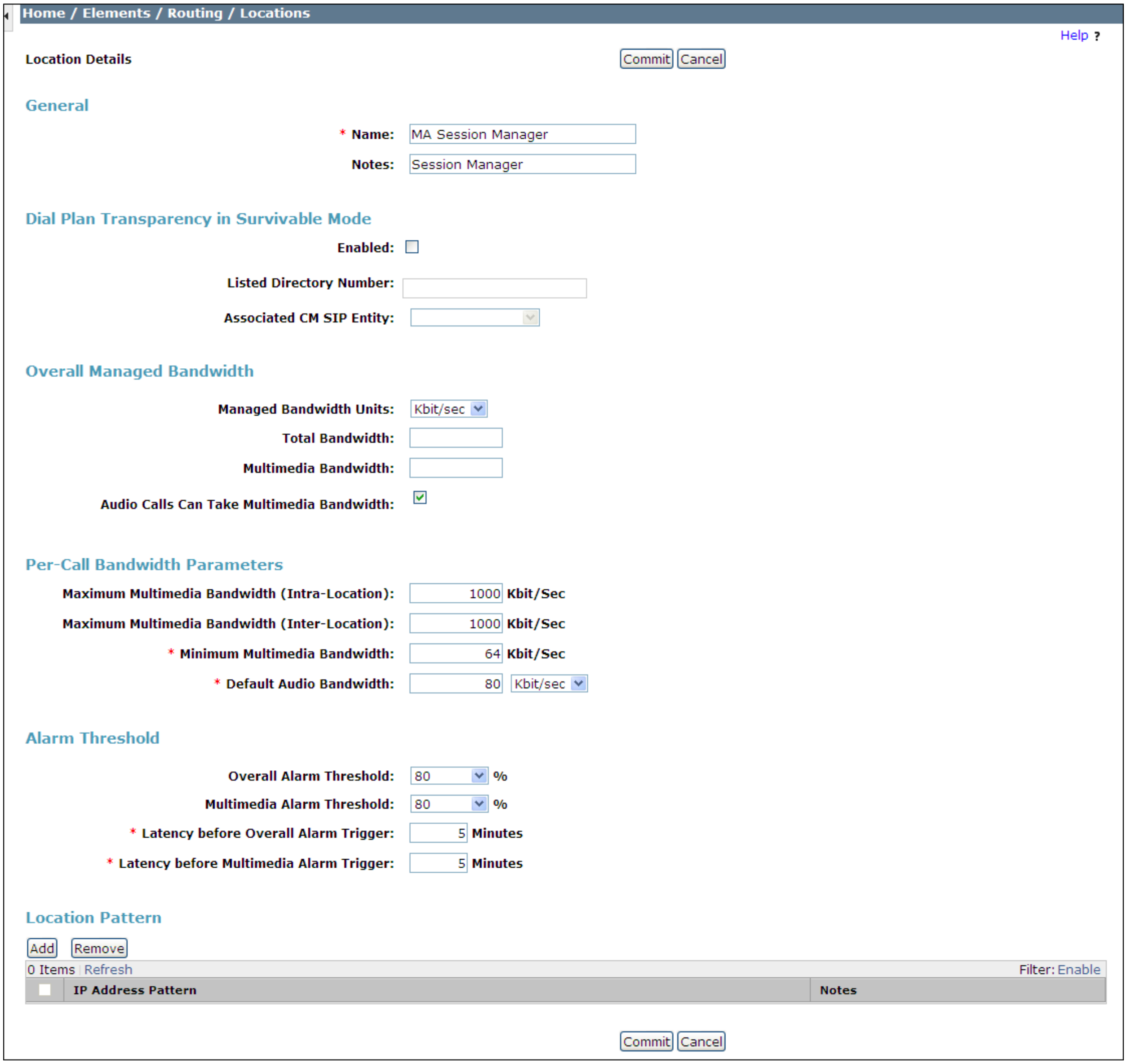
6.3. Locations

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

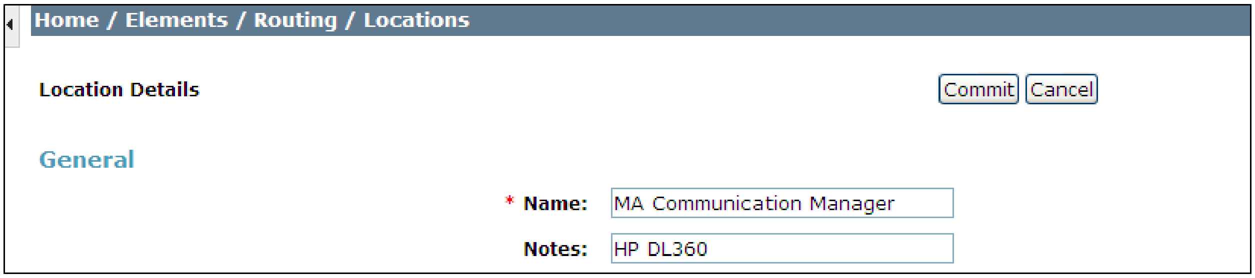
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

Defaults can be used for all other parameters.

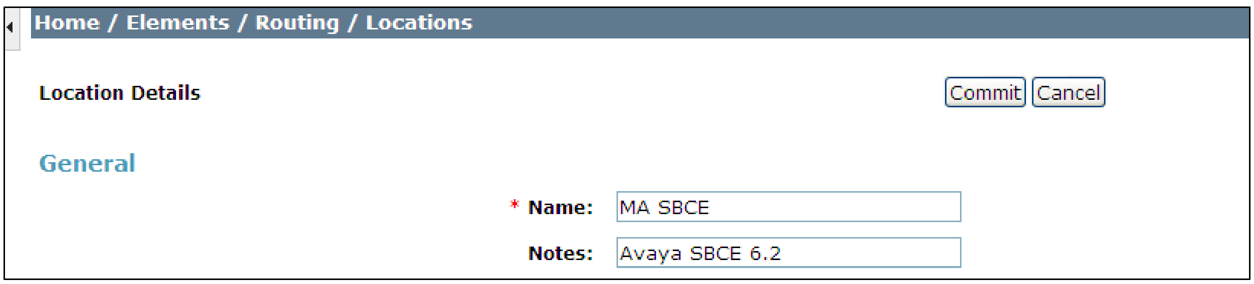
The following screen shows the location details for the location named “MA Session Manager”. Later, this location will be assigned to the SIP Entity corresponding to Session Manager.



The following screen shows the location details for the location named “MA Communication Manager”. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.



The following screen shows the location details for the location named “MA SBCE”. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

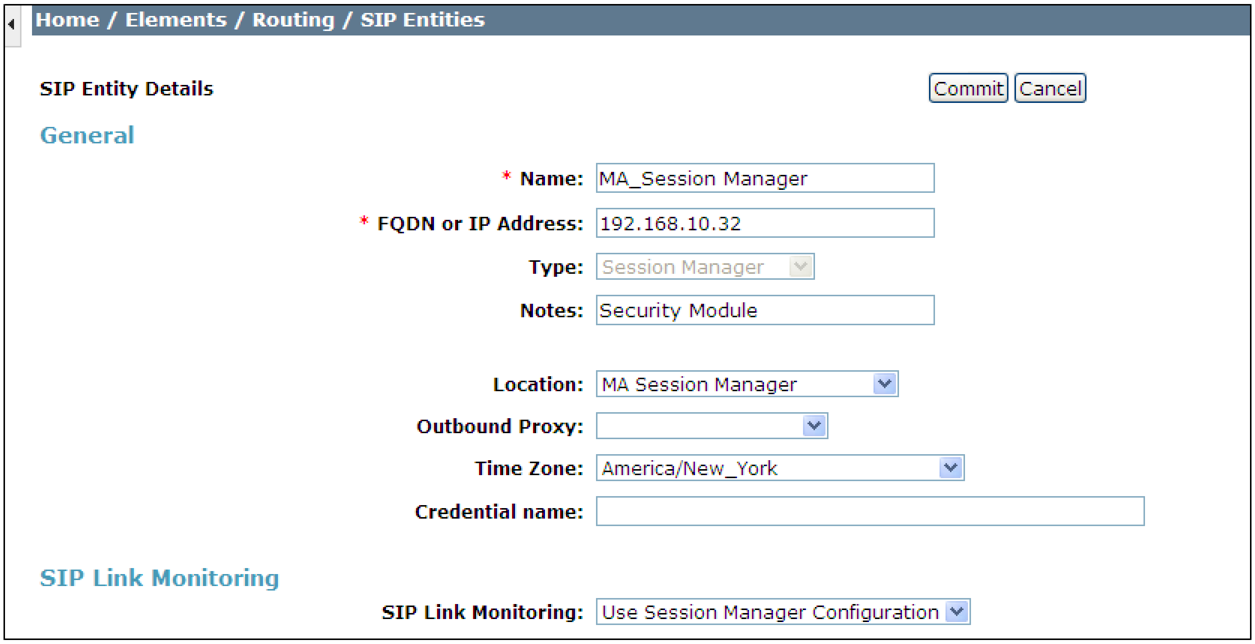


6.4. SIP Entities

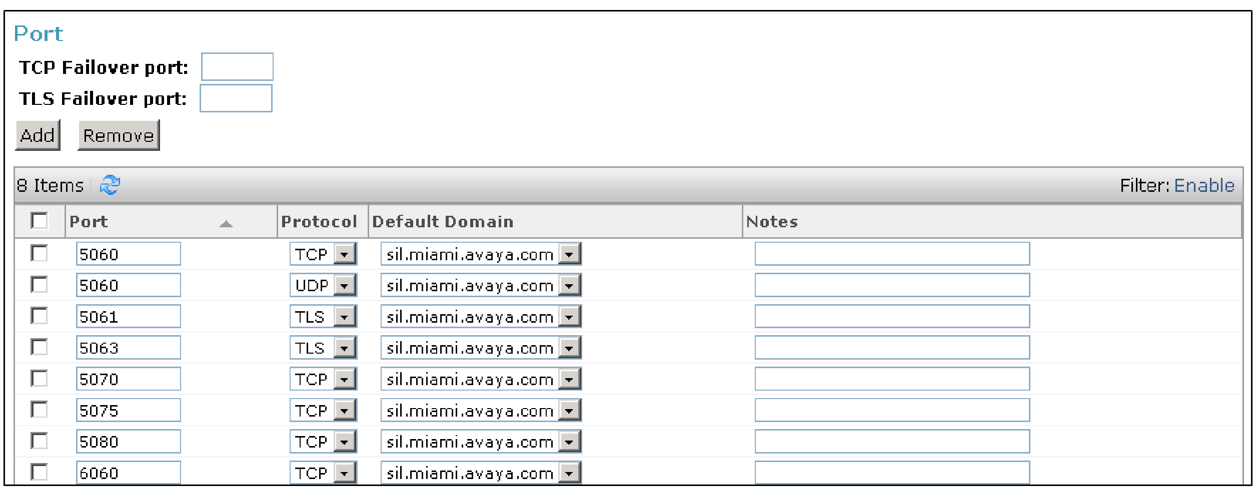
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager** If adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

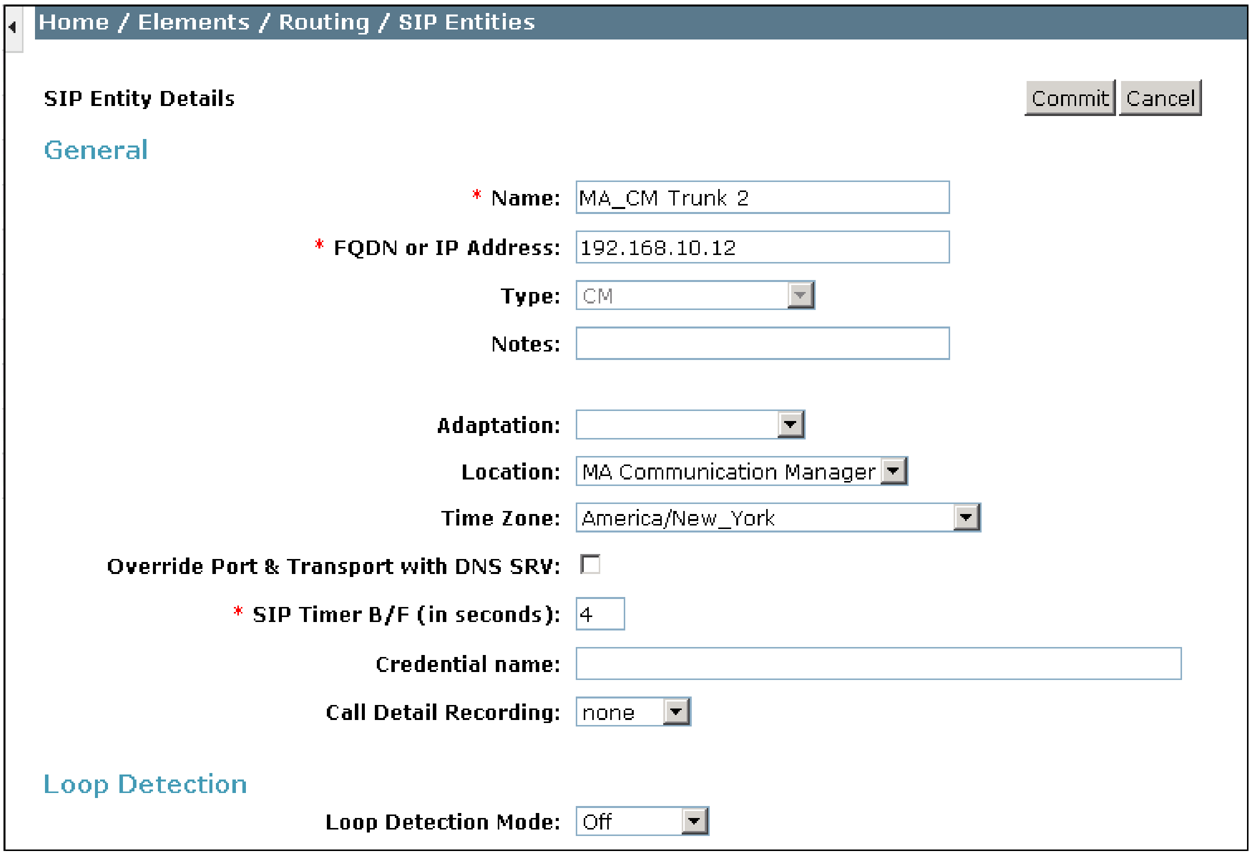
The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.



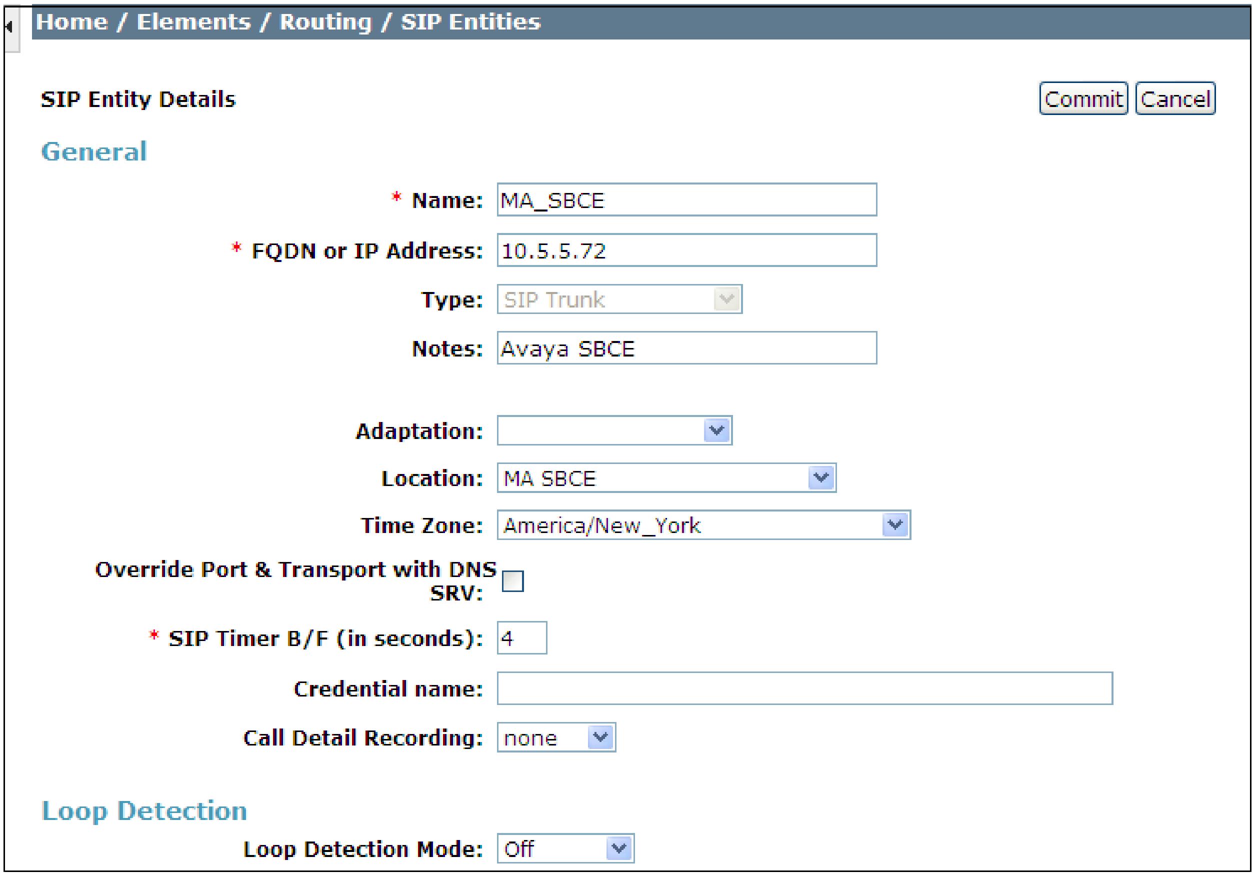
To define the ports that Session Manager will use to listen for SIP requests, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. The screen below shows the ports used by Session Manager in the shared lab environment. TLS port 5063 and TCP port 5060 are the ones directly relevant to the SIP trunk to Telesur in the reference configuration.



The following screen shows the addition of the SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the "**procr**" interface in Communication Manager, as seen in **Section 5.3**.



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



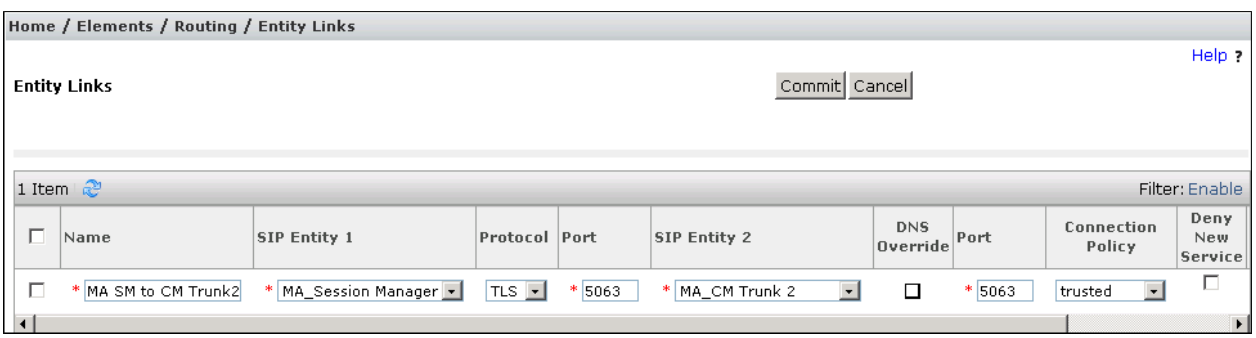
6.5. Entity Links

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

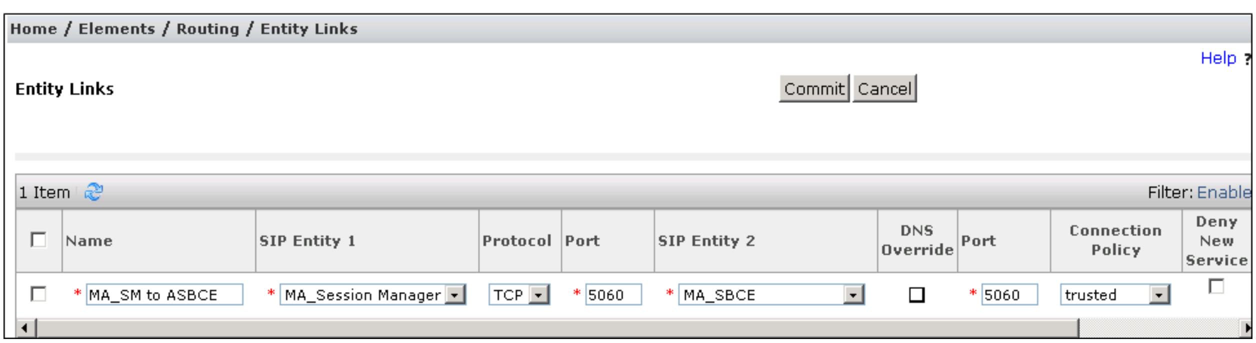
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

Click **Commit** to save.

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



Entity Link to the Avaya SBCE:

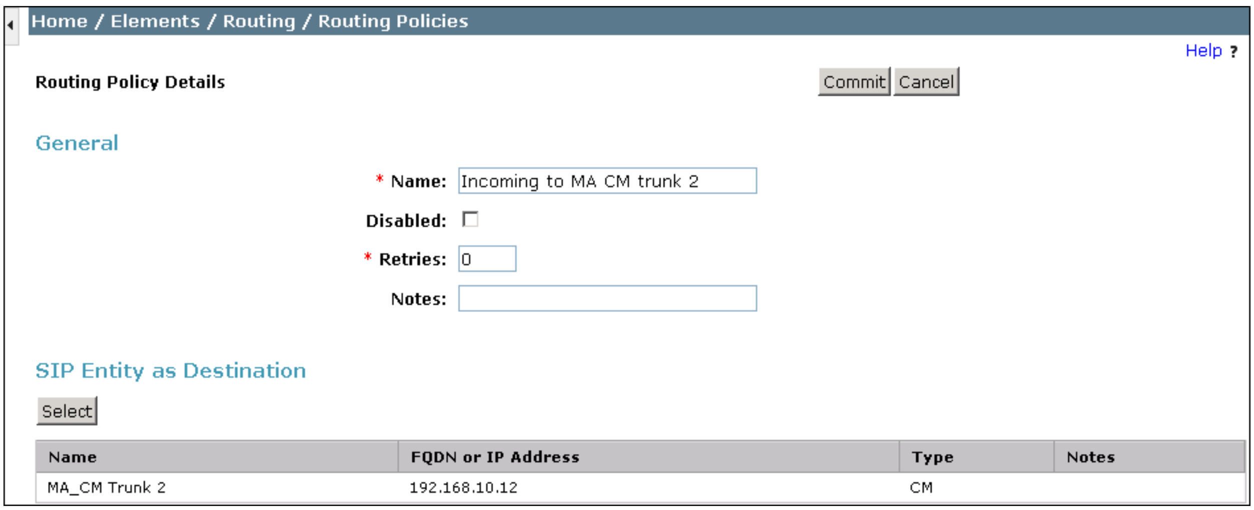


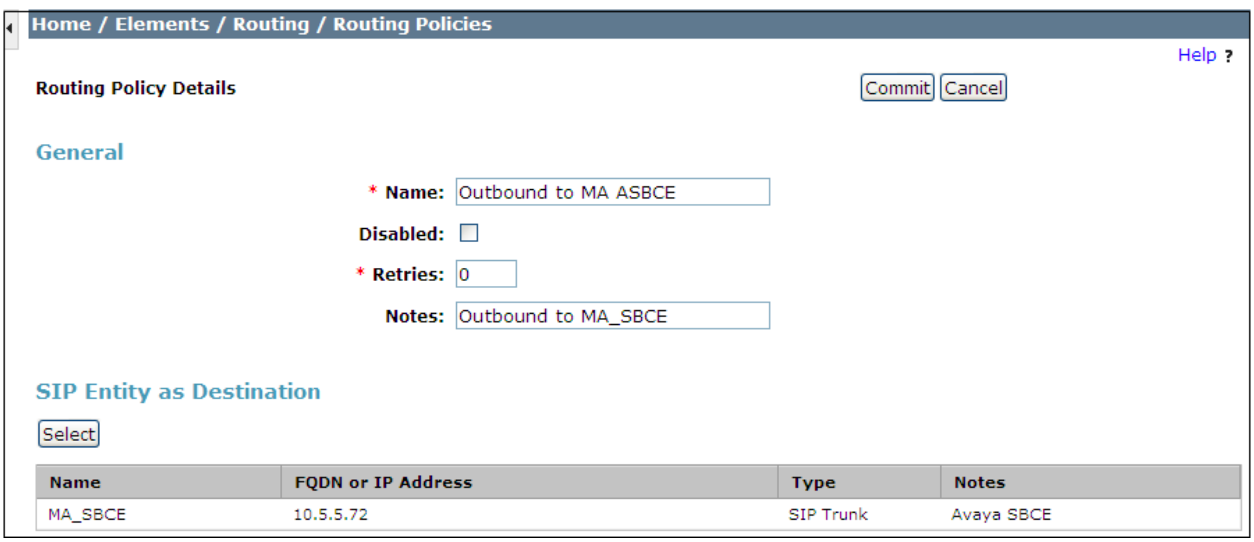
6.6. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).

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

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





6.7. Dial Patterns

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

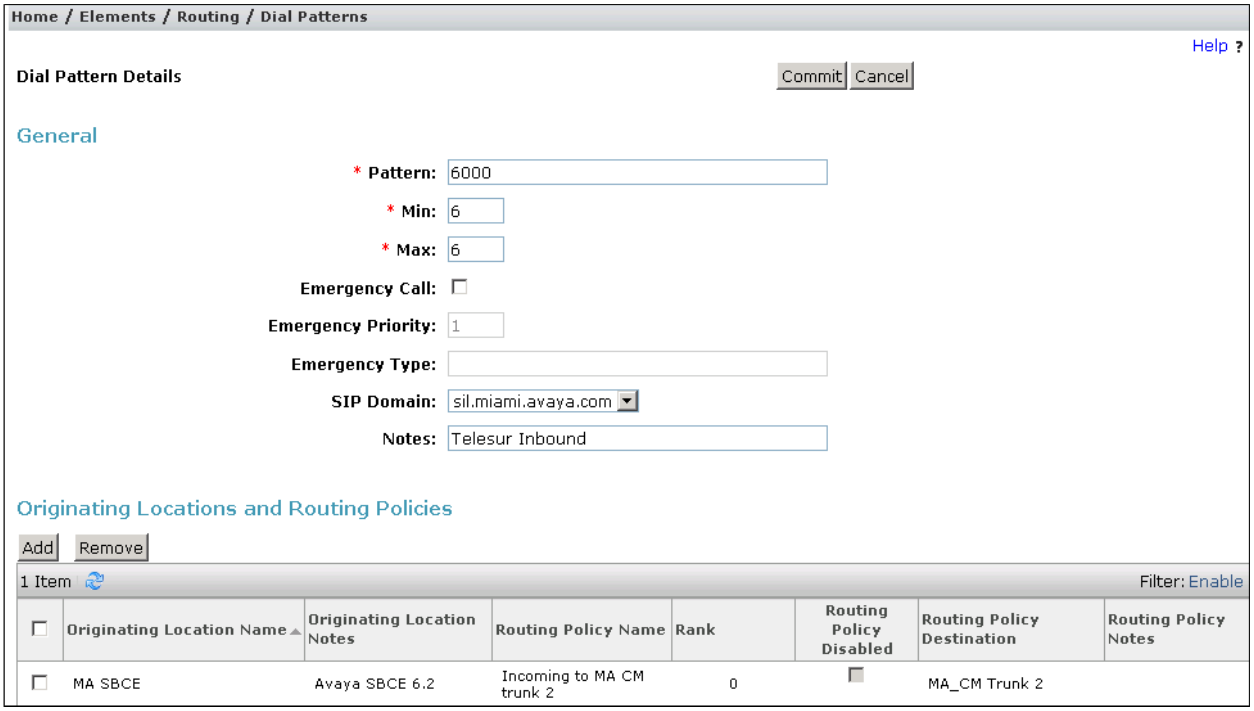
In the **General** section, enter the following values:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select "**ALL**" to route incoming calls to all SIP domains.
- **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**.

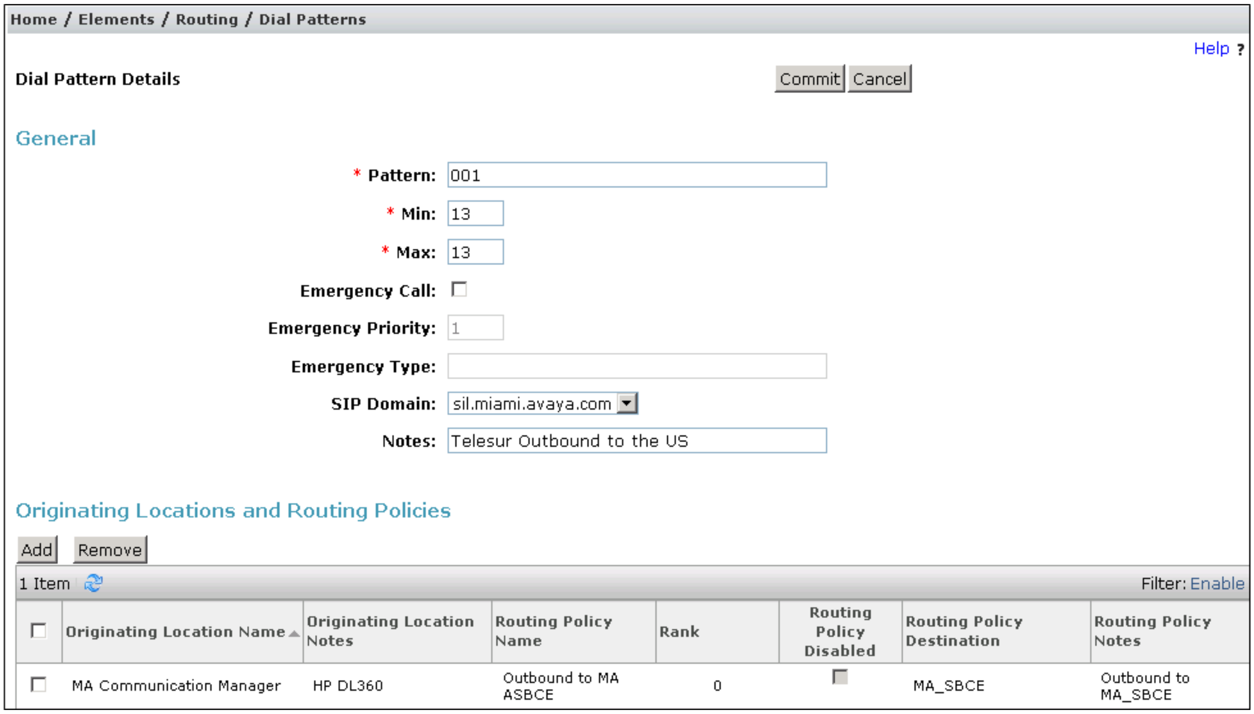
Default values can be used for the remaining fields. Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 6 digit numbers starting with ***6000***, which was the DID range of numbers assigned by Telesur to the SIP trunk, arriving from location ***MA SBCE***, used route policy ***Incoming To MA CM Trunk 2*** to Communication Manager.



Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The example in this screen shows that 13 digit dialed numbers for outbound calls, beginning with the international long distance code ***001*** used for test purposes during the compliance test, arriving from the ***MA Communication Manager*** location**,** will use route policy ***Outbound to MA ASBCE***, which sends the call out to the PSTN via Avaya SBCE and the Telesur SIP Trunk.



Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

Commit Cancel

General

* Pattern: 001

* Min: 13

* Max: 13

Emergency Call:

Emergency Priority: 1

Emergency Type:

SIP Domain: sil.miami.avaya.com

Notes: Telesur Outbound to the US

Originating Locations and Routing Policies

Add Remove

1 Item

Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
	MA Communication Manager	HP DL360	Outbound to MA ASBCE	0		MA_SBCE	Outbound to MA_SBCE

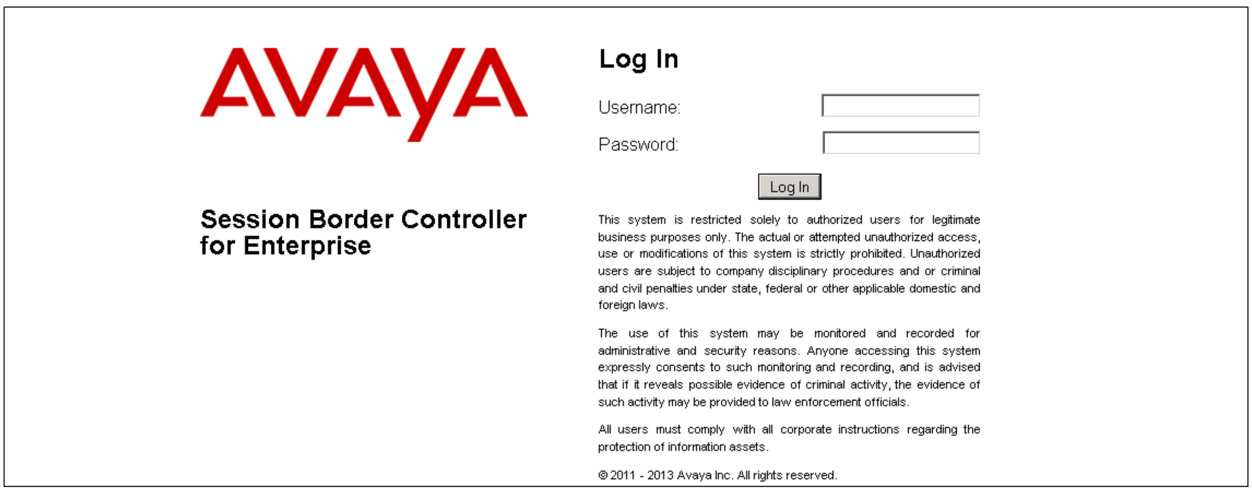
Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

7. Configure Avaya Session Border Controller for Enterprise

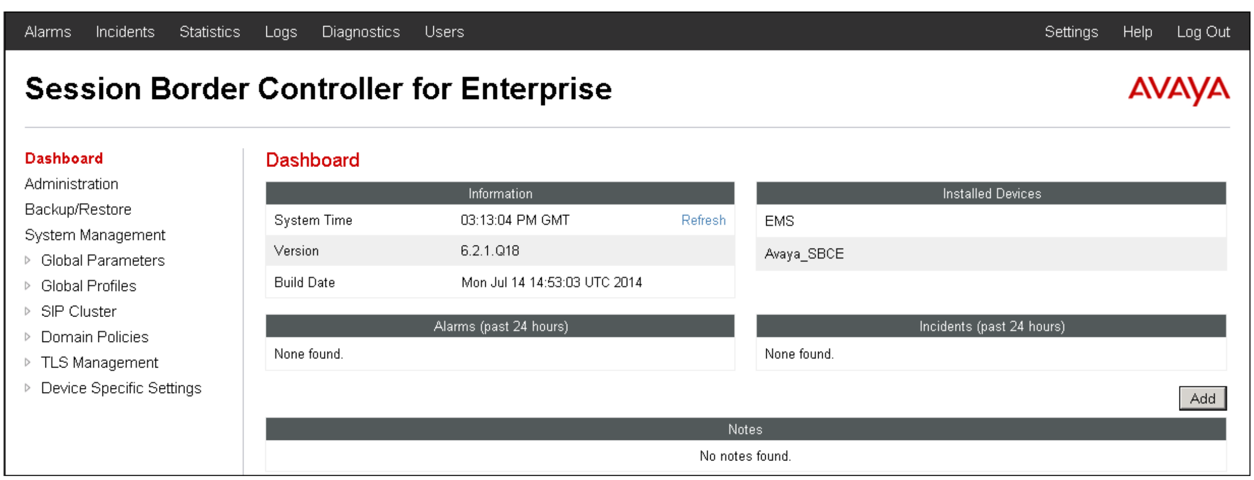
In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Telesur SIP Trunking service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For more information on the SBC installation and initial provisioning, consult the Avaya SBCE documentation listed in the **References** section.

7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.

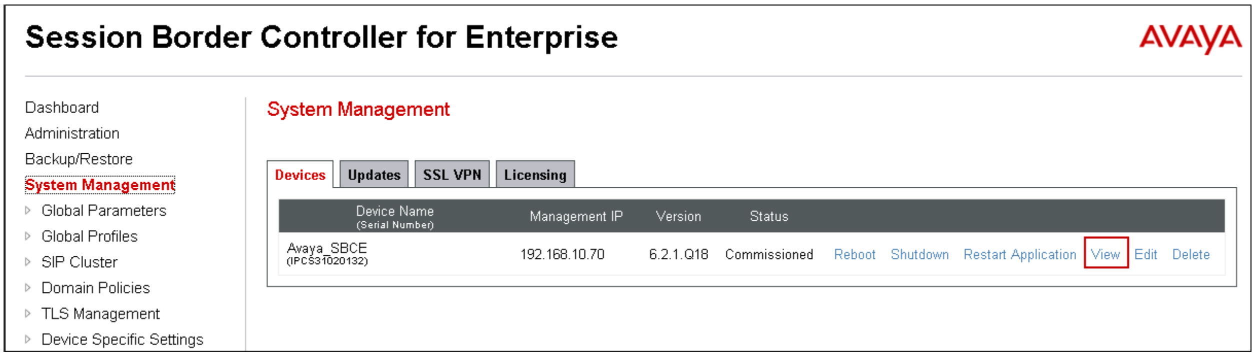


Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.

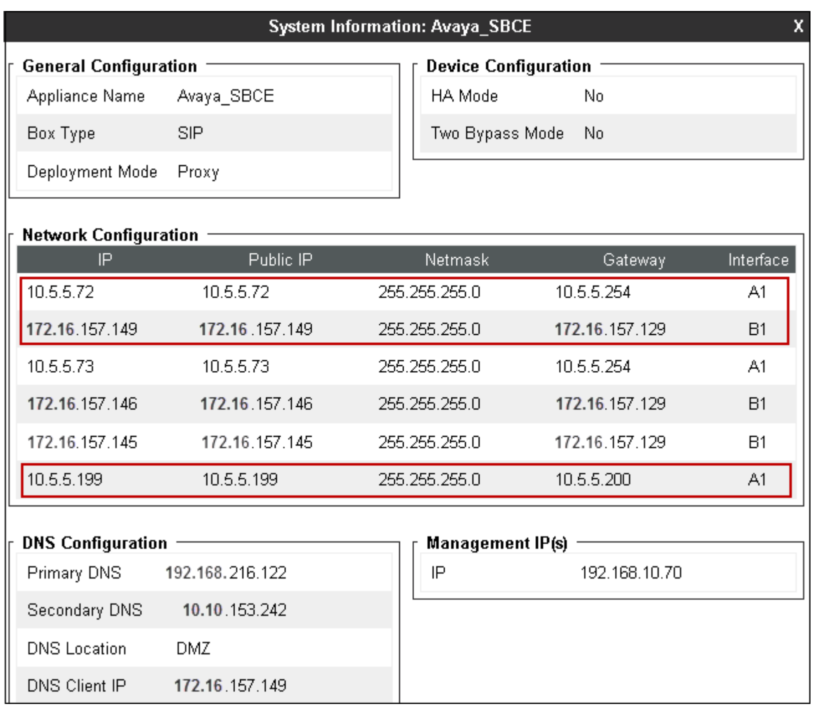


7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named **Avaya_SBCE** is shown. The management IP address that was configured during installation and the current software version are shown here. Note that the management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is ***Commissioned***, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings. Note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces for the Avaya SBCE. The highlighted **A1** and **B1** IP addresses are the ones relevant to these Application Notes. Other IP addresses assigned to these interfaces on the screen below are used to support remote workers and they are not discussed in this document.

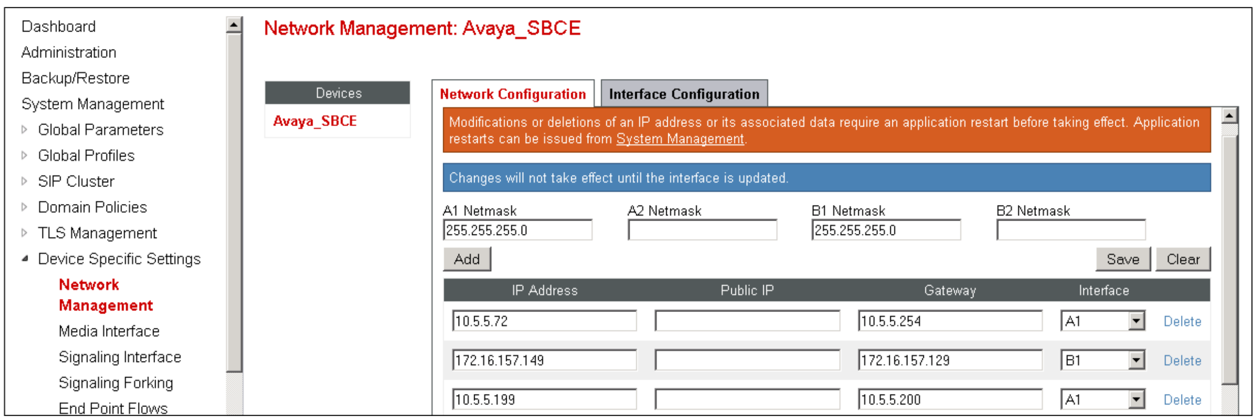


7.3. Network Management

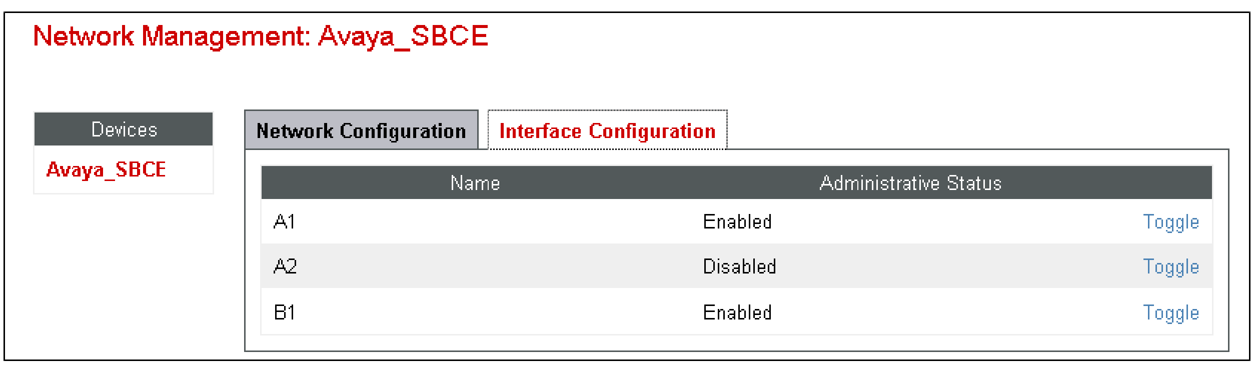
The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, **Avaya_SBCE** in the sample configuration. On the **Network Configuration** tab, verify or enter the network information as needed. Note that the **A1** and **B1** interfaces correspond to the private and public interfaces for the Avaya SBCE.

In the configuration used during the compliance test, two IP addresses were assigned to interface **A1**. IP address **A1:10.5.5.72** was used to handle both signaling and media traffic on the private enterprise network. SIP signaling traffic on the SIP trunk was routed via interface **A1:10.5.5.199** to a VPN gateway, and ultimately to Telesur via a VPN IPsec tunnel over the public Internet. RTP media traffic on the SIP trunk was routed through interface **B1:172.16.157.149** directly over the Internet. See **Figure 1** on **Section 3**.



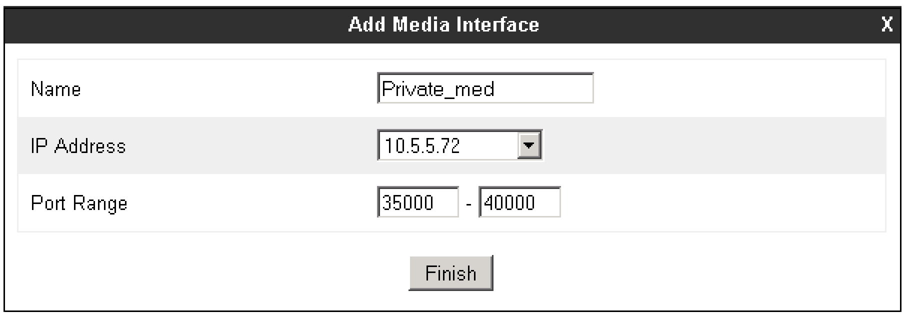
On the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. Click the **Toggle** buttons if necessary to enable the interfaces.



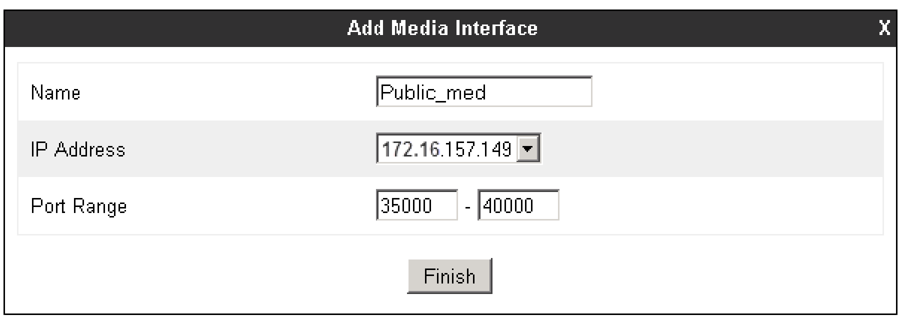
7.4. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call or the Trunk Server.

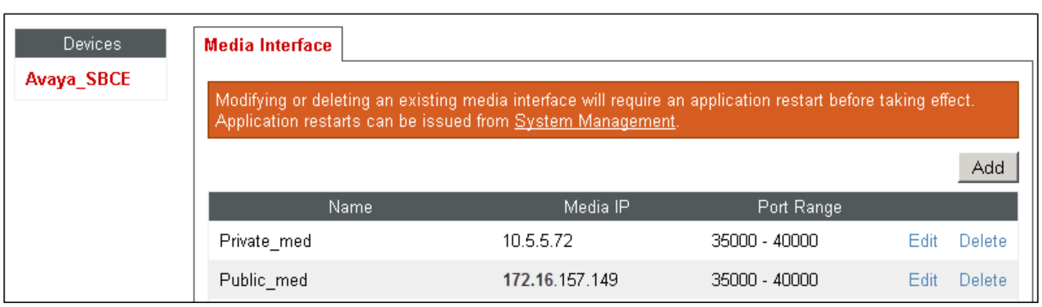
To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the private IP Address for the Avaya SBCE facing the enterprise network from the **IP Address** drop-down menu. The **Port Range** was left at the default values of ***35000-40000***. Click **Finish**.



A Media Interface facing the public network side was similarly created with the name **Public_med**, as shown below. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was left at the default values. Click **Finish**.



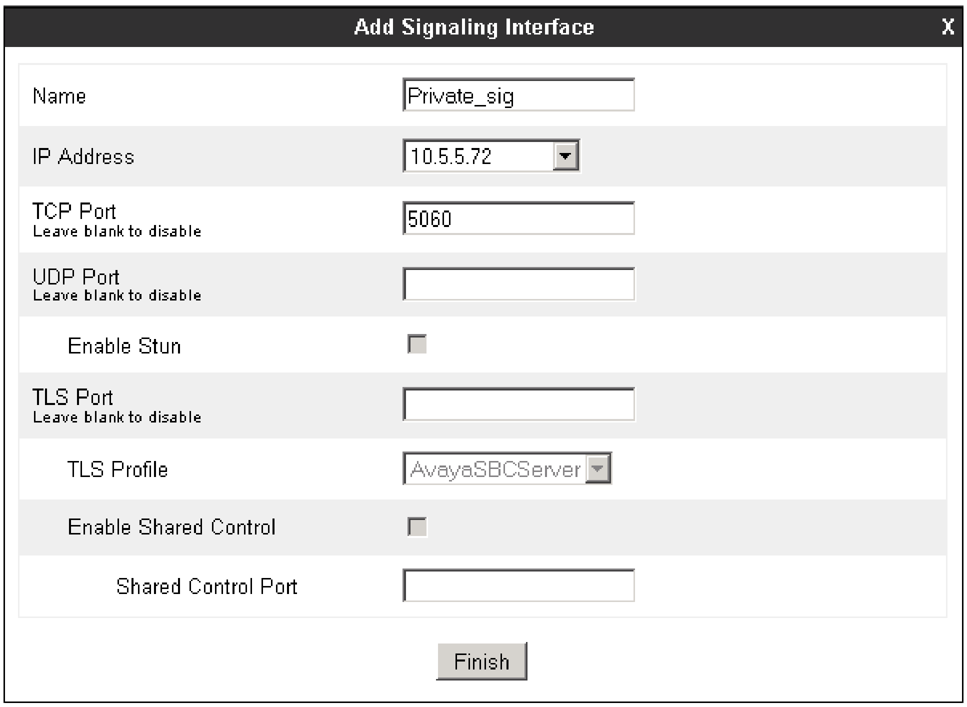
Once the configuration is completed, the **Media Interface** screen will appear as follows.



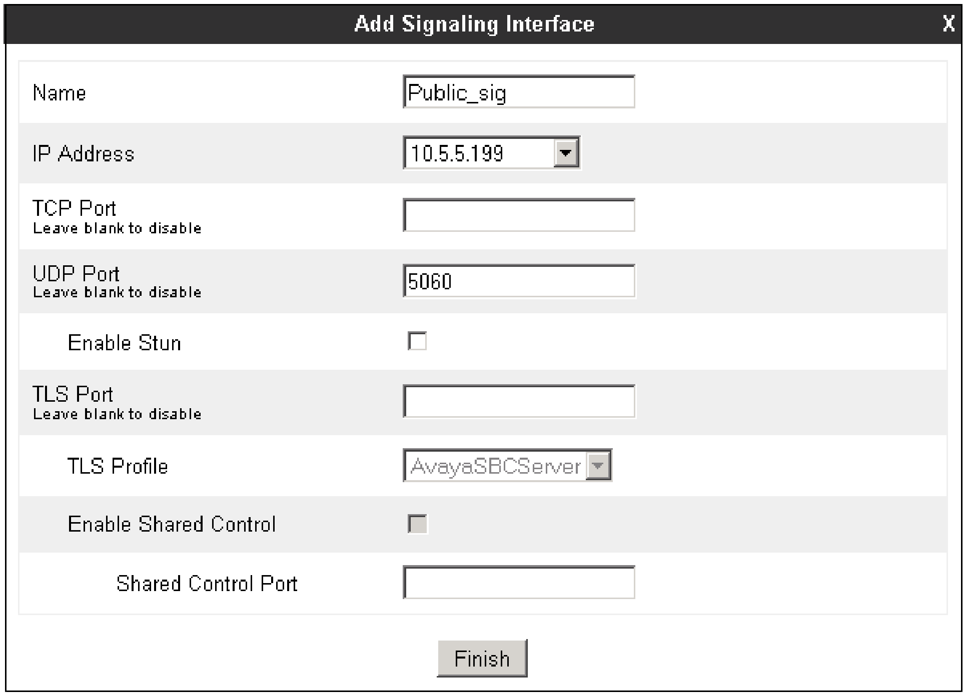
7.5. Signaling Interfaces

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

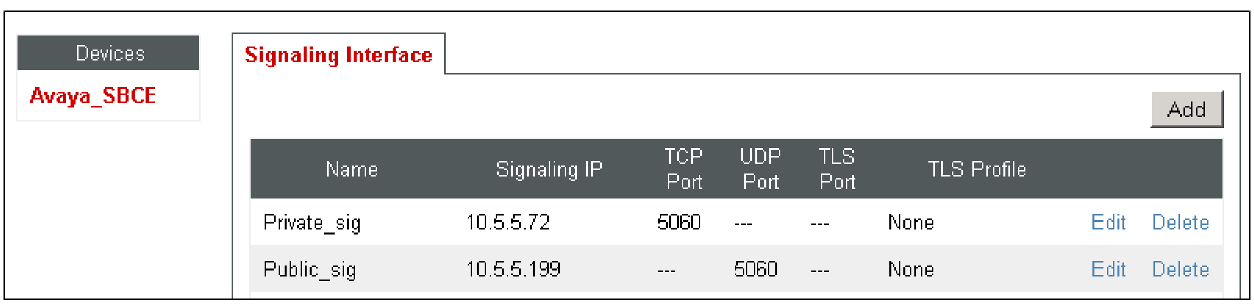
To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address of the Avaya SBCE facing the enterprise network from the **IP Address** drop-down menu. Enter ***5060*** for **TCP Port**, since TCP port 5060 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.5**. Click **Finish**.



A second Signaling Interface with the name **Public_sig** was similarly created in the service provider's direction. The private IP Address of the Avaya SBCE facing the service provider (via VPN gateway in the reference configuration) was selected from the **IP Address** drop-down menu. Enter ***5060*** for **UDP Port**. Click **Finish**.



Once the configuration is completed, the **Signaling Interface** screen will appear as follows:

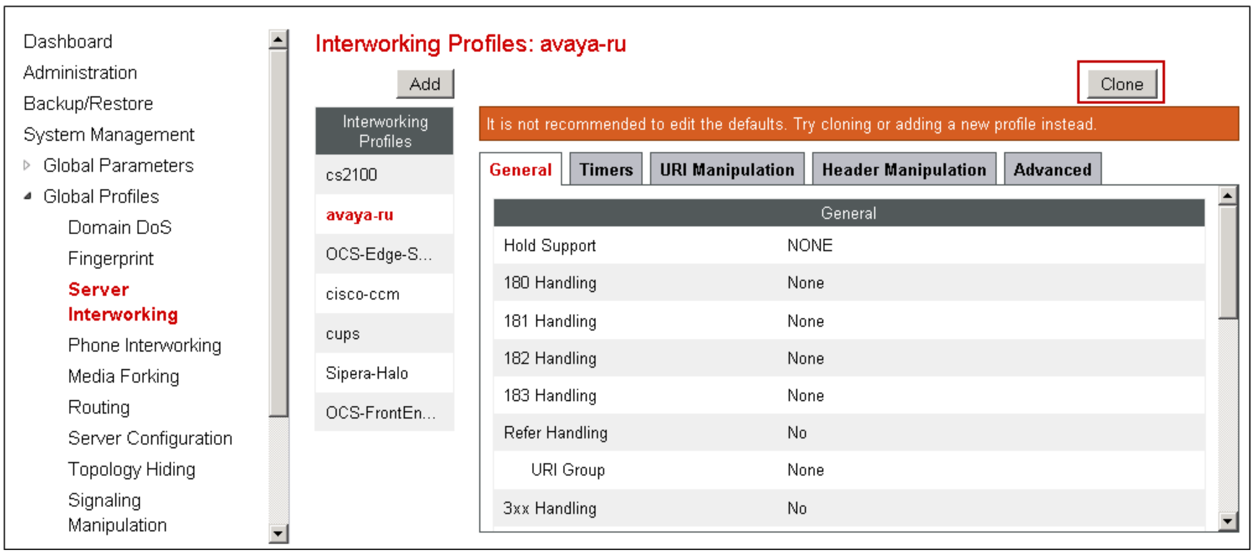


7.6. Server Interworking

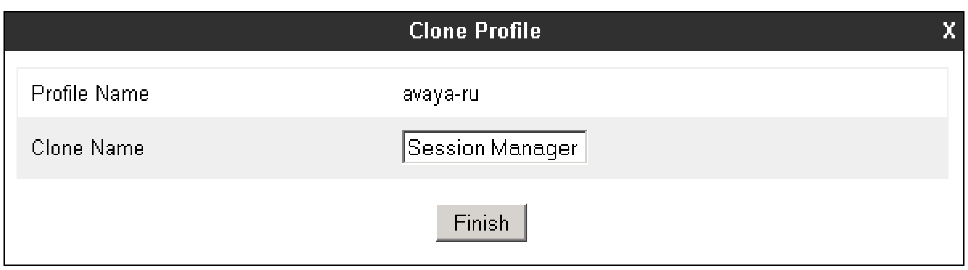
Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server). In the reference configuration, Session Manager functions as the Call Server and the Telesur SIP Proxy as the Trunk Server.

7.6.1. Server Interworking Profile – Session Manager

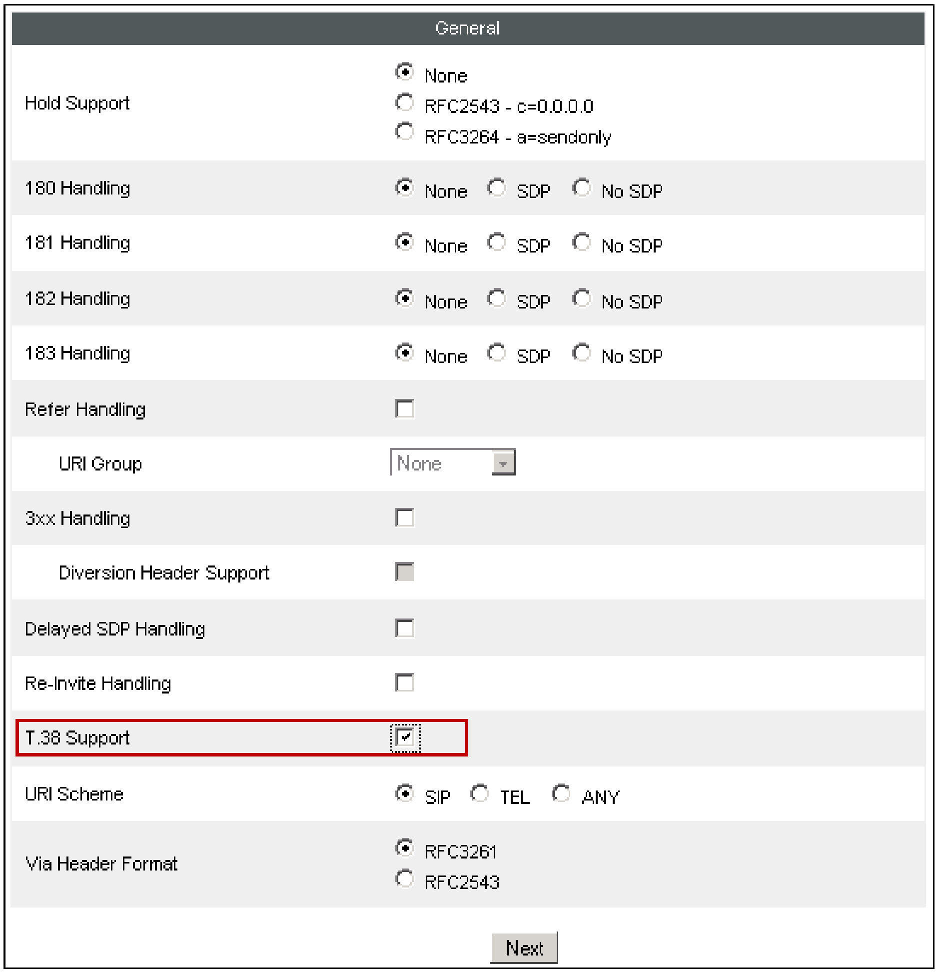
Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select ***avaya-ru*** from the list of pre-defined profiles. Click **Clone**.



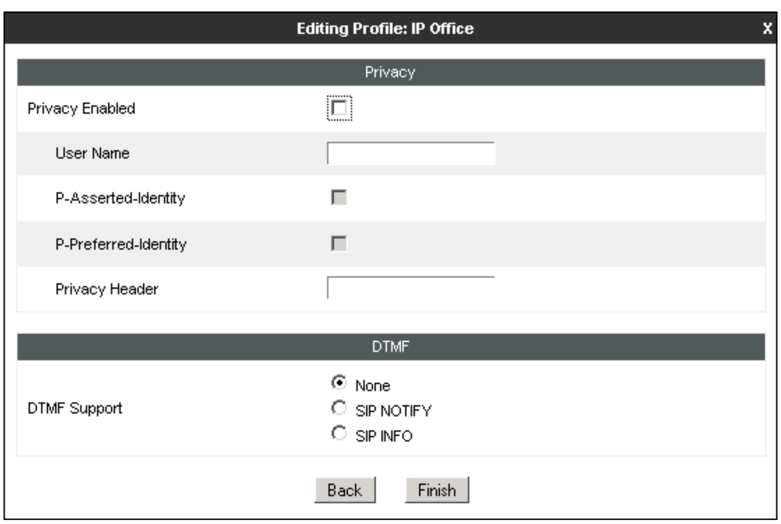
Enter a descriptive name for the cloned profile. Click **Finish**.



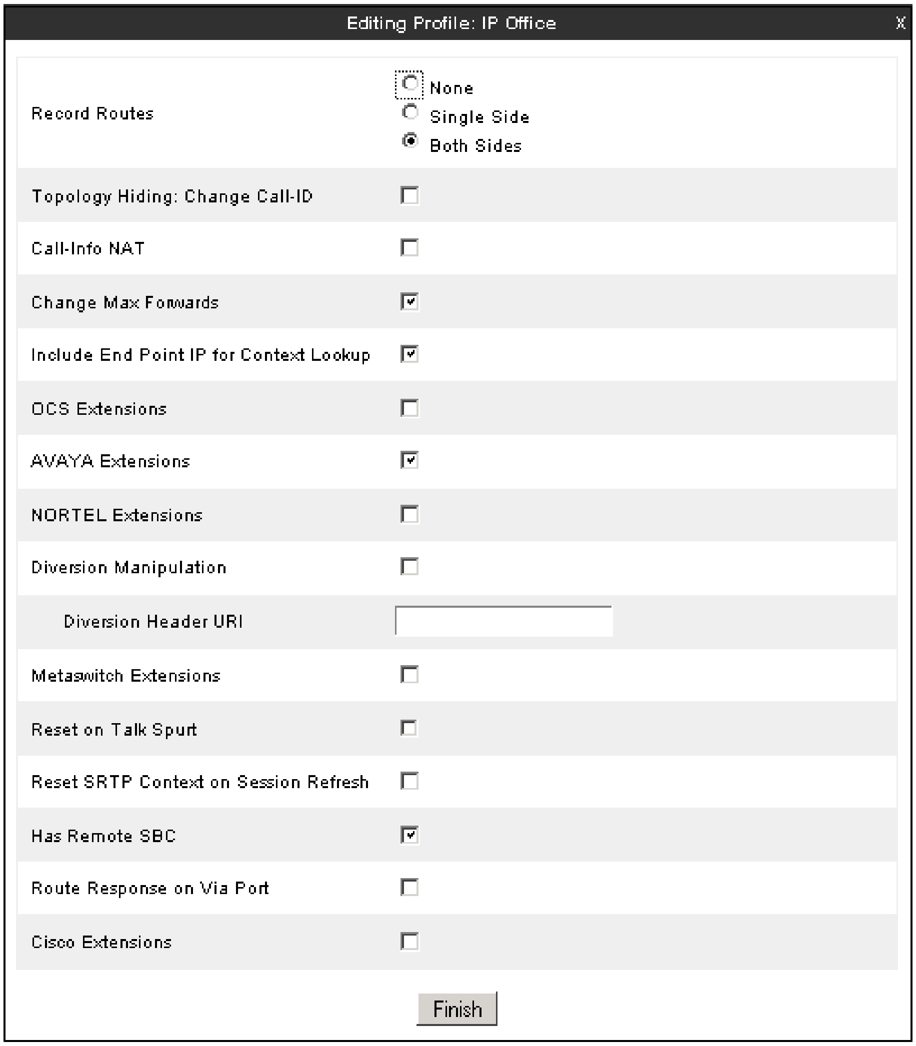
On the newly cloned ***Session Manager*** interworking profile, scroll down on the **General** tab and click **Edit** (not shown). On the **General** screen, check the **T.38 Support** box. All other parameters retain their default values. Click **Next**.



On the **Privacy/DTMF** screen, keep all the default settings. Click **Finish**.

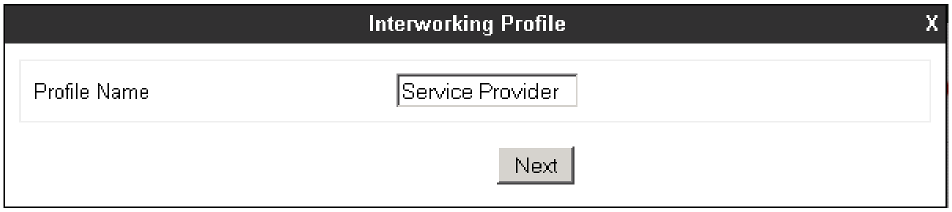


Select the **Advanced** tab. It should look like the screen below:

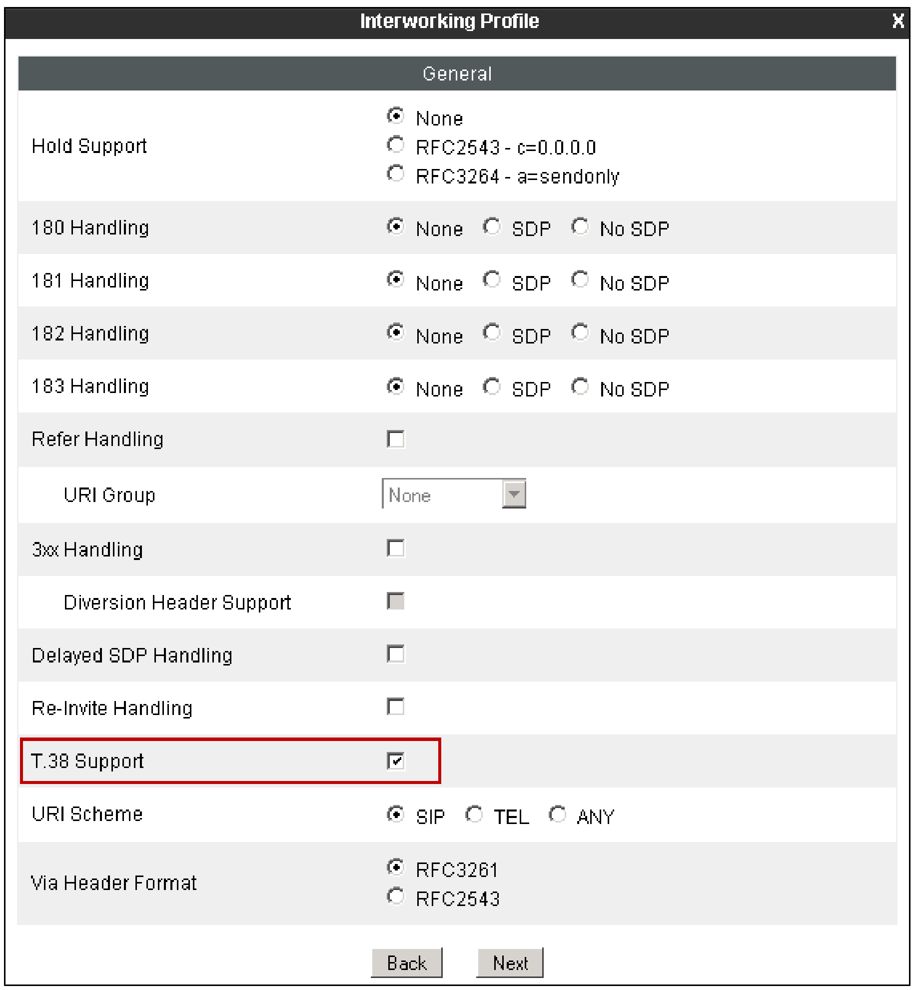


7.6.2. Server Interworking Profile – Service Provider

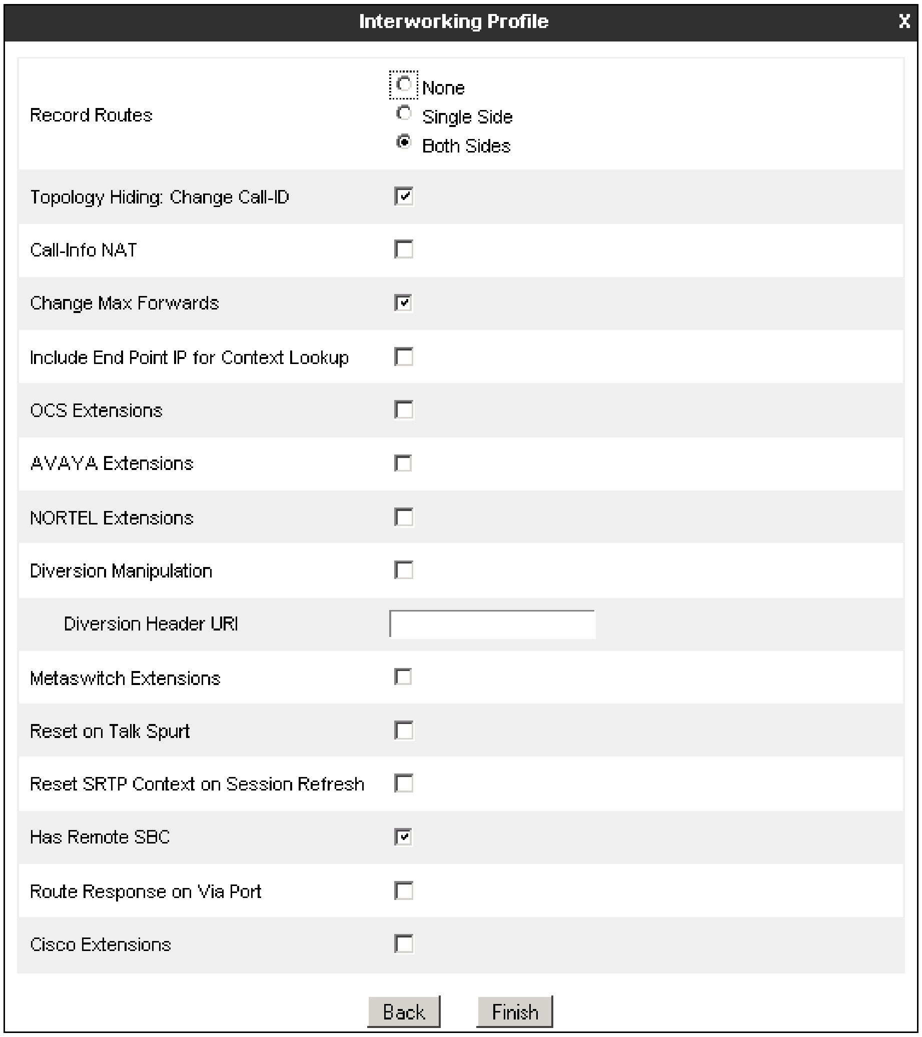
A second interworking profile in the direction of the SIP trunk to Telesur was created, by adding a new profile in this case. Select **Global Profiles** → **Server Interworking** on the left navigation pane and click **Add** (not shown). Enter a descriptive name for the new profile. Click **Next**.



On the **General** tab, default values were used for all parameters except for **T.38 Support**, which was enabled. Click **Next**.



Click **Next** on the **Privacy/DTMF** and **SIP Timers/Transport Timers** tabs (not shown). Accept all defaults in the **Advanced Settings** tab. Click **Finish**.



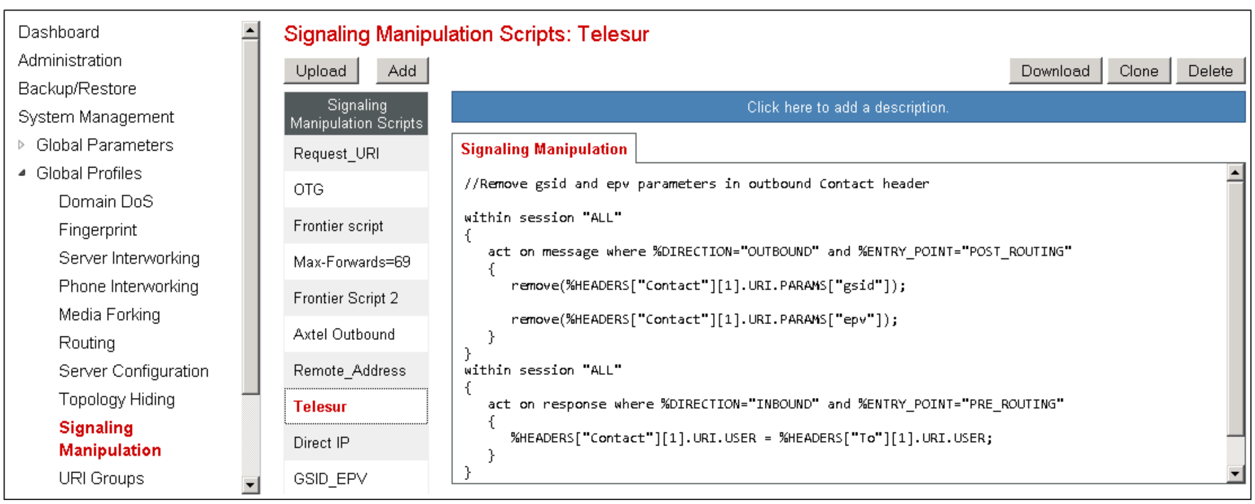
7.7. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform a granular header manipulation on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Sigma Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult **[5]** in the **References** section for more information on this topic.

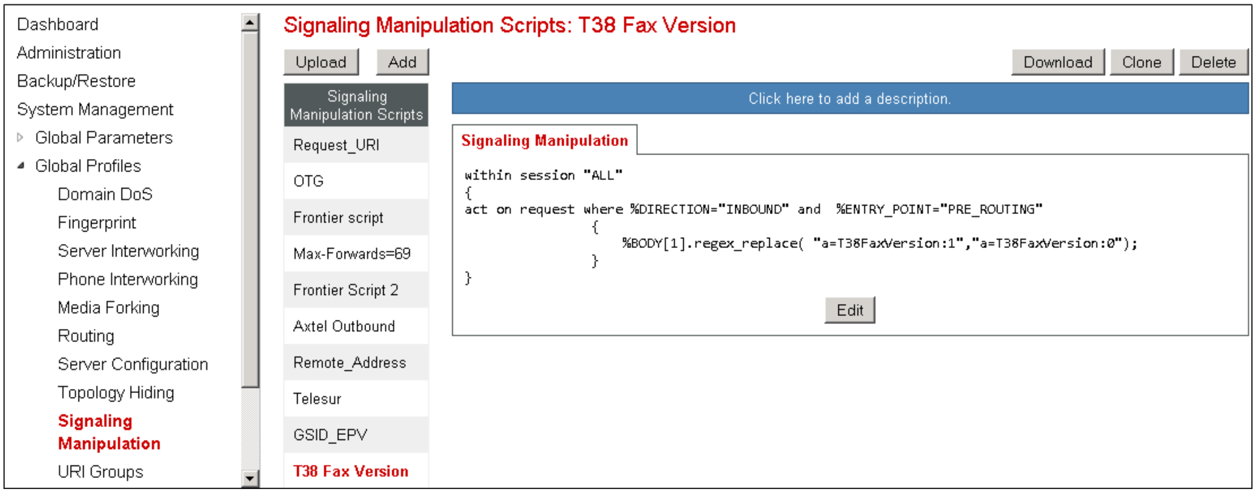
To add a Signaling Manipulation script, from the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click **Add** to open the SigMa Editor screen, where the text of the script can be entered.

The screen below shows the finished Signaling Manipulation script named ***Telesur*** created during the compliance test. This script named was used to remove the “gsid” and “epv” parameters from outbound Contact headers. These parameters add unnecessary size to outbound messages and have no significance to the service provider. Additionally, the script was used to manipulate the Contact header in responses received from Telesur, as a workaround to the issue of incorrect telephone numbers shown on enterprise extensions displays on outbound calls, as mentioned in **Section 2.2**.



Note: Additional Avaya SBCE header manipulation was performed to remove unnecessary headers from outbound messages, by implementing Signaling Rules in **Section 7.11**.

The screen below shows the finished script named ***T38 Fax Version***. This script was used to manipulate the "T38FaxVersion" parameter contained on the SDP of T.38 re-INVITES sent by Communication Manager during inbound fax calls, enabling in this way the successful negotiation of T.38 Fax Version 0, which was the only version acceptable to the Telesur softswitch, as mentioned in **Section 2.2**.



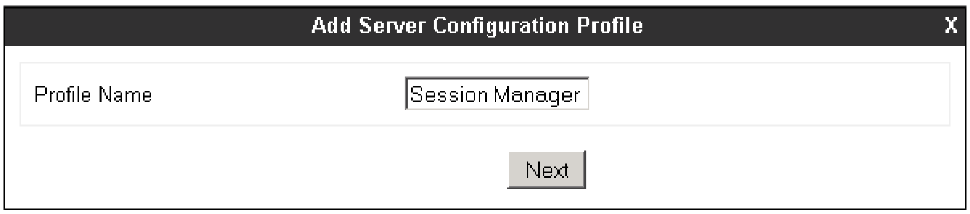
The details of the two scripts used in the compliance test can be found in **Appendix A** in this document.

7.8. Server Configuration

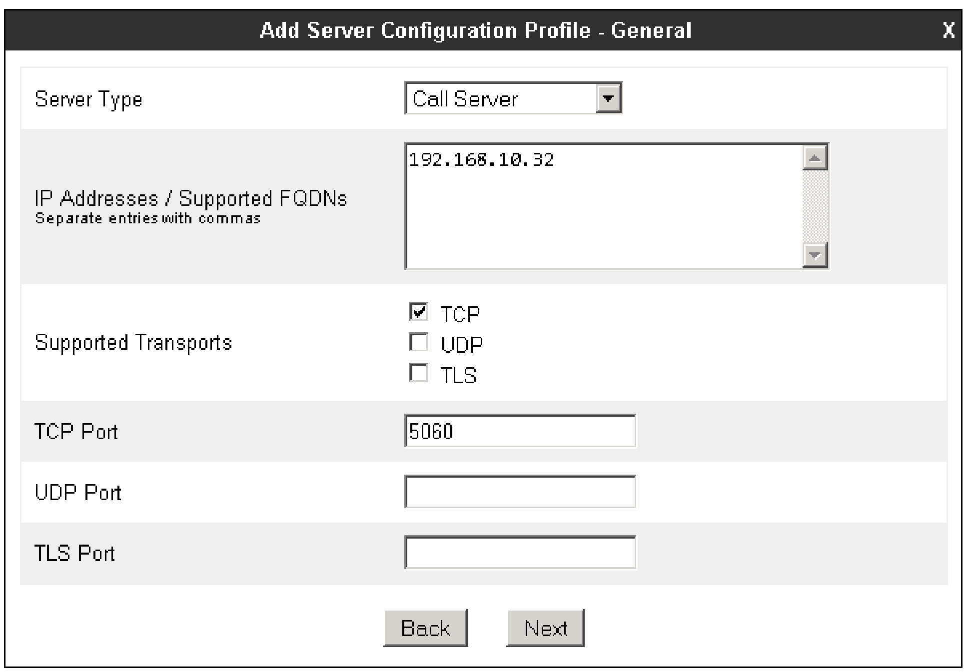
Server Profiles are created to define the parameters for the Avaya SBCE two peers, i.e., Session Manager (Call Server) and the SIP Proxy at the service provider's network (Trunk Server).

7.8.1. Server Configuration Profile – Session Manager

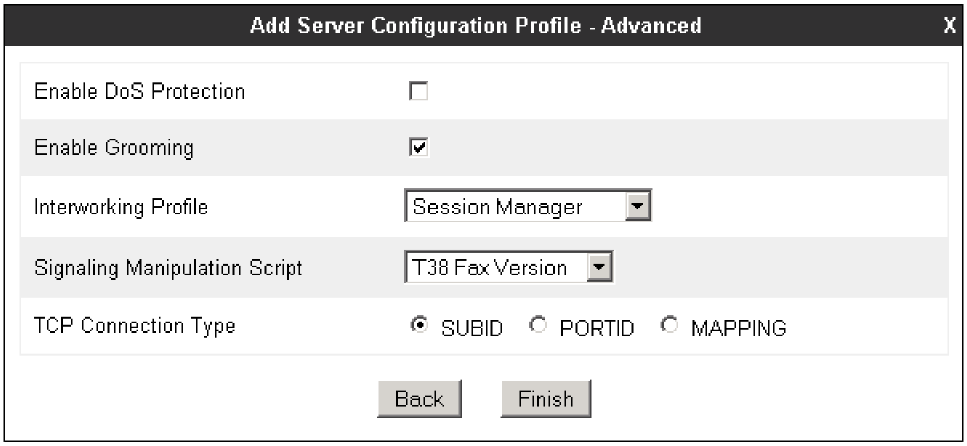
From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server. Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



On the **Add Server Configuration Profile - General** Tab select ***Call Server*** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field**,** enter the IP address of the Session Manager Security Module. Select **TCP** for **Supported Transports**, and enter ***5060*** under **TCP Port**. The transport protocol and port selected here must match the values defined for the Session Manager SIP Entity previously in **Section 6.4**. Click **Next**.

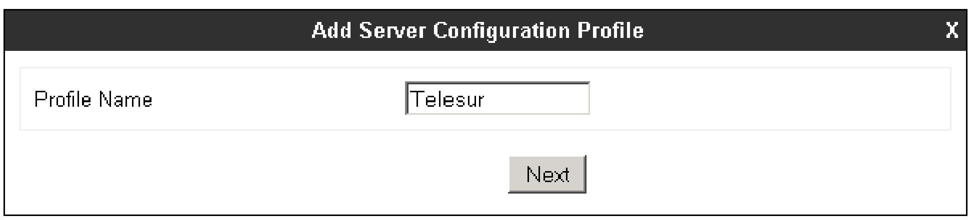


Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, since TCP is used, check the **Enable Grooming** box. Select ***Session Manager*** from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the ***T38 Fax Version*** script created in **Section 7.7**. Click **Finish**.

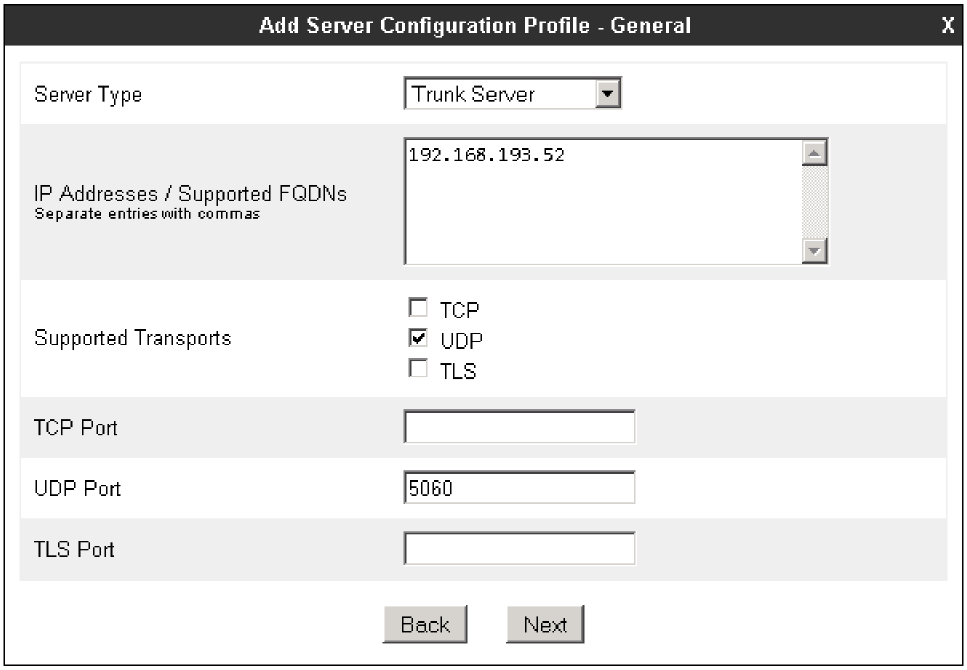


7.8.2. Server Configuration Profile – Service Provider

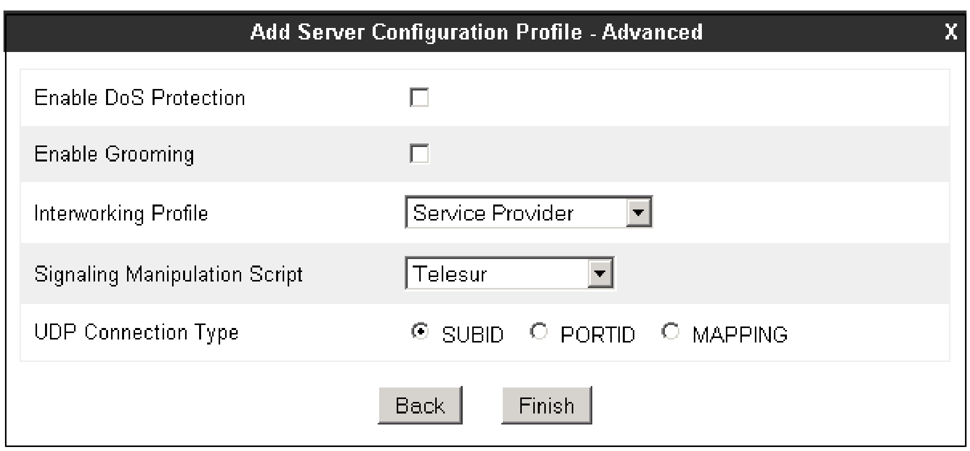
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



On the **Add Server Configuration Profile-General** Tab select ***Trunk Server*** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter ***192.168.193.52***, the IP Address of the Telesur SIP proxy server. Select **UDP** for **Supported Transports**, and enter ***5060*** under **UDP Port**, as specified by Telesur.



Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, select ***Service Provider*** from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the ***Telesur*** script created in **Section 7.7**. Click **Finish**.

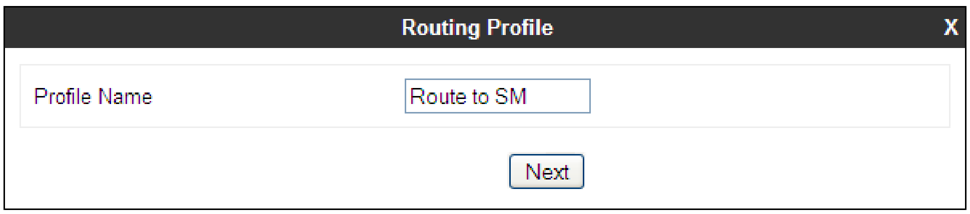


7.9. Routing

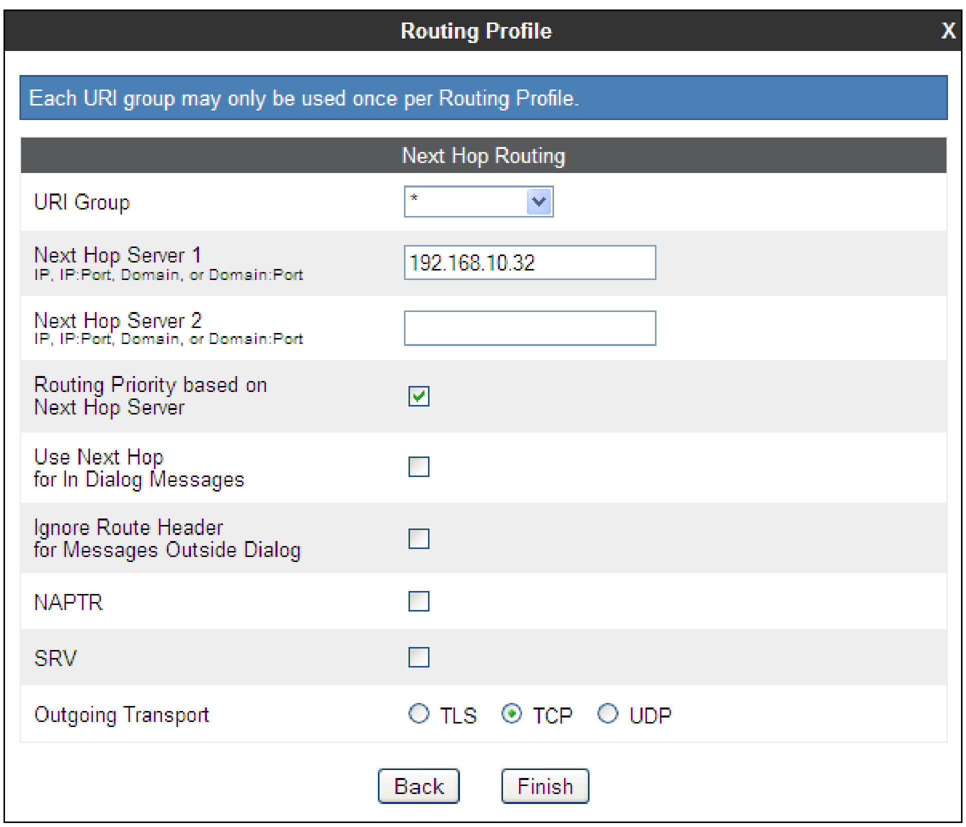
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the Telesur SIP trunk.

7.9.1. Routing Profile – Session Manager

To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown). Enter an appropriate **Profile Name** similar to the example below. Click **Next.**

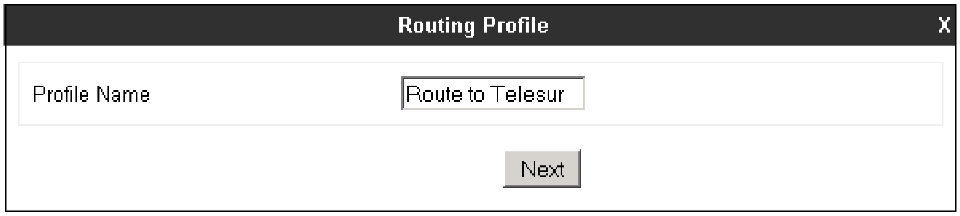


On the **Next Hop Routing** tab, enter the IP Address of Session Manager as **Next Hop Server 1**. Since the default well-known port value of 5060 for TCP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **TCP** for **Outgoing Transport**. Click **Finish**.

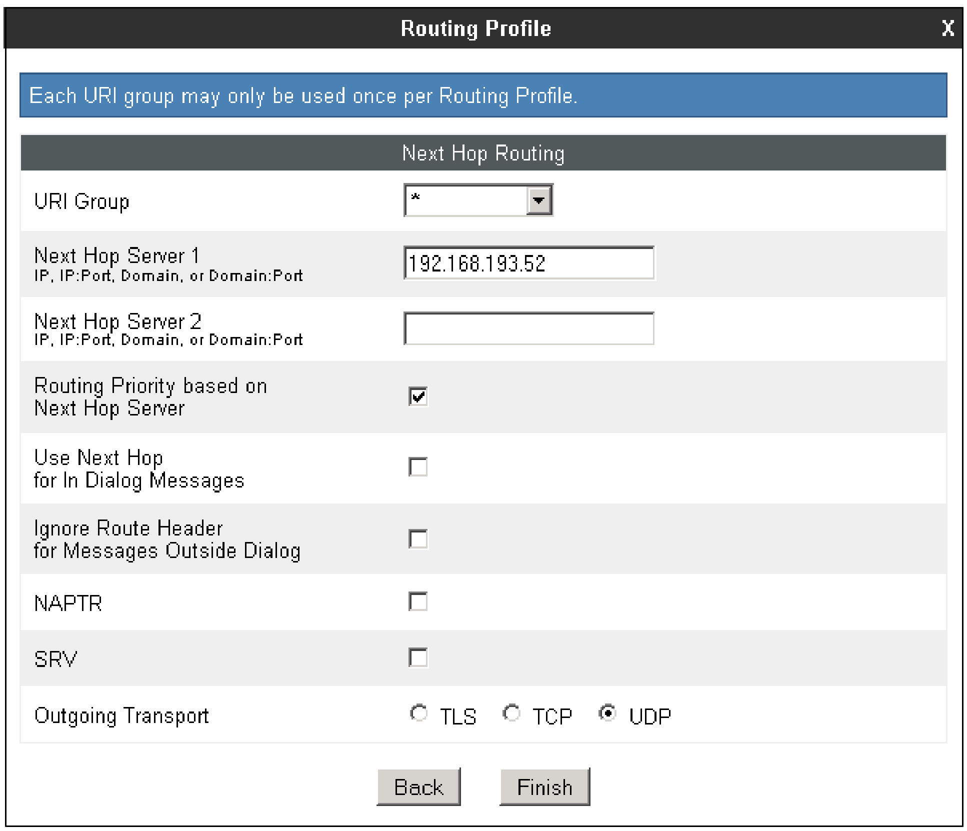


7.9.2. Routing Profile – Service Provider

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route. Enter an appropriate **Profile Name** similar to the example below. Click **Next.**



On the Next Hop Routing tab, under **Next Hop Server** 1, enter the IP Address of the service provider's SIP proxy server. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**. Click **Finish**.



7.10. Topology Hiding

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

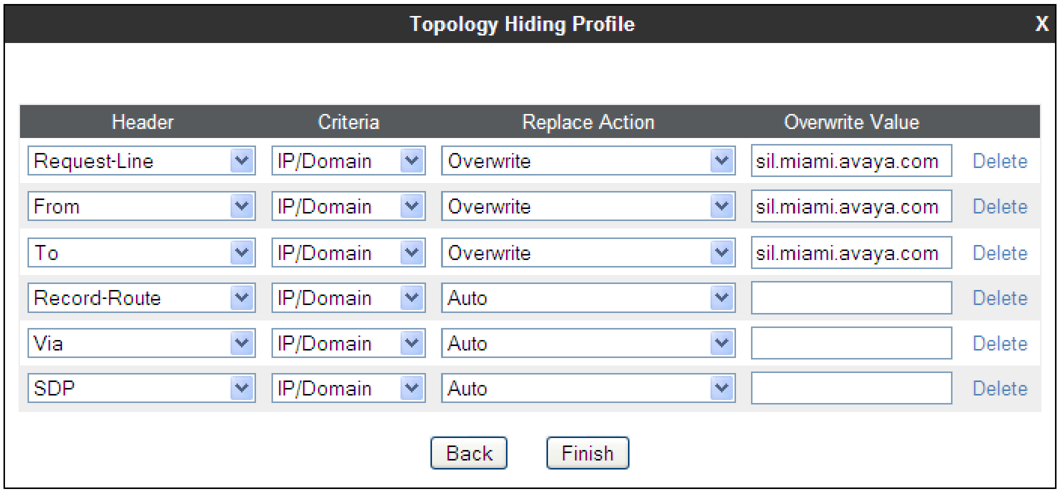
Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

7.10.1. Topology Hiding Profile – Session Manager

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side and click the **Add** button (not shown). Enter a **Profile Name** such as the one shown below. Click **Next**.

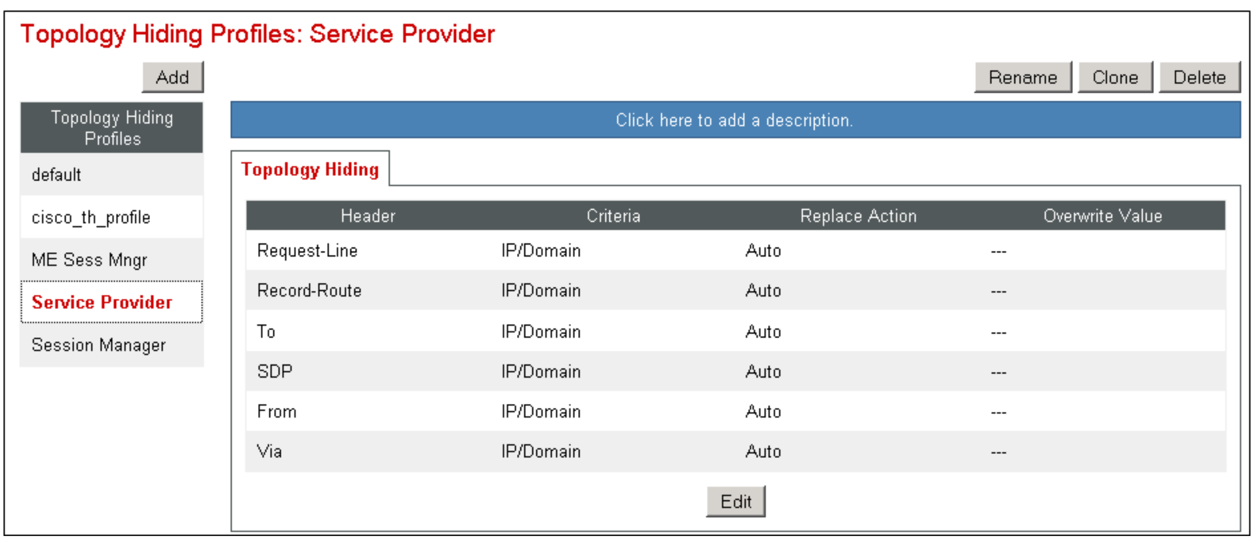
On the **Topology Hiding Profile** screen, click the **Add Header** button repeatedly to show the rest of the headers in the profile.

For the **Request-Line**, **From** and **To** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***sil.miami.avaya.com***, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**. Default values were used for all other fields. Click **Finish**.



7.10.2. Topology Hiding Profile – Service Provider

A Topology Hiding profile named ***Service Provider*** was similarly configured in the direction of the SIP trunk to the service provider. During the compliance test, IP addresses instead of domains were used in all SIP messages between the Telesur SIP proxy server and the Avaya SBCE. Note that since the default action of ***Auto*** implies the insertion of IP addresses in the host portion of these headers, it was not necessary to modify any of the headers sent to the service provider. The screen below shows the ***Service Provider*** profile once the configuration was completed.



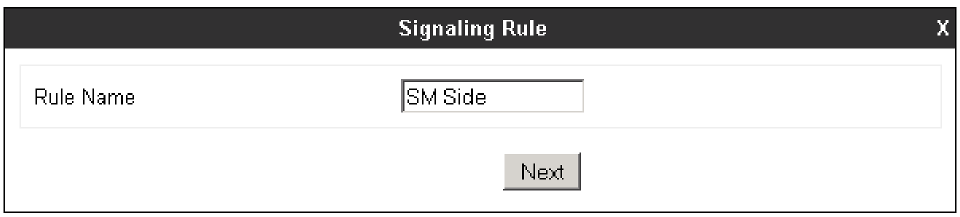
7.11. Signaling Rules

A Signaling Rule was created in the sample configuration to remove (block) the following headers:

- AV-Correlation-ID
- AV-Global-Session-ID
- Alert-Info
- Endpoint-View
- P-AV-Message-ID
- P-Location
- P-Charging-Vector

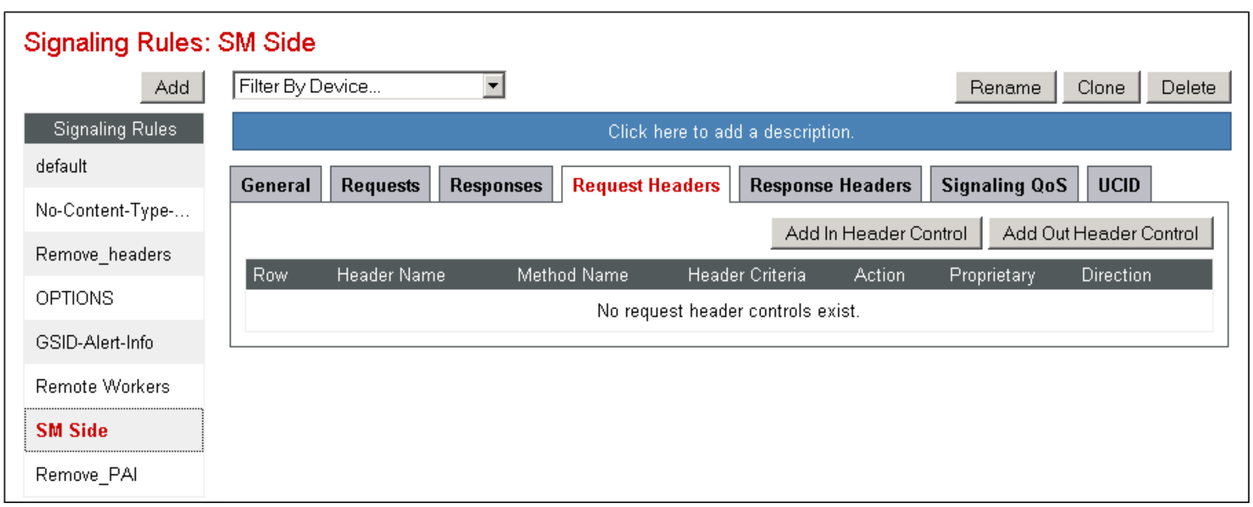
These headers are sent in SIP messages from the Session Manager to the Avaya SBCE. They contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries.

In the **Domain Policies** menu on the left-hand side, select **Signaling Rules**, then **Add Rule** (not shown). Enter an appropriate name like in the example below. Click **Next**.



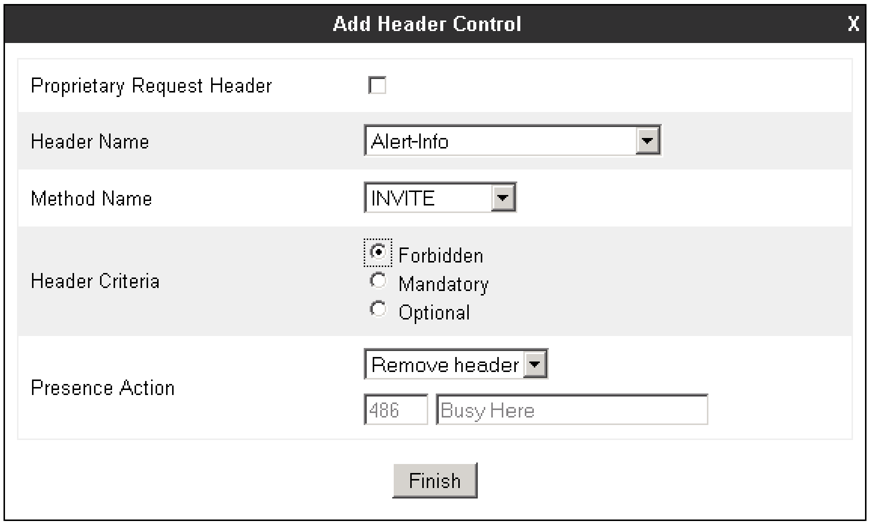
Click **Next** on the next four tabs (not shown), leaving all fields in sections **Inbound Outbound**, **Content-Type Policy**, **QoS** and **UCDI** with their default values. Click **Finish**.

On the newly created Signaling Rule, select the **Request Headers** tab to create the manipulations performed on request messages. Select **Add In Header Control**.

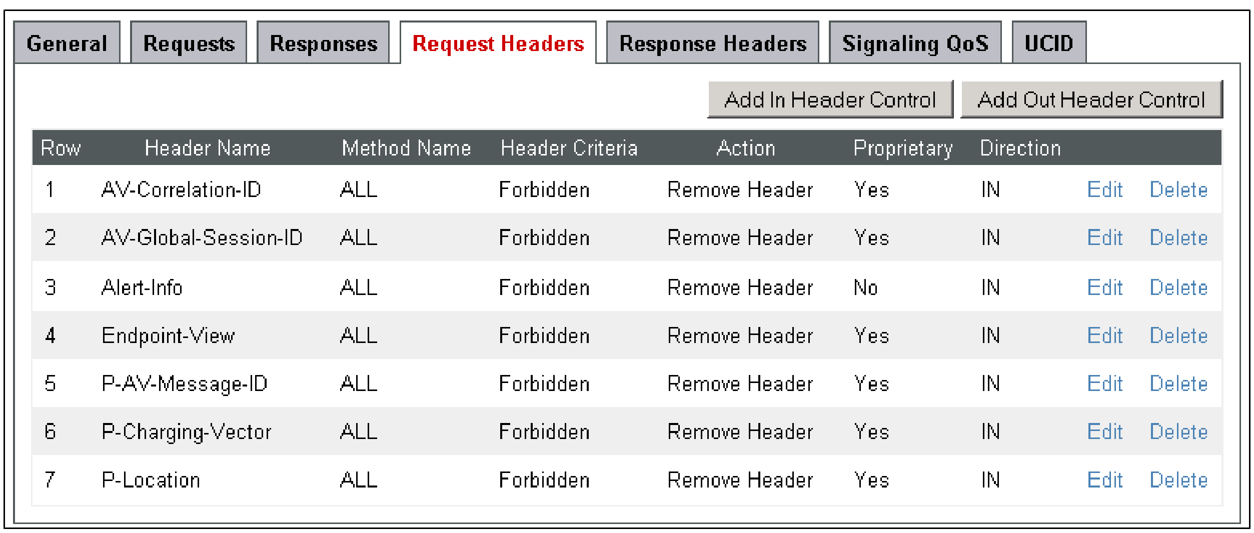


In the **Add Header Control** screen select the following:

- **Header Name:** Select ***Alert-Info*** from the drop down menu.
- **Method Name:** Select ***INVITE***.
- **Header Criteria:** Check **Forbidden**.
- **Presence Action:** Select ***Remove Header***.
- Click **Finish**



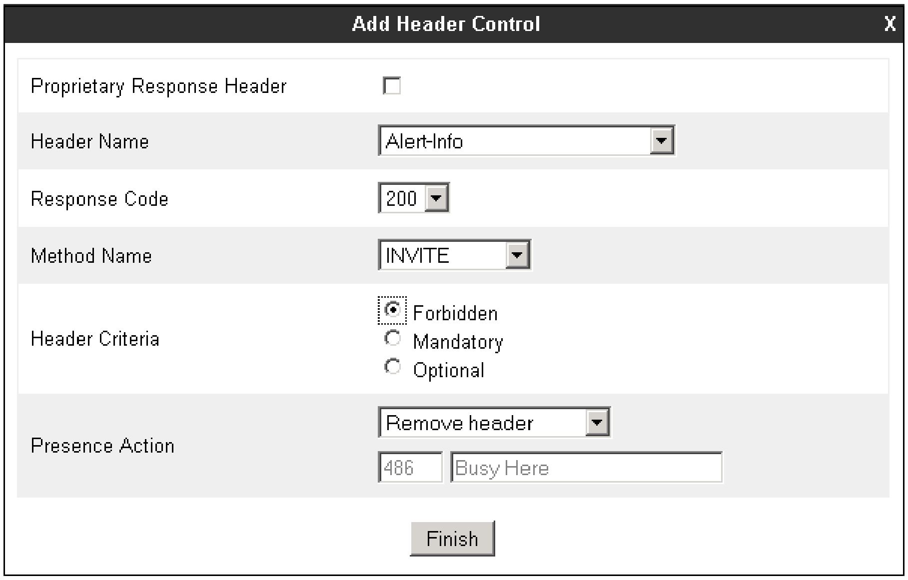
Select **Add In Header Control** as needed to configure the remaining header control rules. For these headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Request Headers** tab should look like the following screen.



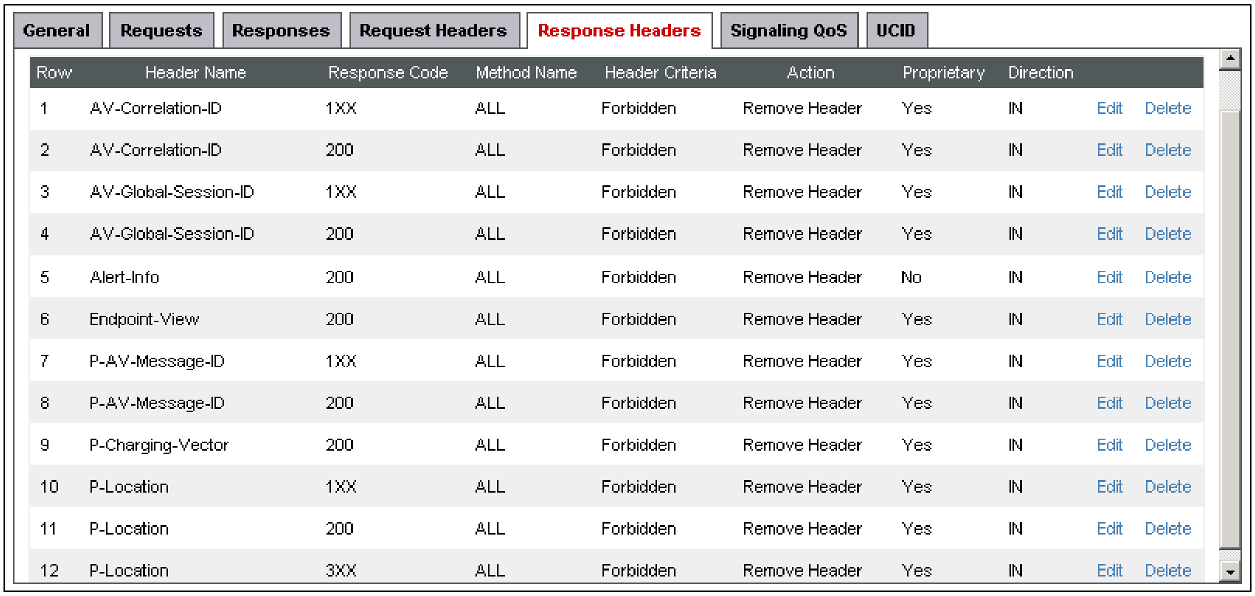
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
4	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Select the **Response Headers** tab to similarly create the manipulations performed on response messages. Select **Add In Header Control** (not shown).

The screen below shows the settings for the Alert-Info header on response messages.



Select **Add In Header Control** as needed to configure the remaining header control rules. For these headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Response Headers** tab should look like the following screen.



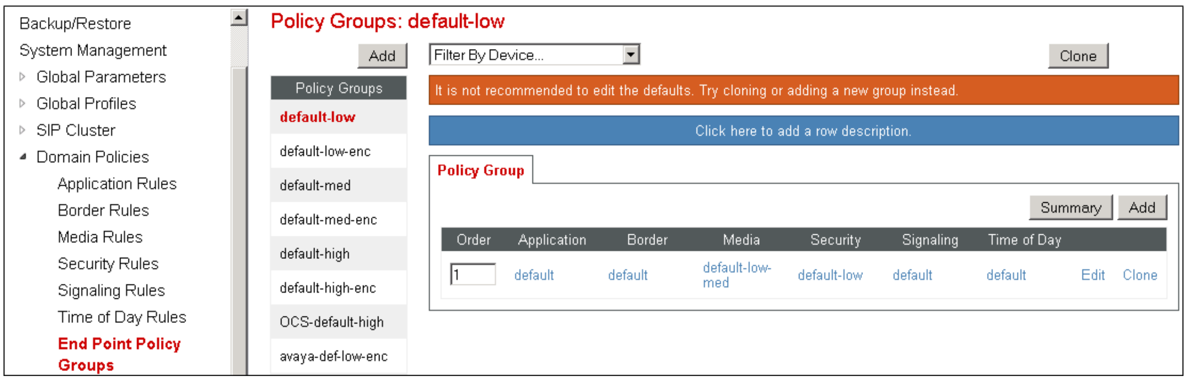
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Correlation-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	AV-Global-Session-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
6	Endpoint-View	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-AV-Message-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-AV-Message-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
10	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
11	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
12	P-Location	3XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE. In the reference configuration, the End Point Policy Groups used default sets of rules already pre-defined in the configuration, with the exception of the new Signaling Rule defined in **Section 7.11**. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

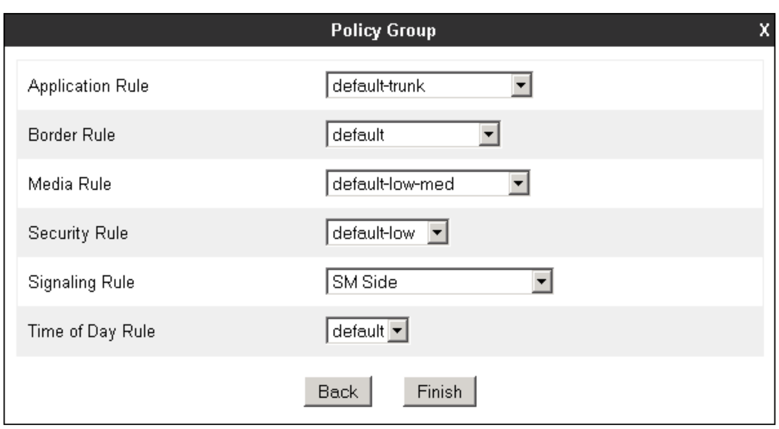
7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu. Select **Add**.

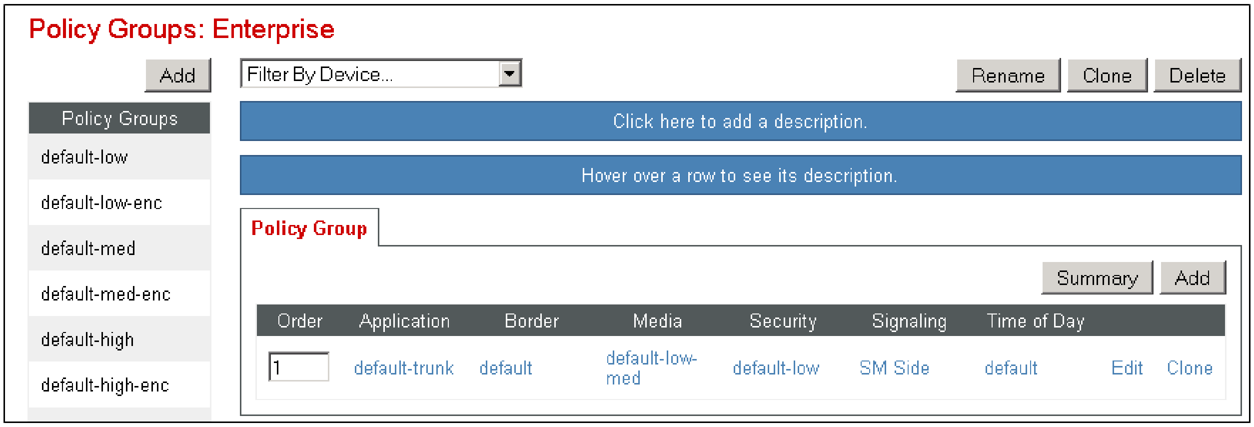


Enter an appropriate name in the **Group Name** field. Click **Next**.

In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, with the exception of the **Signaling Rule**, where the ***SM Side*** rule created previously was selected. Click **Finish**.

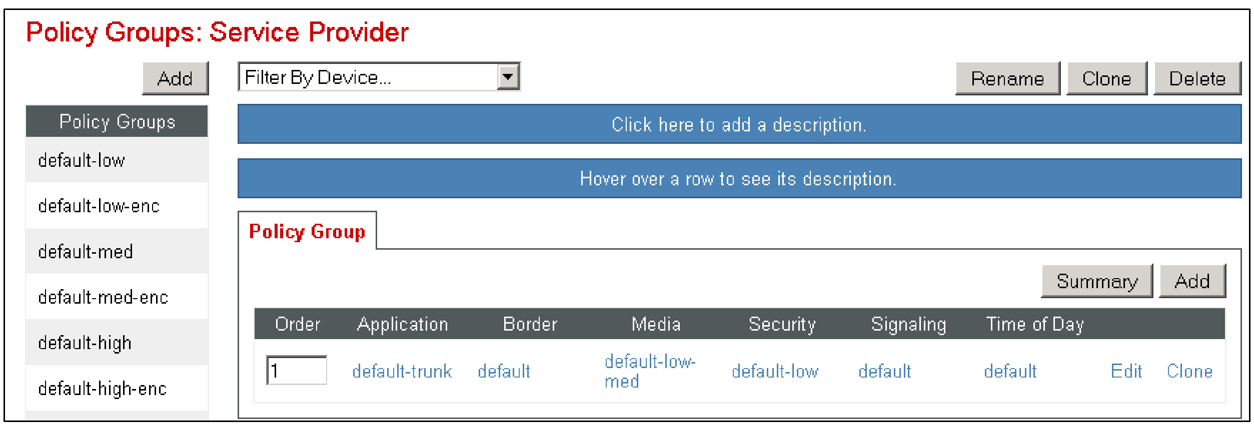


The screen below shows the ***Enterprise*** End Point Policy Group after the configuration was completed.



7.12.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described, but using defaults in this case for all fields. The screen below shows the ***Service Provider*** End Point Policy Group after the configuration was completed.

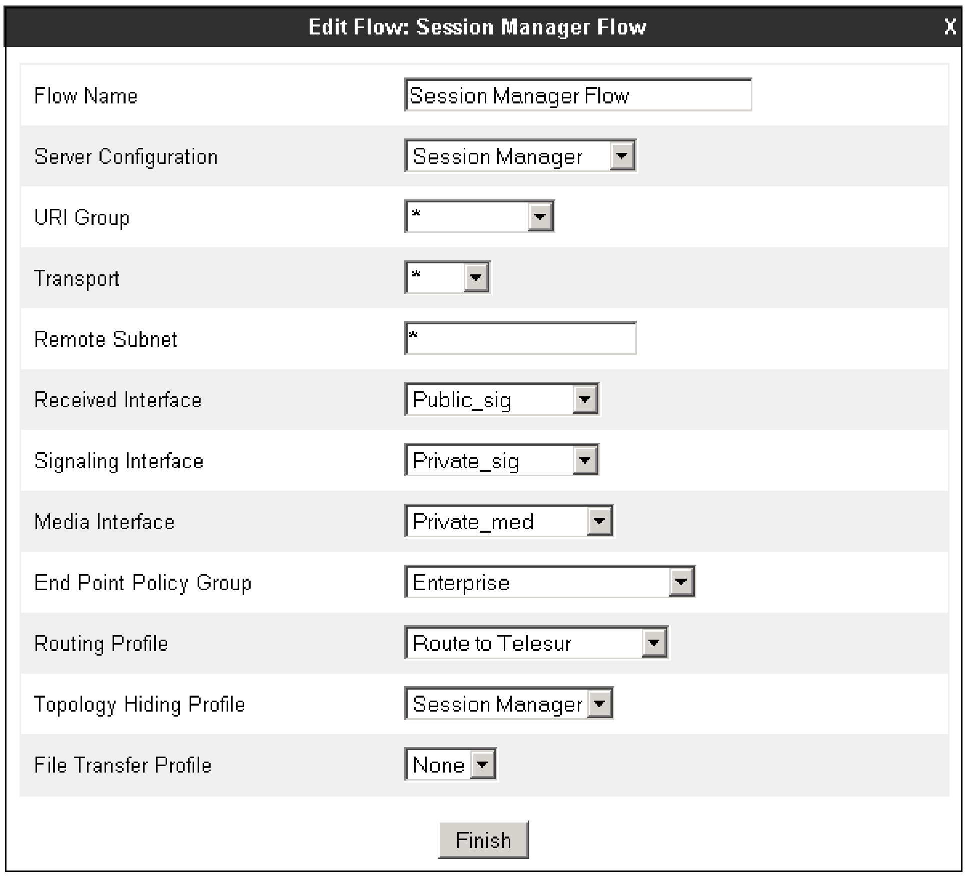


7.13. End Point Flows

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

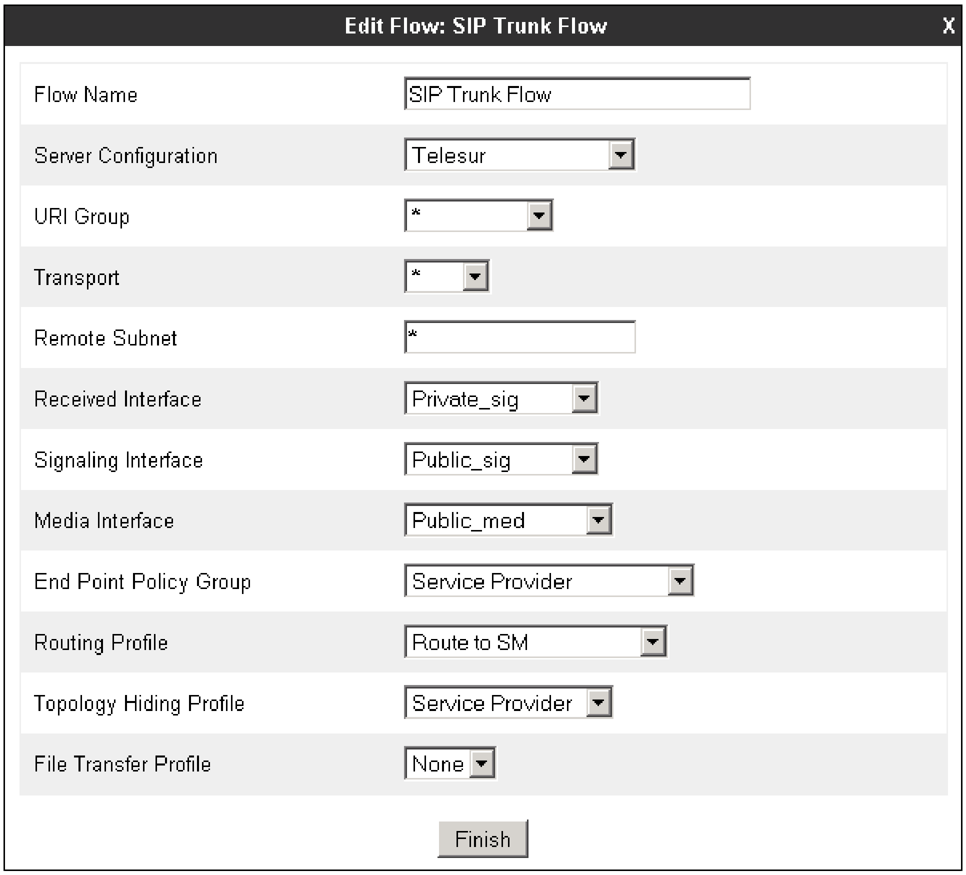
7.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named ***Session Manager Flow*** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.



7.13.2. End Point Flow – Service Provider

A second Server Flow with the name ***SIP Trunk Flow*** was similarly created in the network direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.



8. Telesur SIP Trunking Configuration

Telesur is responsible for the configuration of the Telesur SIP Trunking service in its network. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Telesur will provide the customer the necessary information to configure the SIP trunk connection from the enterprise site to the network, including:

- IP address, protocol and port used to reach the Telesur SIP Proxy server.
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

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

9. Verification and Troubleshooting

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

9.1. General Verification Steps

- 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.
- 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.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

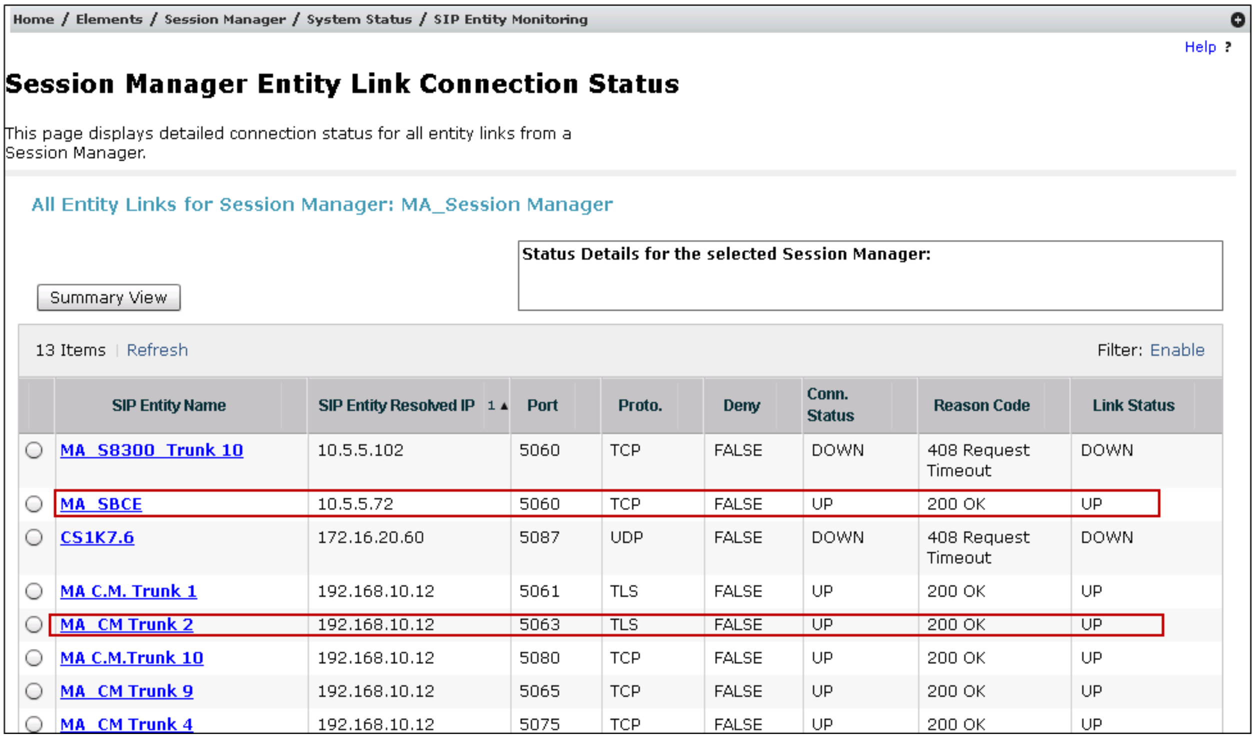
9.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

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

9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager → System Status → SIP Entity Monitoring.** Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is ***UP***, like shown on the screen below.


Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Help ?

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: MA_Session Manager

Status Details for the selected Session Manager:

Summary View

13 Items | Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	MA_S8300_Trunk 10	10.5.5.102	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
○	MA_SBCE	10.5.5.72	5060	TCP	FALSE	UP	200 OK	UP
○	CS1K7.6	172.16.20.60	5087	UDP	FALSE	DOWN	408 Request Timeout	DOWN
○	MA C.M. Trunk 1	192.168.10.12	5061	TLS	FALSE	UP	200 OK	UP
○	MA_CM Trunk 2	192.168.10.12	5063	TLS	FALSE	UP	200 OK	UP
○	MA C.M.Trunk 10	192.168.10.12	5080	TCP	FALSE	UP	200 OK	UP
○	MA_CM Trunk 9	192.168.10.12	5065	TCP	FALSE	UP	200 OK	UP
○	MA_CM Trunk 4	192.168.10.12	5075	TCP	FALSE	UP	200 OK	UP

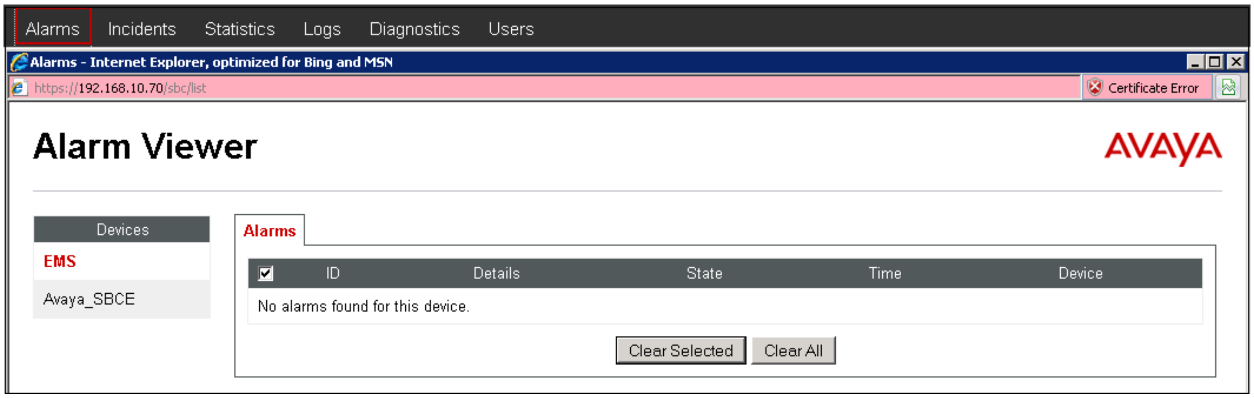
Other Session Manager useful verification and troubleshooting tools include:

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

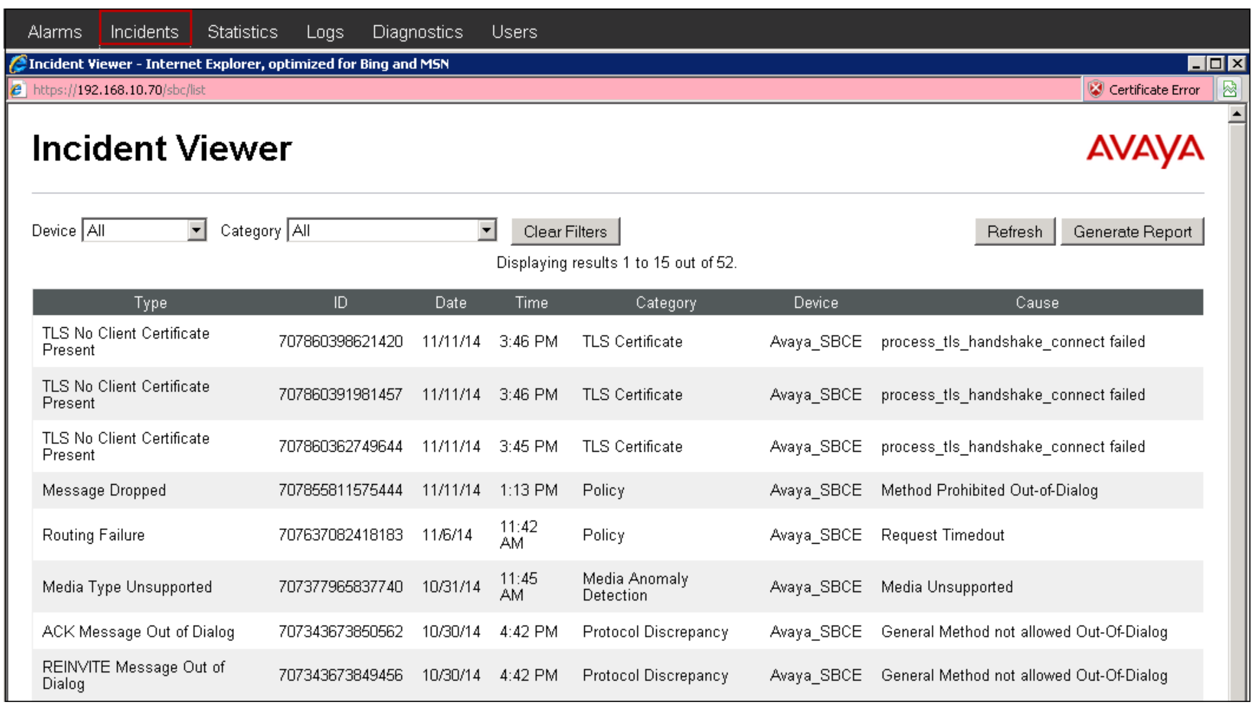
9.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

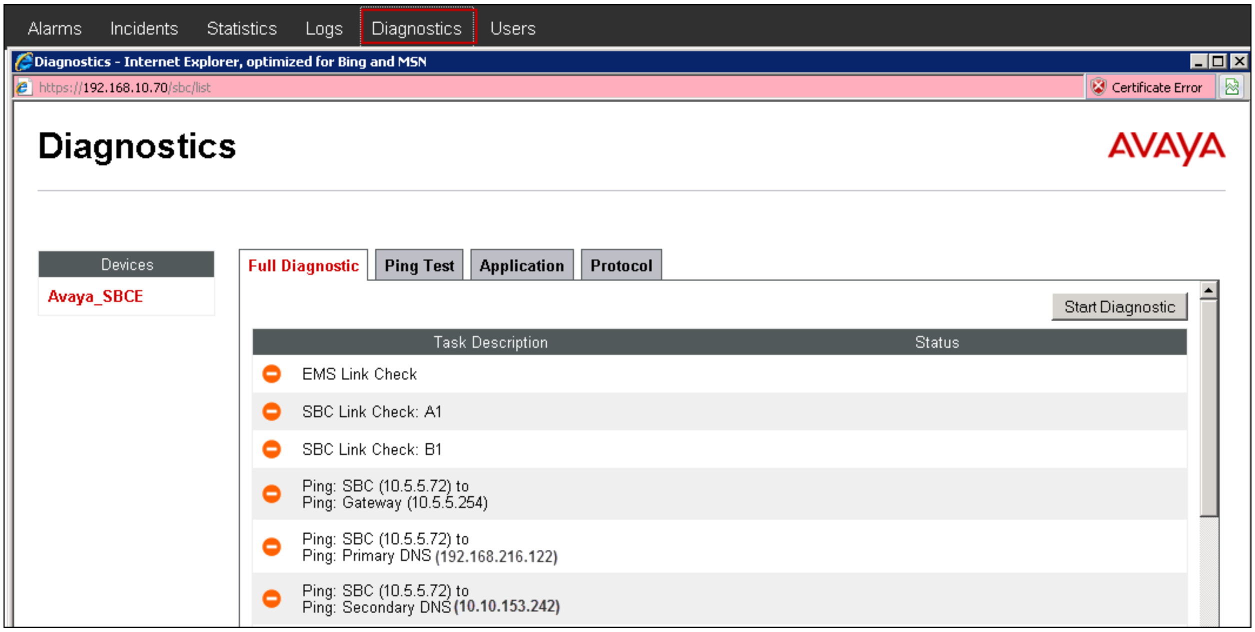
Alarms: Provides information about the health of the SBC.



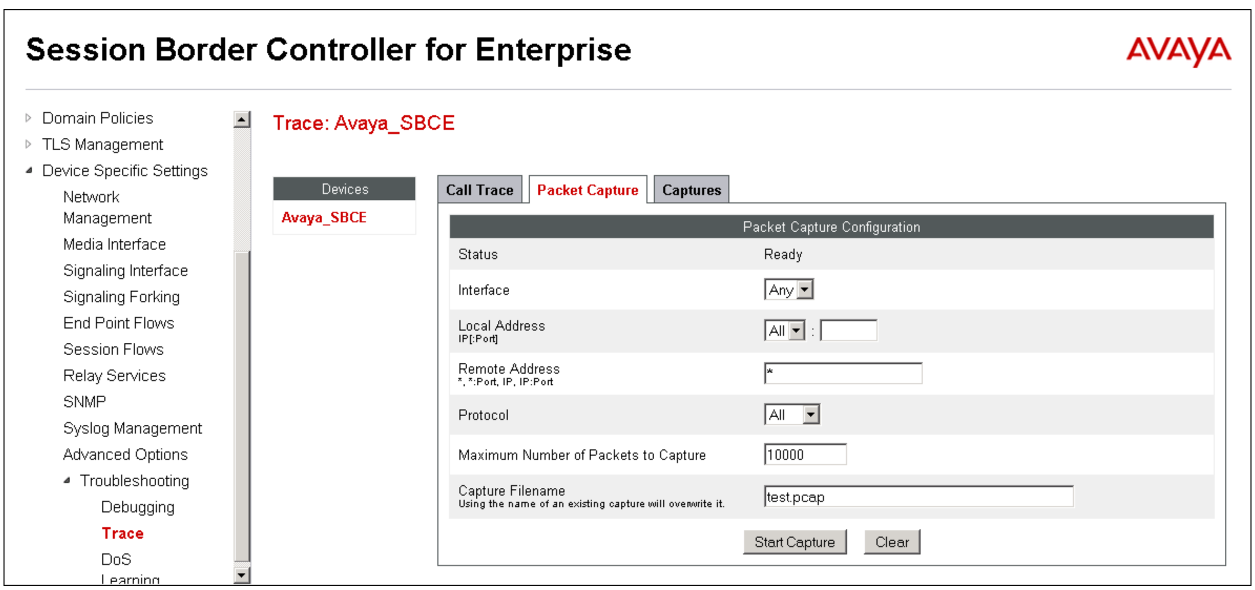
Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.



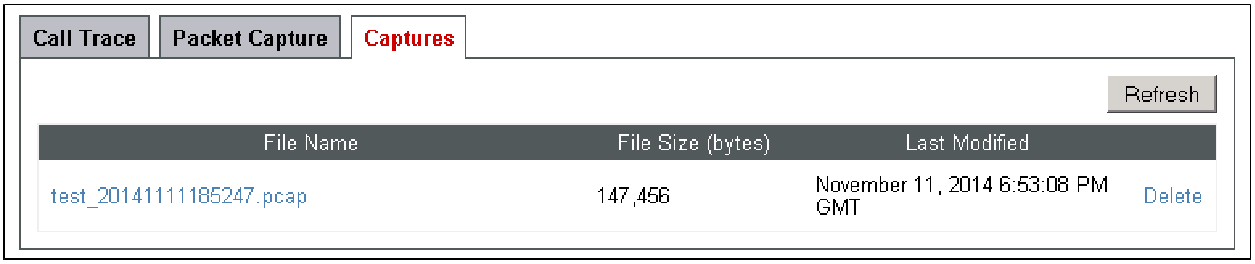
Diagnostics: This screen provides a variety of tools to test and troubleshoot the SBC network connectivity.



Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings → Troubleshooting → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.



Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2, to connect to the Telesur SIP Trunking service, as shown in **Figure 1**.

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

11. References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 6.3, June 2014, Document Number 03-300509.
[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, June 2014, Document Number 555-245-205.
[3] *Administering Avaya Aura® Session Manager*, Release 6.3, June 2014.
[4] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
[5] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, June 2014
[6] *Avaya Session Border Controller for Enterprise Release Notes.* Release 6.2. FP1 SP2, August 2014
[7] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3*, Avaya Solution and Interoperability Test Lab Application Notes, https://downloads.avaya.com/css/P8/documents/100183254
[8] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[9] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

12. Appendix A: SigMa Scripts

The following are Signaling Manipulation scripts used in the configuration of the Avaya SBCE, on **Section 7.7**.

Telesur script, applied to the **Telesur** Server Configuration profile, **Section 7.8.2**:

```
//Remove gsid and epv parameters in outbound Contact header

within session "ALL"
{
   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
   {
      remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);

      remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
   }
}

// Inbound Contact header manipulation

within session "ALL"
{
   act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
   {
      %HEADERS["Contact"][1].URI.USER = %HEADERS["To"][1].URI.USER;
   }
}
```

T38 Fax Version script, applied to the **Session Manager** Server Configuration profile, **Section 7.8.1**:

```
within session "ALL"
{
    act on request where %DIRECTION="INBOUND" and  %ENTRY_POINT="PRE_ROUTING"
    {
         %BODY[1].regex_replace( "a=T38FaxVersion:1","a=T38FaxVersion:0");
    }
}
```

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.