Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Evolution Server, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise with AT&T Mobility in Puerto Rico SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between the service provider AT&T Mobility in Puerto Rico and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.0.1, Avaya Aura® Session Manager 6.1, Avaya Session Border Controller for Enterprise and various Avaya endpoints.

The AT&T Mobility in Puerto Rico SIP Trunk Service provides PSTN access via a SIP trunk between the enterprise and the AT&T network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

AT&T Mobility in Puerto Rico is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the AT&T Mobility in Puerto Rico SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for Enterprise or Avaya Aura® Session Manager.

The AT&T Mobility in Puerto Rico SIP Trunk Service referenced within these Application Notes is designed for enterprise business customers. 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.

During the next pages and for brevity in these Application Notes, the service provider's name "AT&T Mobility in Puerto Rico" will be abbreviated and referred as "AT&T Mobility" or just "AT&T".

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the AT&T Mobility SIP Trunk service by means of a broadband connection to the public 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 to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator soft phones.

- Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X® Communicator also supports two signaling protocols: H.323 and SIP. Each supported protocol was tested.
- Various call types, including: local, long distance, international, outbound toll-free, emergency (911) and local directory assistance (411, 611).
- Codecs G729A and G.711MU and proper codec negotiation.
- DTMF tone transmissions passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection, using the SIP REFER and the 302 Redirection methods for the transfer of inbound call back to PSTN.
- Inbound and outbound fax calls to the PSTN.

Items not supported or not tested included the following:

- Operator services such as dialing 0 or 0 + 10 digits are not supported in this offer by AT&T Mobility in Puerto Rico.
- Inbound toll-free calls are supported but were not tested as part of the compliance test.

2.2 Test Results

Interoperability testing of the AT&T Mobility SIP Trunk Service with the Avaya Aura® SIP-enabled enterprise solution was completed with successful results with the exception of the observations and limitations described below:

- **T.38 Fax**: Even though incoming T.38 fax calls to the enterprise worked successfully, outbound T.38 fax calls failed to complete. Thus, T.38 Fax should not be used with this solution.
- **Network Call Redirection using REFER with redirected party Busy**: In the testing environment, when an inbound call was made to the enterprise, to a vector redirecting the call to another PSTN endpoint that was busy, the caller will hear a busy tone, but AT&T will not return a "486 Busy Here", preventing any additional processing of the call by Communication Manager, like the routing of the call to a local agent on the enterprise.
- **SIP User to User Information:** When a Communication Manager vector is programmed to send "User-to-User Information" (UUI) to a remote party, the information is generated and included in the REFER header sent to AT&T, but the UUI is not passed to the destination SIP endpoint.
- **RTP Payload type**: Interoperability problems were observed on outbound calls to the PSTN originated from SIP desktop phones and Avaya one-X® Communicator SIP clients, when using the default RTP payload type 120. For SIP hard phones, the solution was to change the RTP payload type in the *46xxsettings.txt* file in the associated HTTP server from the default type 120 to 101, the value preferred by AT&T. For the Avaya one-X® Communicator SIP clients, the workaround was to disable shuffling in their

specific IP Network Region. This approach is discussed in **Section 5.5** later in this document.

- **Avaya SBCE Patch**: On the current load of the Avaya SBCE, 4.0.5.Q02, a software patch was needed to support a SigMa script implemented to manipulate the Request-URI headers on requests arriving from AT&T. This script is discussed in **Section 7.3.5** later in this document. It should be noted that this patch will not be necessary with any subsequent software loads of the Avaya SBCE, as the functionality will be included as part of the core software.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on the AT&T Mobility SIP Trunk Services offer, call the AT&T Mobility Network Operations Center at 787-717-9900.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the AT&T Mobility SIP Trunk Service through a public Internet WAN connection, which is the configuration used for the Compliance Testing.

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

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

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

The Avaya SBCE constitutes the single point of connection between the public network and the Local Area Network in the enterprise. In addition to providing comprehensive Voice over IP and Unified Communications security to all SIP and RTP traffic entering the private network, the Avaya SBCE enables the interoperability with dissimilar SIP trunk service providers, by allowing the manipulation and adjustment of the elements in the packets flowing through its interfaces.

The transport protocol between the Avaya SBCE and AT&T Mobility across the public IP network is UDP. The transport protocol between the Avaya SBCE and the enterprise Session Manager across the enterprise IP network is TCP.

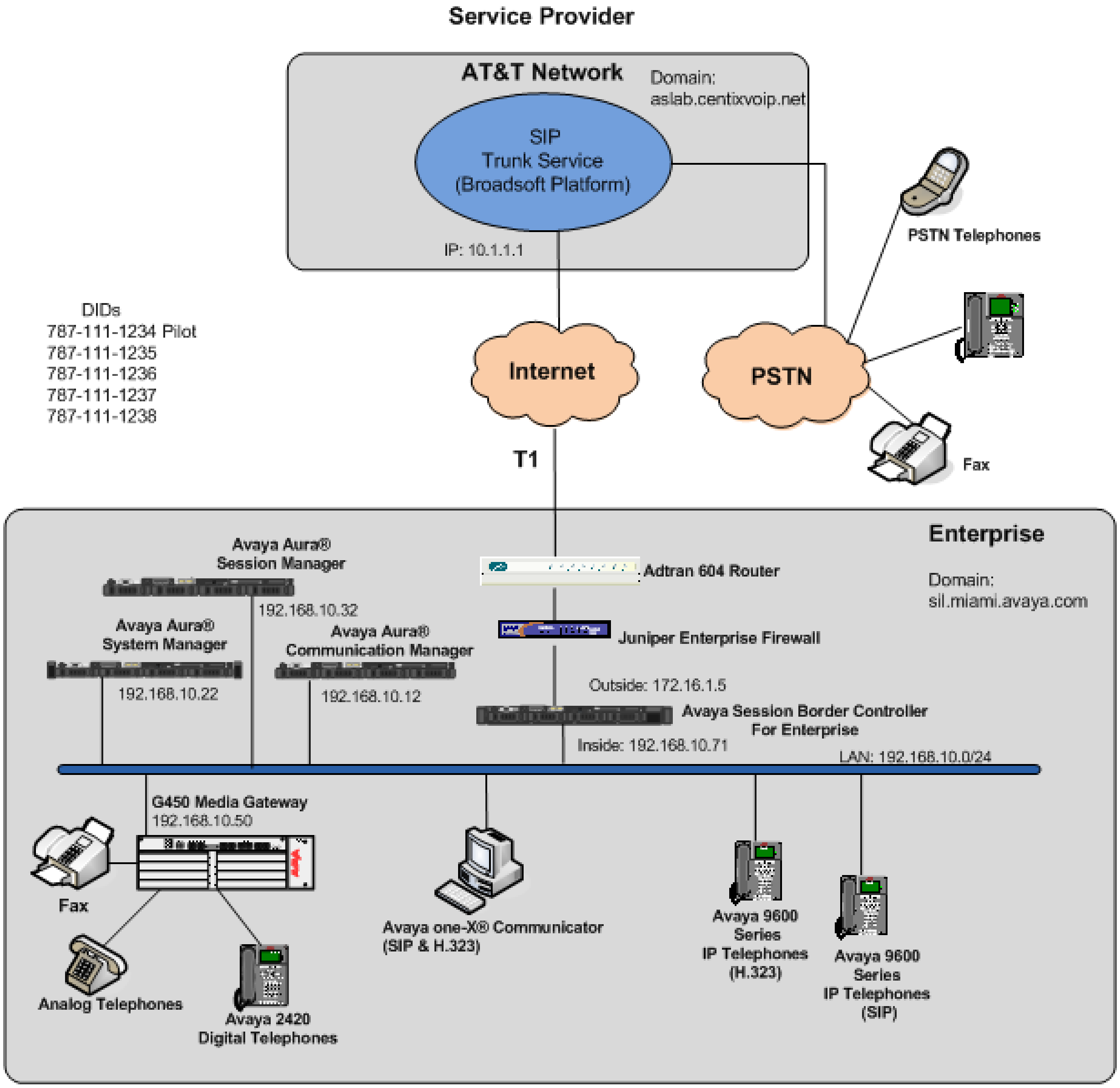


Figure 1: Avaya SIP Enterprise Solution connecting to AT&T Mobility SIP Trunk Service.

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

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

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

Since Puerto Rico is a country member of the North American Numbering Plan (NANP), the user dialed 10 digits for local calls, and 11 (1 + 10) or 10 digits for other calls between the NANP.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager on a HP® Proliant DL360 G7 Server.	6.0.1 SP5 (R016x.00.1.510.1)
Avaya Aura® Session Manager on a HP® Proliant DL360 G7 Server.	6.1 Service Pack 5 (ASM 6.1.5.0.615006)
Avaya Aura® System Manager on a HP® Proliant DL360 G7 Server.	6.1 Service Pack 5 Build No. 6.1.0.0.7345-6.1.5.502
Avaya Aura® Communication Manager Messaging	vcm-016-00.1.510.1 service pack 2
Avaya Session Border Controller for Enterprise	Sipera Systems 4.0.5.Q02 Patch bin-lib-Q02.tar.gz
Avaya G450 Media Gateway	31.20.0
Avaya 96x0 Series IP Telephones (H.323)	Avaya one-X® Deskphone H.323 3.1 SP2
Avaya 96x0 Series IP Telephones (SIP)	Avaya one-X® Deskphone SIP 2.6.6
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X® Deskphone H.323 6.0 SP5
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X® Deskphone SIP 6.0.2
Avaya one-X® Communicator (H.323, SIP)	6.1.2.06-SP2-33739
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
AT&T Puerto Rico SIP Trunking	
Acme-Packet Net-Net 4250 SBC	Firmware SC6.1.0 MR-9 GA (Build 938)
BroadWorks Soft Switch	R17
Nortel CS2K PSTN Gateway	CVM11

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

5. Configure Communication Manager

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

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **269** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                                 USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 1
             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: 18000 0
                   Maximum Video Capable IP Softphones: 18000 2
                       Maximum Administered SIP Trunks: 24000 269
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 100   0

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

5.2. System Features

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

```
change system-parameters features                               Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
                Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                      Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

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




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

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

```
display system-parameters features                              Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

5.3. IP Node Names

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

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
asm                     192.168.10.32
default                 0.0.0.0
msgserver               192.168.10.12
procr                   192.168.10.12
procr6                  ::
rselab                  192.168.0.220
```

5.4. Codecs.

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. The AT&T SIP Trunk Service supports codecs G.729A and G.711MU, in this order of preference. Enter ***G.729A*** and ***G.711MU*** 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.729A            n            2        20
 2: G.711MU           n            2        20
 3:
```

Since T.38 fax testing was not reliable, it is recommended to disable T.38 Fax by setting the **Fax Mode** field to ***off*** on **Page 2**.

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

                           IP Codec Set

                               Allow Direct-IP Multimedia? n



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

5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 2 was chosen for the service provider trunks. 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.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1        Authoritative Domain: sil.miami.avaya.com
    Name: AT&T PR SIP Trunk
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 example below shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

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

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

A separate network region was additionally created with the purpose of containing the SIP soft phones of the enterprise. This was necessary to implement the workaround to the interoperability problem observed with the RTP payload type 120 mentioned in **Section 2.2**, on calls originating from Avaya one-X® Communicator SIP soft clients to the PSTN.

Use the **change ip-network-region 3** command and enter the following parameters:

- **Authoritative Domain**: **sil.miami.avaya.com**
- Enter a descriptive name in the **Name** field.
- Change the **Inter-region IP-IP Direct Audio** to **no.** This will 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 3                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 3
Location: 1         Authoritative Domain: sil.miami.avaya.com
    Name: Softphones
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: no
   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
```

On **Page 4**, specify the IP codec set to be used for traffic between region 3 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Codec set **1** was be used for calls between region 3 (the soft phones region) and region 1 (the rest of the enterprise). Note that since shuffling is not allowed, it is not necessary to specify a codec set between network regions 3 and 2.

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

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

In the compliance test scenario, all the soft phones in the enterprise were placed in the subnet **10.5.5.128/25**. Use the **change ip-network-map** command to assign the subnet to the network region 3.

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

                                                 Subnet Network    Emergency
 IP Address                                      Bits   Region VLAN Location Ext
 ----------------------------------------------- ------ ------ ---- -------------
 FROM: 10.5.5.128_______________________________ /25__  3__    n___ _____________
   TO: 10.5.5.255_______________________________
 FROM: _________________________________________ /___   ___    n___ _____________
   TO:
```

5.6. Signaling Group

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

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

- Set the **Far-end Node Name** to ***asm***. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise

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

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? n                                Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM


   Near-end Node Name: procr                    Far-end Node Name: asm
 Near-end Listen Port: 5070                   Far-end Listen Port: 5070
                                           Far-end Network Region: 2
                                   Far-end Secondary Node Name:
Far-end Domain: sil.miami.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? 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 **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 SIP trunk and the enterprise endpoint. Note that media shuffling can also be enabled or restricted on each IP network regions forms.
- 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 step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

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

Group Number: 2                   Group Type: sip             CDR Reports: y
  Group Name: AT&T PR SIP Trunk           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. For the compliance test, the default value of ***600*** seconds was used.

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

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

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

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

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



                     Numbering Format: private
                                                UUI Treatment: service-provider

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

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

On **Page 4**, set the **Network Call Redirection** field to ***y***. This enables the use of the SIP REFER method for calls transferred back to the PSTN. Set the **Send Diversion Header** field to ***y***. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to ***n***.

Set the **Telephone Event Payload Type** to ***101***, and **Convert 180 to 183 for Early Media** to ***y***, the values preferred by AT&T. Default values were used for all other fields.

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

                              Mark Users as Phone? n
                    Prepend '+' to Calling Number? n
              Send Transferring Party Information? n
                         Network Call Redirection? y
                            Send Diversion Header? y
                          Support Request History? n
                     Telephone Event Payload Type: 101


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

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are 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. In the sample configuration, 5 DID numbers were assigned for testing. These 5 numbers were mapped to 5 extensions, 3001 to 3005. These 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 5 extensions.

```
change private-numbering 3                                      Page   1 of   2
                                NUMBERING - PRIVATE FORMAT

Ext Ext              Trk          Private              Total
Len Code             Grp(s)       Prefix               Len
 4  3                                                   4     Total Administered: 11
 4  3001             2            7871111234            10       Maximum Entries: 540
 4  3002             2            7871111235            10
 4  3003             2            7871111236            10
 4  3004             2            7871111237            10
 4  3005             2            7871111238            10
```

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

```
change private-numbering 3                                      Page   1 of   2
                                NUMBERING - PRIVATE FORMAT

Ext Ext              Trk          Private              Total
Len Code             Grp(s)       Prefix               Len
 4  3                2            787111                10    Total Administered: 11
                                                                 Maximum Entries: 540
```

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 AT&T is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. 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   10 7871111234        10  3001
 public-ntwrk   10 7871111235        10  3002
 public-ntwrk   10 7871111236        10  3003
 public-ntwrk   10 7871111237        10  3004
 public-ntwrk   10 7871111238        10  3005
 public-ntwrk
```

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

```
change inc-call-handling-trmt trunk-group 2                  Page   1 of  30
                   INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk   10 787111            6
 public-ntwrk
 public-ntwrk
```

5.10. Outbound Routing

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

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

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

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

```
change feature-access-codes                                    Page   1 of  11
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
                      Announcement Access Code: #1
                       Answer Back Access Code: ____
                         Attendant Access Code: __
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9       Access Code 2: ____
                 Automatic Callback Activation: ____     Deactivation: ____
Call Forwarding Activation Busy/DA: ____    All: ____     Deactivation: ____
   Call Forwarding Enhanced Status: ____    Act: ____     Deactivation: ____
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** 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   2 of   2
                            ARS DIGIT ANALYSIS TABLE
                                 Location: all            Percent Full: 1

          Dialed              Total     Route     Call    Node   ANI
          String             Min  Max  Pattern    Type    Num    Reqd
    011                      10   18    2         intl           n
    787                      10   10    2         hnpa           n
    1305                     11   11    2         fnpa           n
    1786                     11   11    2         fnpa           n
    1800                     11   11    2         fnpa           n
    411                      3    3     2         svcl           n
    611                      3    3     2         svcl           n
                                                                 n
                                                                 n
                                                                 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. For the compliance test, trunk group 2 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format**: **unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**.

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2   Pattern Name: AT&T SIP Trunk
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 2    0          1                                                     n   user
 2:                                                                       n   user
 3:                                                                       n   user
 4:                                                                       n   user
 5:                                                                       n   user
 6:                                                                       n   user

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

6. Configure Avaya Aura® Session Manager

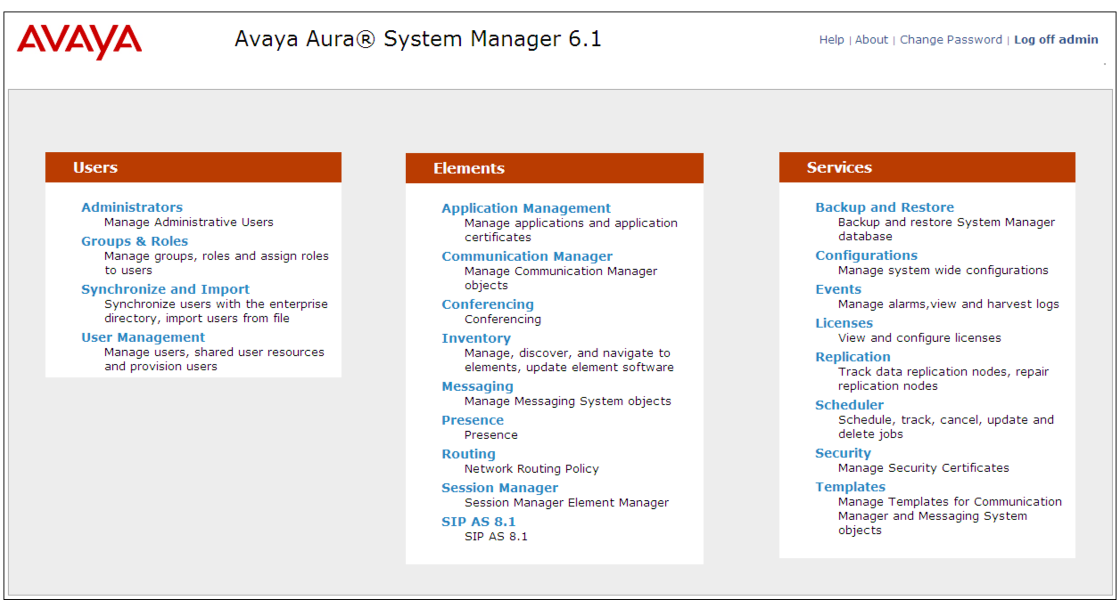
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

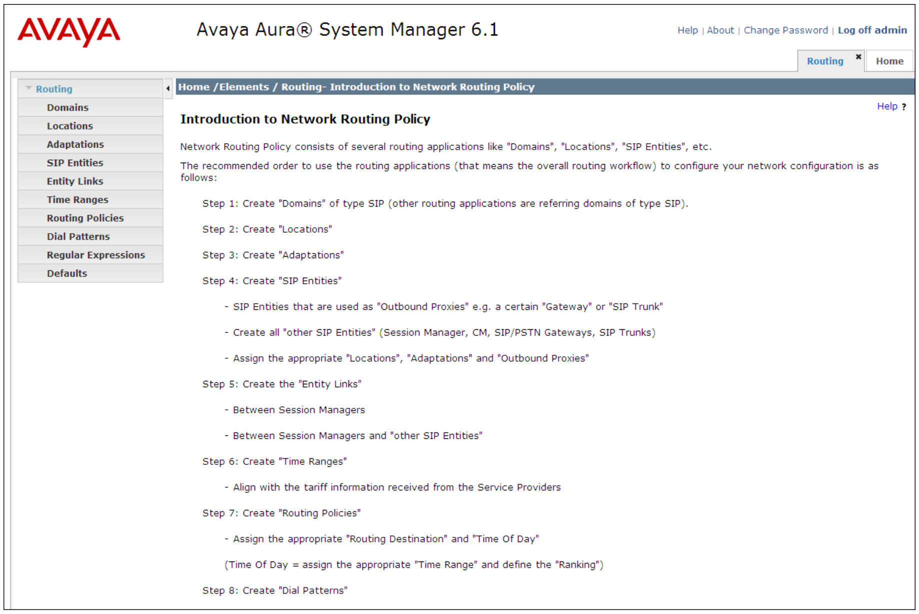
It may not be necessary to create all the items above when creating a connection to the service provider, since some of them would have already been defined as part of the initial Session Manager installation. This includes entries such as certain SIP domains, locations, SIP entities, and Session Manager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

6.1. System Manager Login and Navigation

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



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column to bring up the Introduction to Network Routing Policy screen.

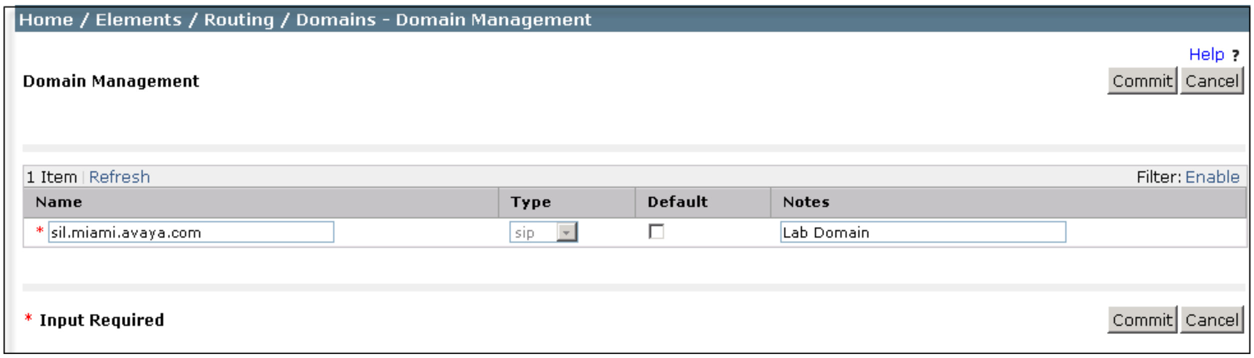


6.2. SIP Domains

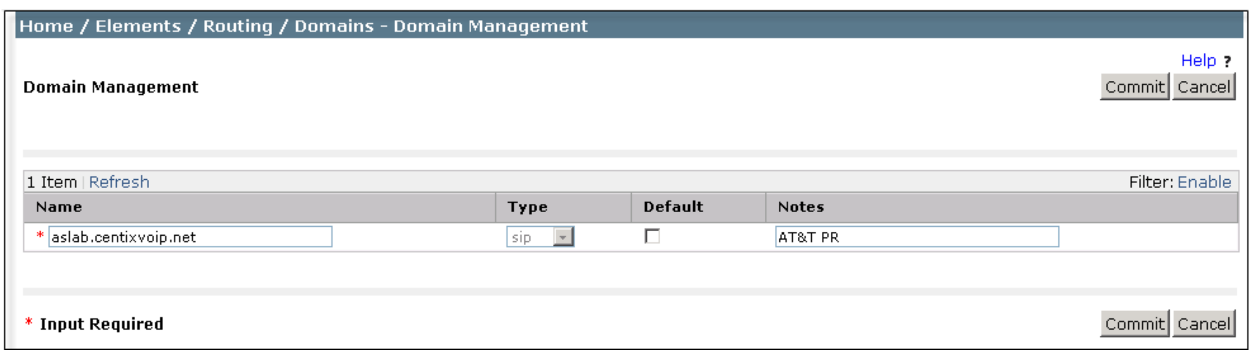
Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain, **sil.miami.avaya.com**, and the AT&T domain, **aslab.centixvoip.net**. Navigate to **Routing → Domains** in the left-hand navigation 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.



The screen below shows the entry for the AT&T test domain.



6.3. Locations

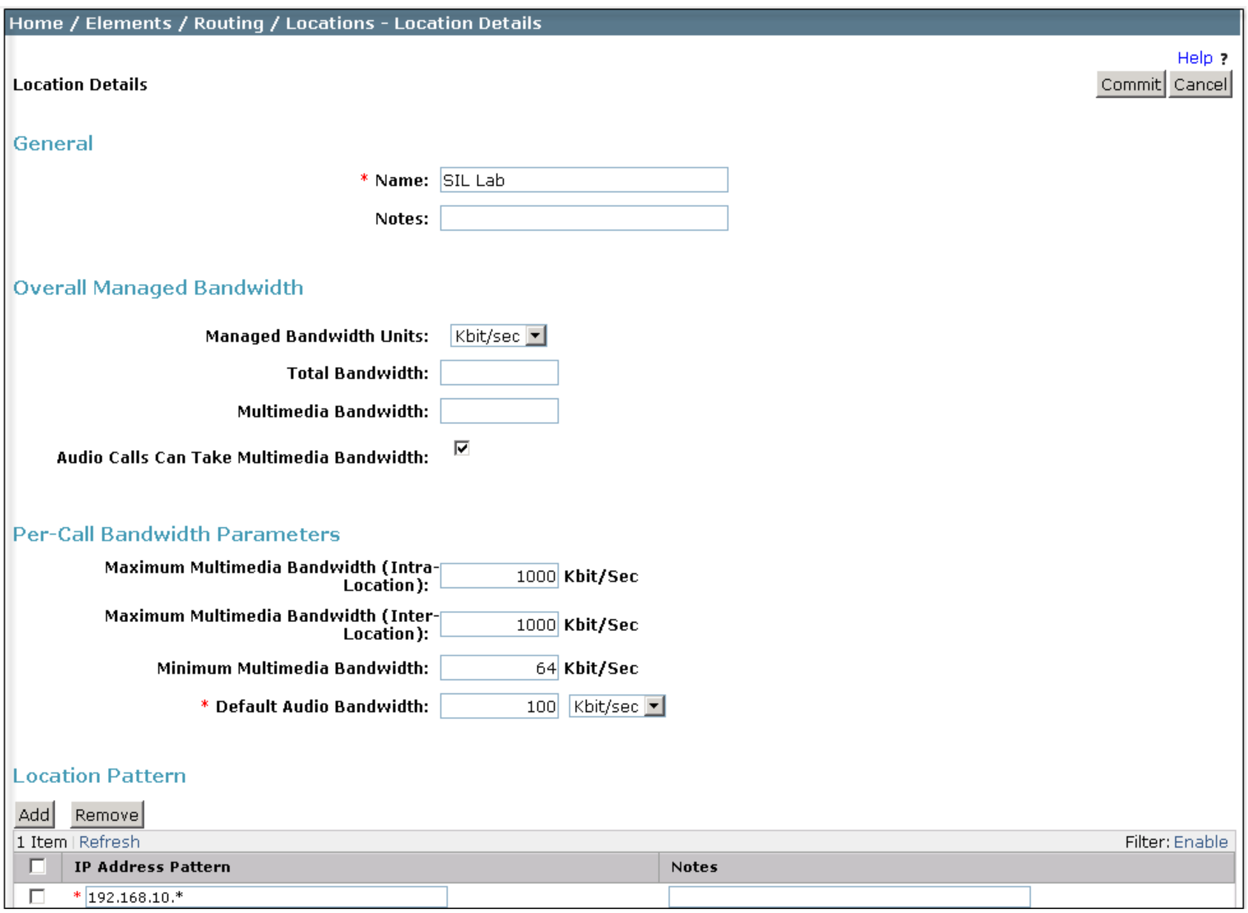
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).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

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

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

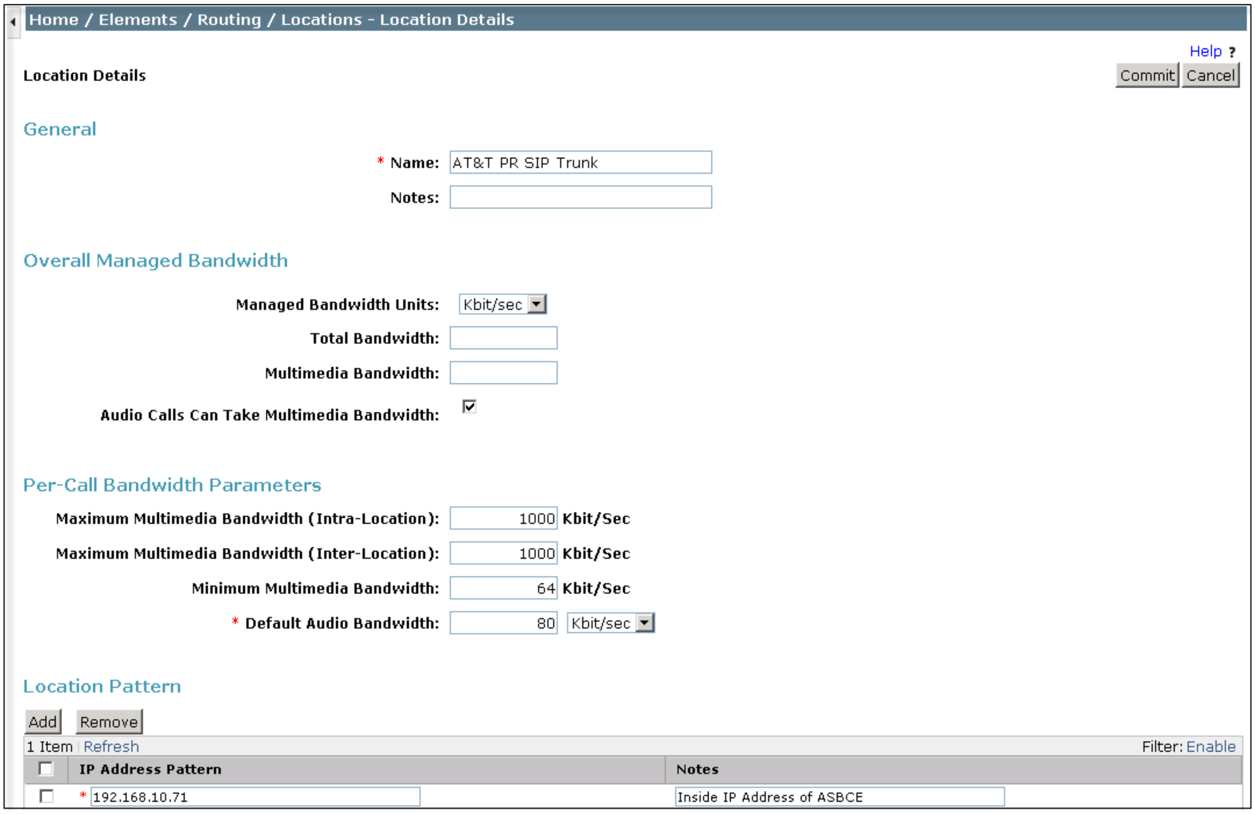
- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

The screen below shows the addition of the location **SIL Lab**, which includes all equipment in the Avaya Interoperability Lab, including Communication Manager and Session Manager itself, and resides in the 192.168.10.0 subnet. Click **Commit** to save.



Note that call bandwidth management parameters should be set per customer requirements.

Repeat the preceding procedure to create a separate Location for the AT&T SIP Trunk. Displayed below is the screen for addition of the ***AT&T PR SIP Trunk*** Location, which specifies the inside IP address for the Avaya SBCE. Click **Commit** to save.

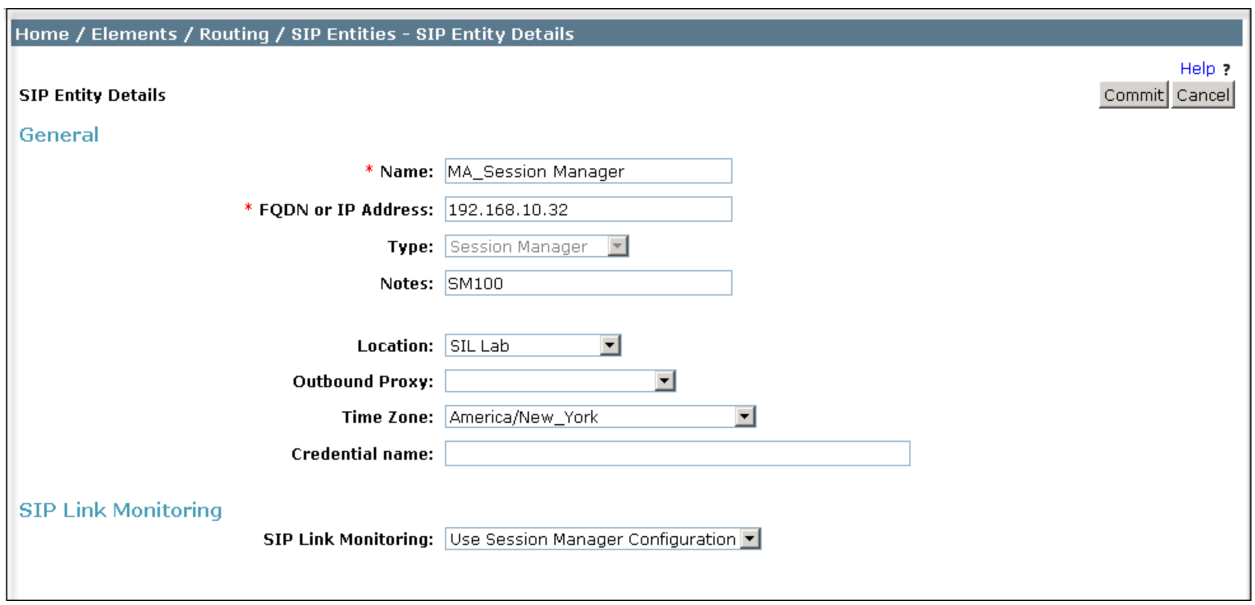


6.4. SIP Entities

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** 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 are applied to the entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

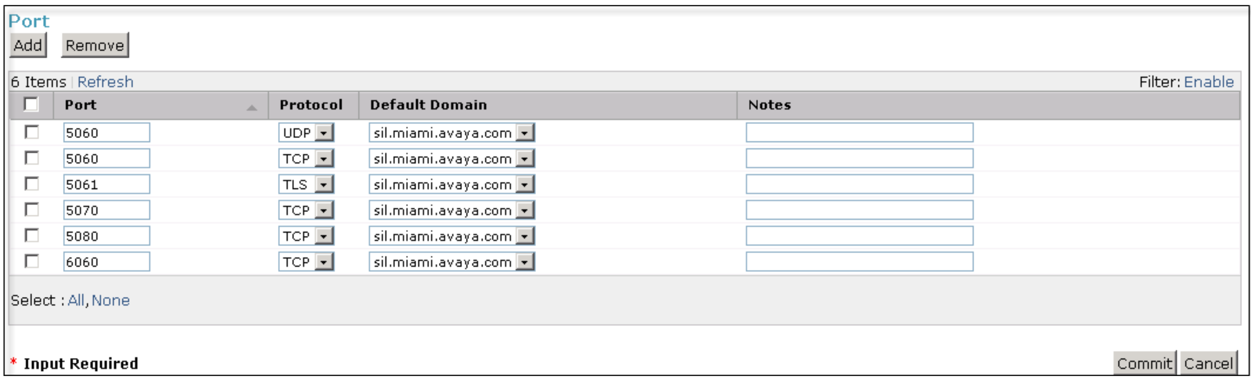
The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager signaling interface (virtual SM-100) is entered for **FQDN or IP Address**.



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

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

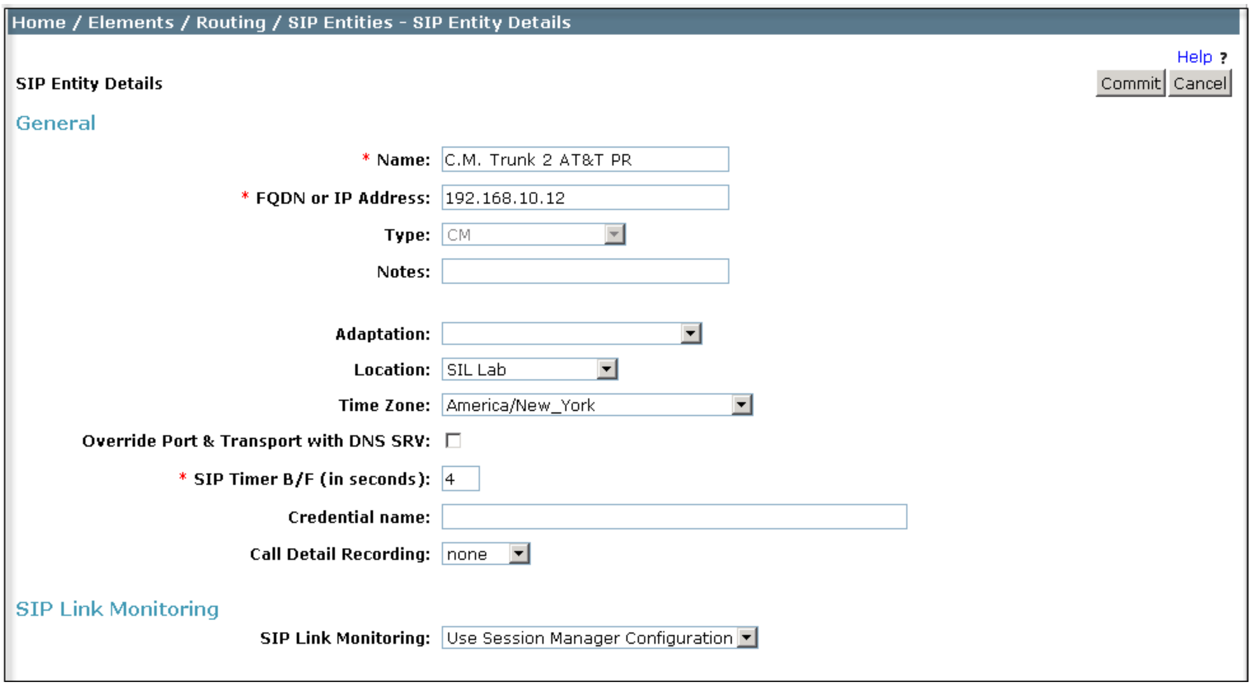
Defaults can be used for the remaining fields. Click **Commit** to save.



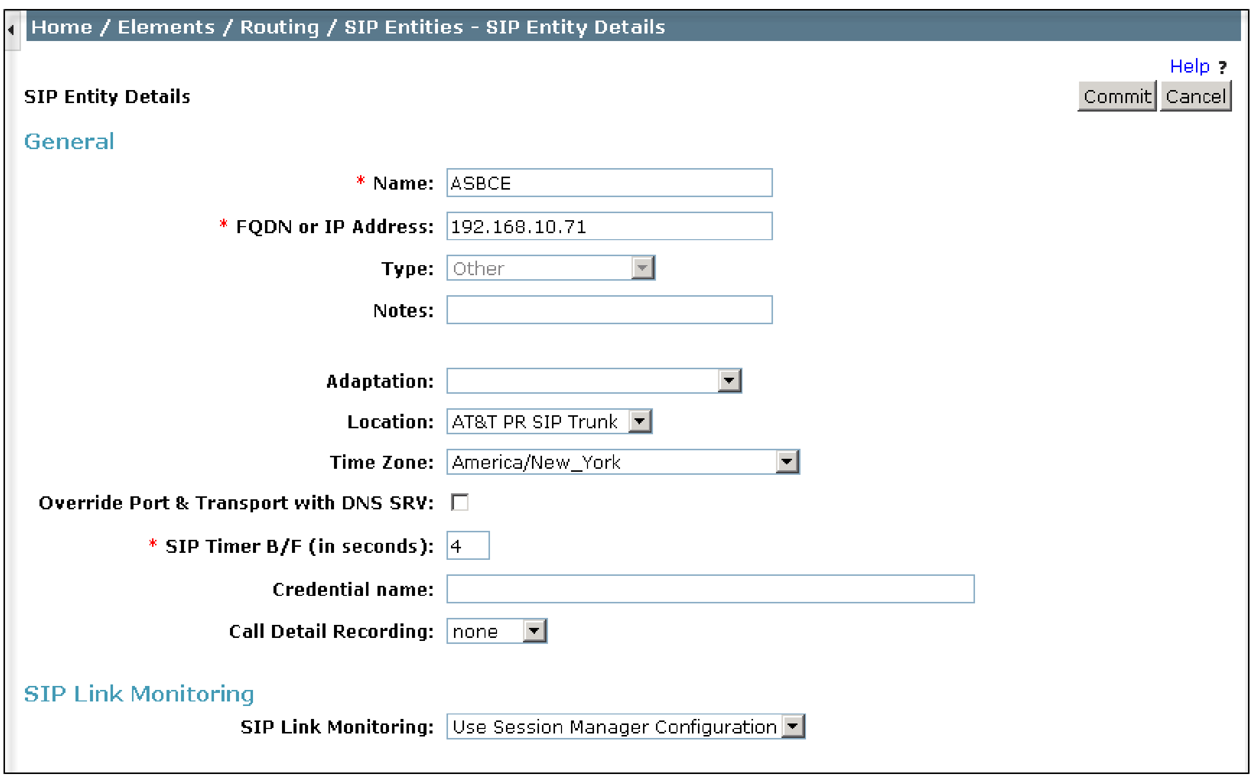
The screen above shows the ports used by Session Manager in the shared lab environment. Only TCP ports 5060 and 5070 are directly relevant to these Application Notes.

In order for Session Manager to route SIP service provider traffic on a specific trunk group in Communication Manager, a separate entity link to Communication Manager is required.

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



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



6.5. Entity Links

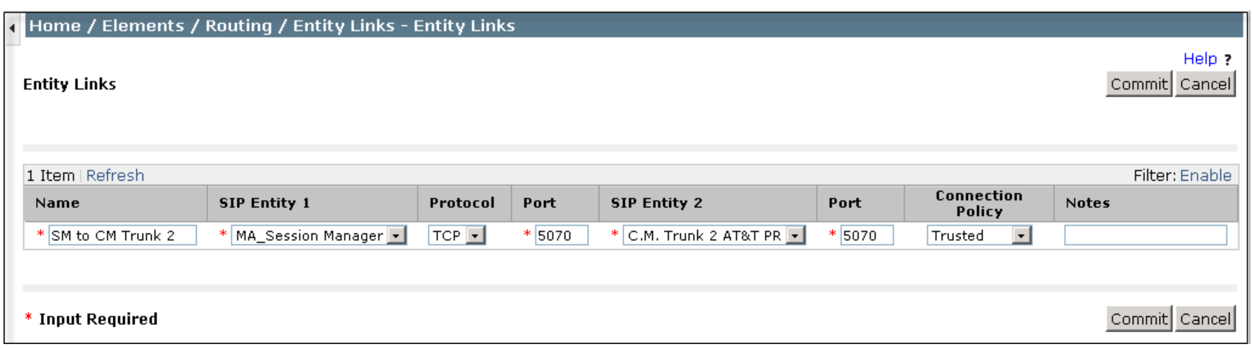
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation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

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

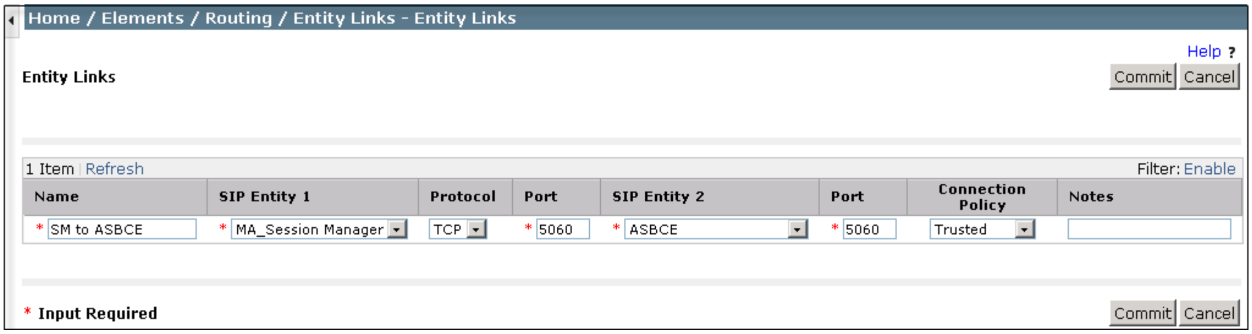
Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and the SBC. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. For the compliance test, TCP was used to facilitate troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager.



Entity Link to the Avaya SBCE.



Home / Elements / Routing / Entity Links - Entity Links

Help ?

Entity Links

Commit Cancel

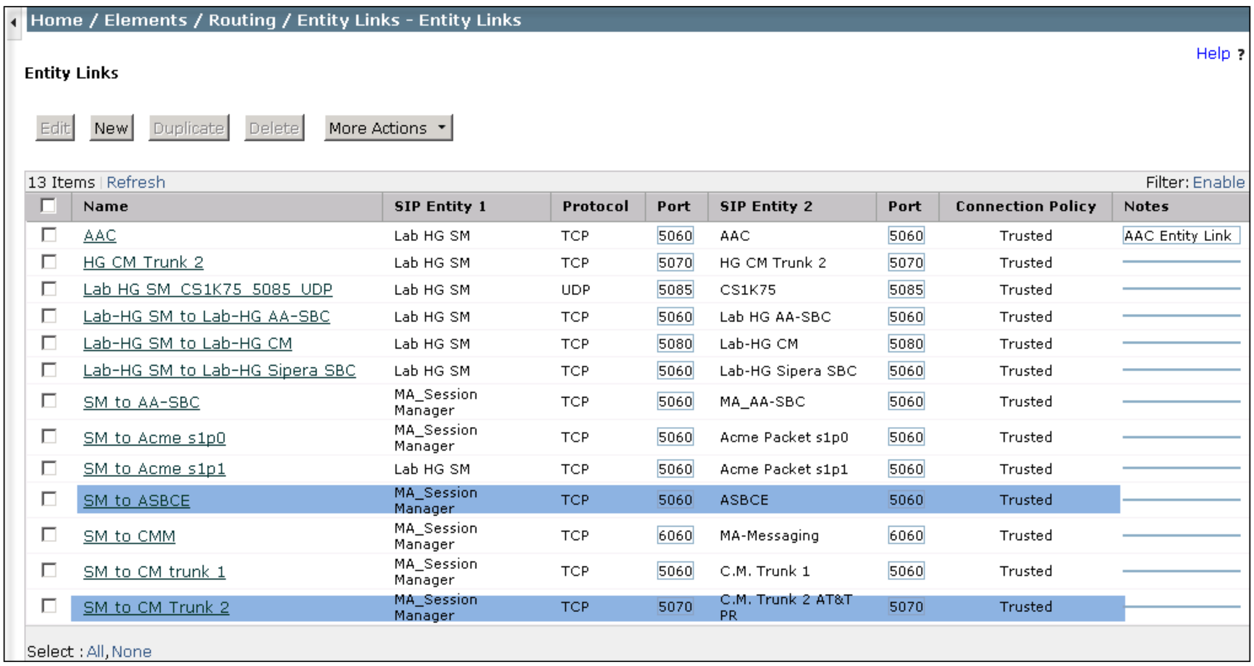
1 Item | Refresh Filter: Enable

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

* Input Required

Commit Cancel

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



Home / Elements / Routing / Entity Links - Entity Links

Help ?

Entity Links

Edit New Duplicate Delete More Actions

13 Items | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
AAC	Lab HG SM	TCP	5060	AAC	5060	Trusted	AAC Entity Link
HG CM Trunk 2	Lab HG SM	TCP	5070	HG CM Trunk 2	5070	Trusted	
Lab HG SM CS1K75 5085 UDP	Lab HG SM	UDP	5085	CS1K75	5085	Trusted	
Lab-HG SM to Lab-HG AA-SBC	Lab HG SM	TCP	5060	Lab HG AA-SBC	5060	Trusted	
Lab-HG SM to Lab-HG CM	Lab HG SM	TCP	5080	Lab-HG CM	5080	Trusted	
Lab-HG SM to Lab-HG Sipera SBC	Lab HG SM	TCP	5060	Lab-HG Sipera SBC	5060	Trusted	
SM to AA-SBC	MA_Session Manager	TCP	5060	MA_AA-SBC	5060	Trusted	
SM to Acme s1p0	MA_Session Manager	TCP	5060	Acme Packet s1p0	5060	Trusted	
SM to Acme s1p1	Lab HG SM	TCP	5060	Acme Packet s1p1	5060	Trusted	
SM to ASBCE	MA_Session Manager	TCP	5060	ASBCE	5060	Trusted	
SM to CMM	MA_Session Manager	TCP	6060	MA-Messaging	6060	Trusted	
SM to CM trunk 1	MA_Session Manager	TCP	5060	C.M. Trunk 1	5060	Trusted	
SM to CM Trunk 2	MA_Session Manager	TCP	5070	C.M. Trunk 2 AT&T PR	5070	Trusted	

Select : All, None

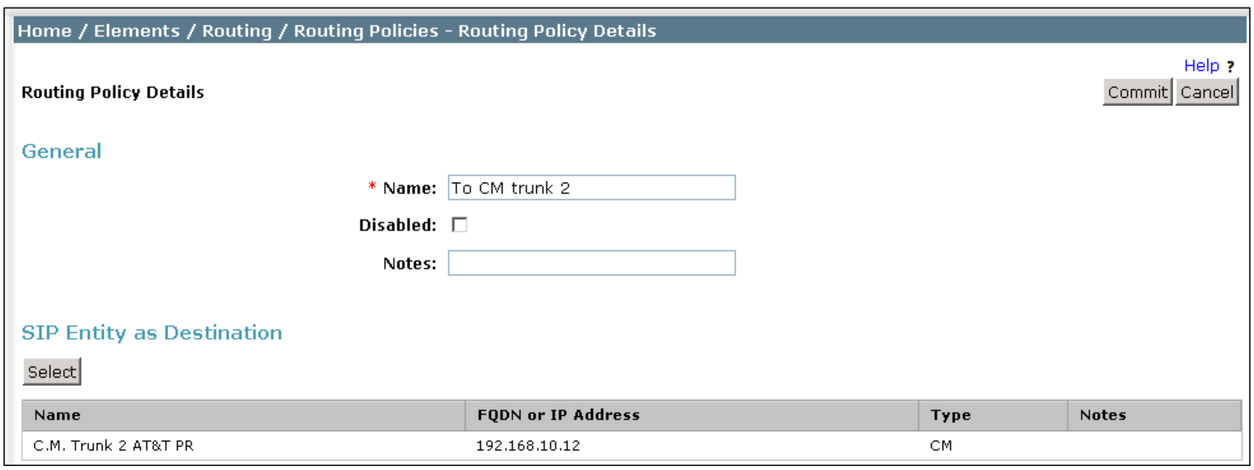
6.6. Routing Policies

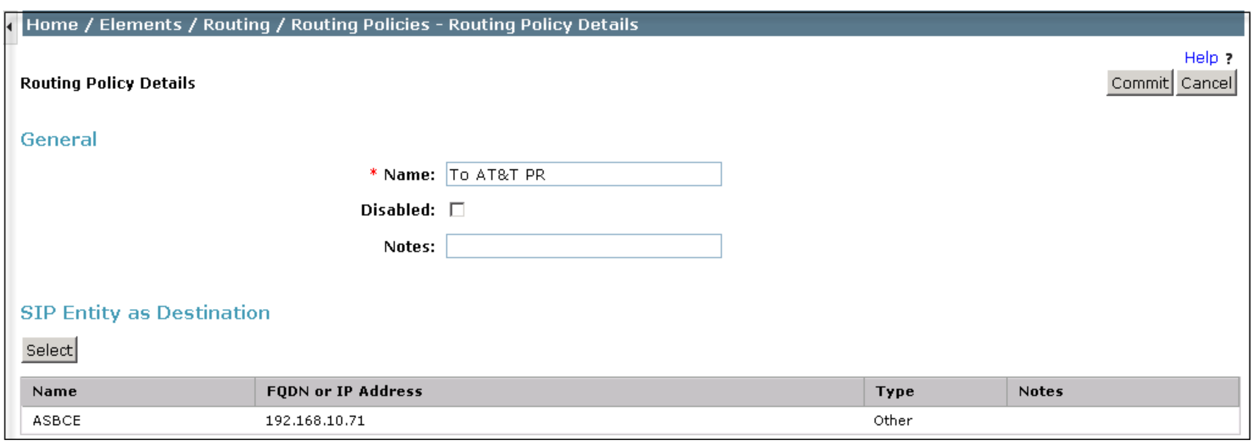
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter the following values:

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

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

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





6.7. Dial Patterns

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

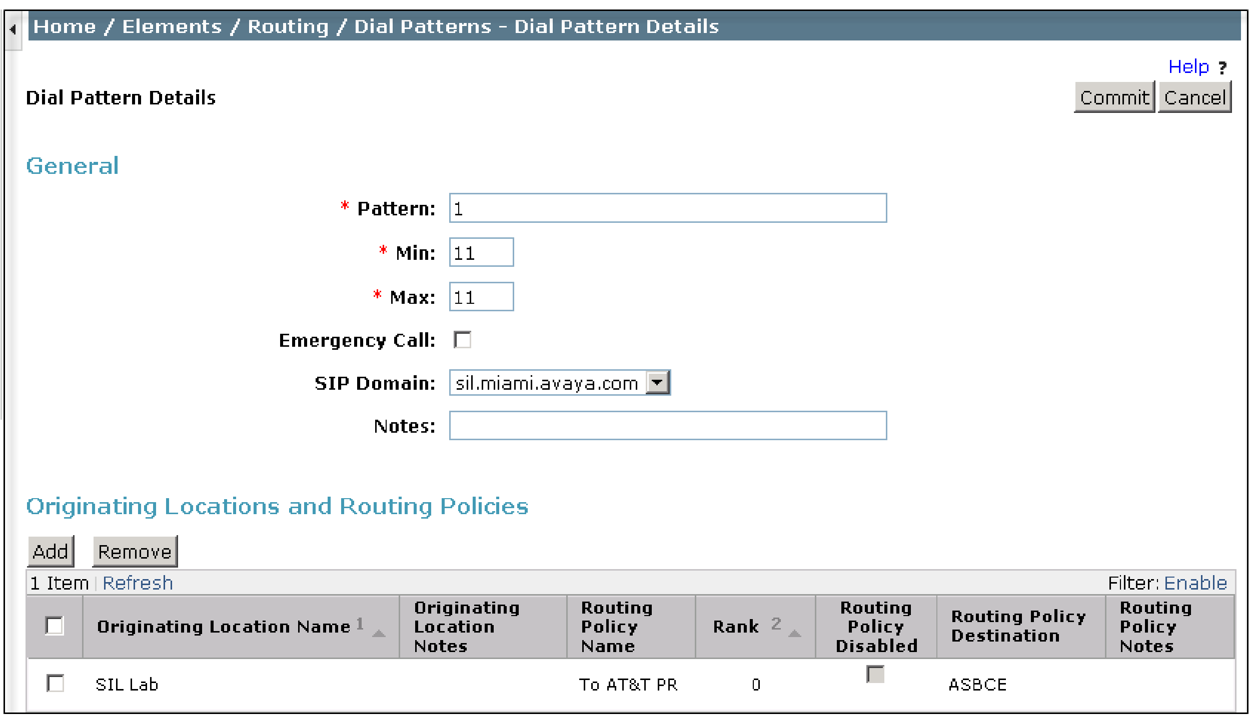
In the **General** section, enter the following values:

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

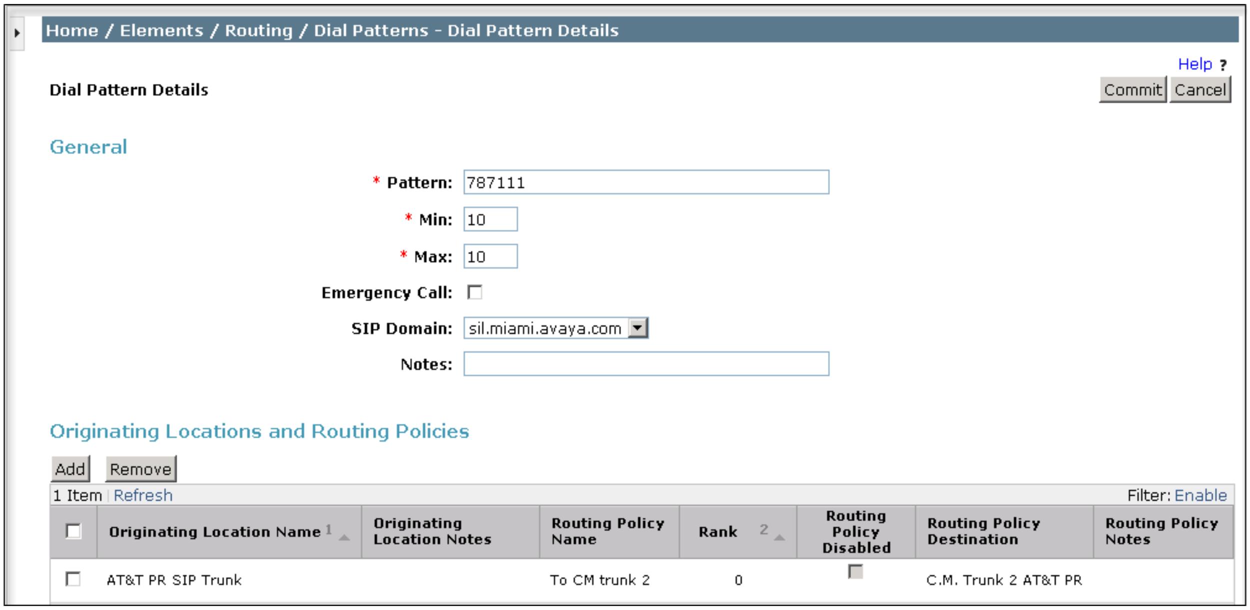
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that 11 digit dialed numbers that begin with 1 uses route policy "**To AT&T PR**".



The second example shows that a 10 digit number starting with **787111**, to domain **sil.miami.avaya.com** and originating from the **AT&T PR SIP Trunk** location, will use route policy **To CM Trunk 2**. This number falls in the DID range assigned to the enterprise by AT&T. **AT&T PR SIP Trunk** is selected for the **Originating Location** because these calls come from the SBC, which resides in that location.



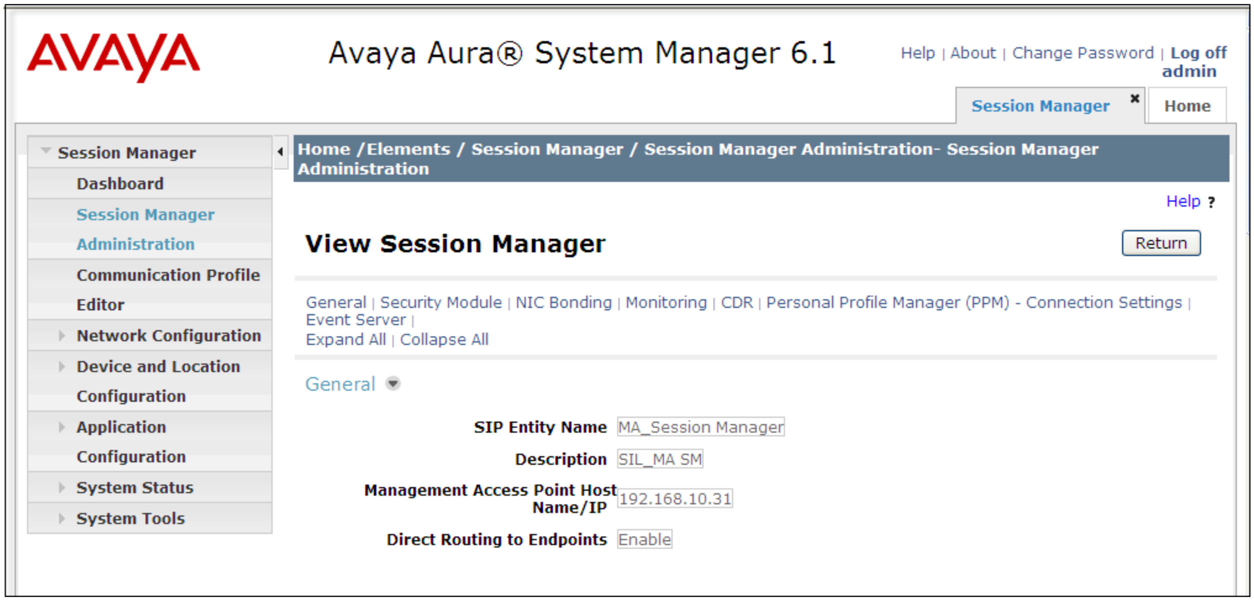
6.8. Add/View Session Manager

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

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

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

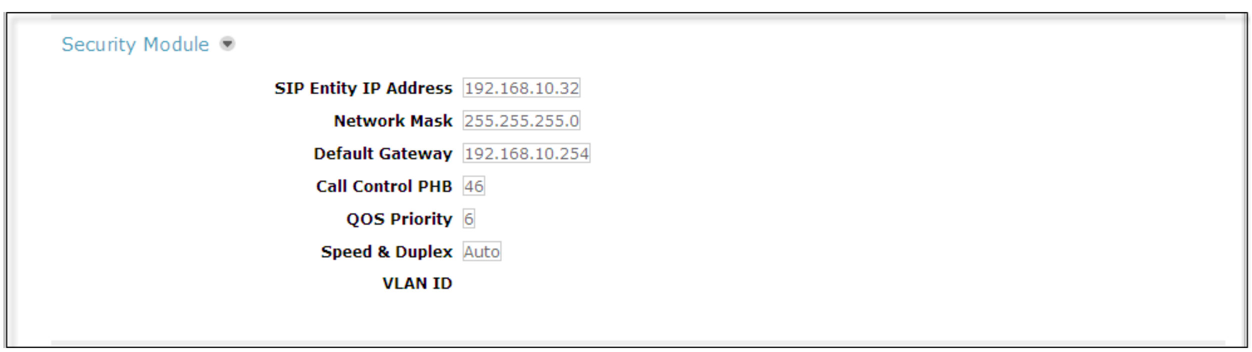
The screen below shows the Session Manager values used for the compliance test.



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

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

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



7. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to the AT&T Mobility SIP Trunk service. This configuration is done in two stages. The first part or initial configuration is done via the Provisioning Script, which requires a serial connection between a terminal device and the Console port of the SBC.

Once the SBC is provisioned and ready to be used on the IP network, the remainder of the configuration is accomplished using the SBC web interface.

It is assumed in these Application Notes that the SBC contains no previous configuration, and it is being provisioned for the first time.

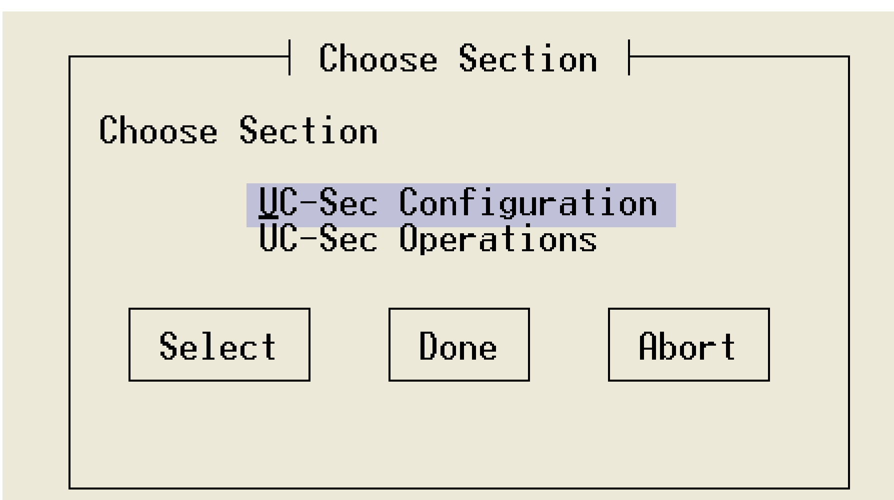
7.1. Provisioning Script

Use the following procedure to establish the initial serial connection to the Avaya SBCE:

- Connect a DB9 serial communications cable from a PC or terminal device to the Console port in the back of the SBC.
- Configure the communications parameters of the terminal program in the PC, like HyperTerminal or Putty, to the following settings: **Baud rate: 19200, Data Bits: 8, Stop Bits: 1, Parity: None**
- Apply power to the chassis.

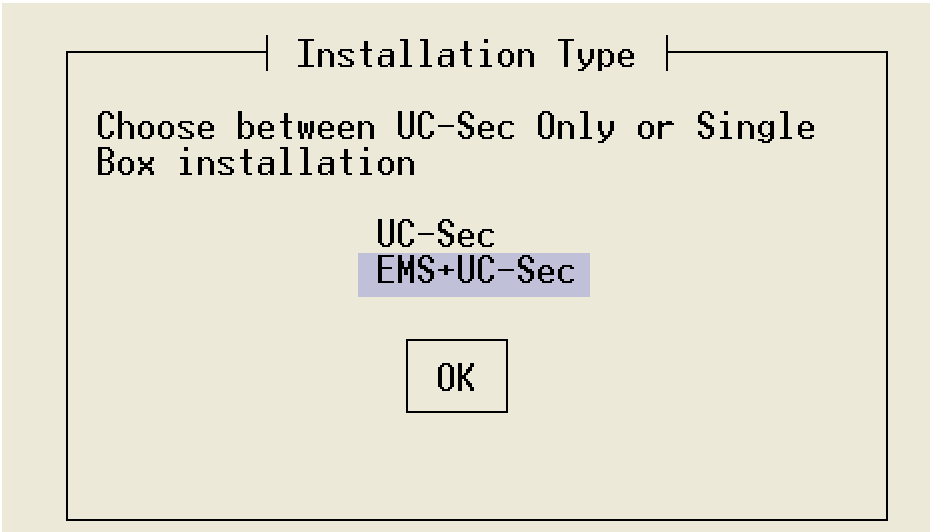
Once power has been applied to the SBC, a series of scripts run automatically preparing the chassis to be configured. The provisioning process is ready to be completed when the prompt **Press ENTER to continue…** is displayed. Press the **ENTER** key.

The Top Level Provisioning Screen is displayed. Use the arrows to select **UC-Sec Configuration** and press **ENTER**.

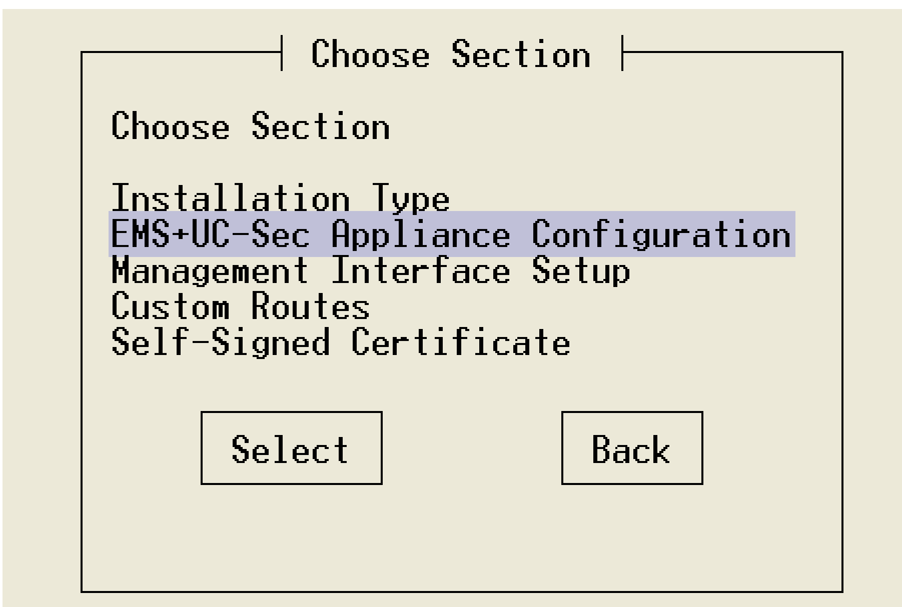


The Provisioning screen is displayed (not shown). Select **Installation Type**. Press **Select**.

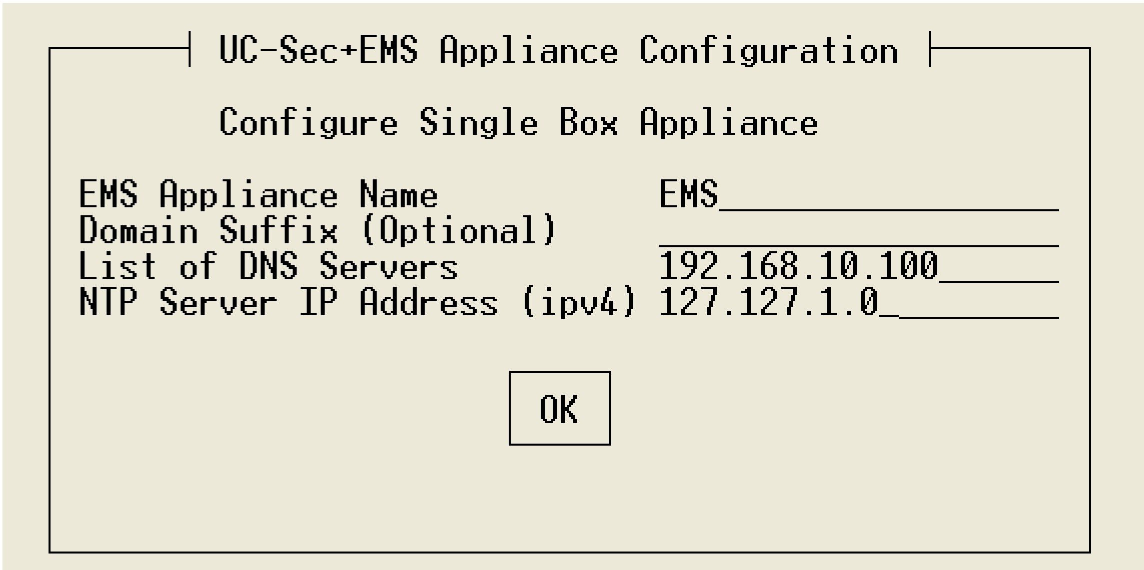
In our test scenario, both the SBC (UC-Sec) and the Element Management System (EMS) reside in the same server. Select **EMS+UC-Sec** for a single box installation. Click **OK**.



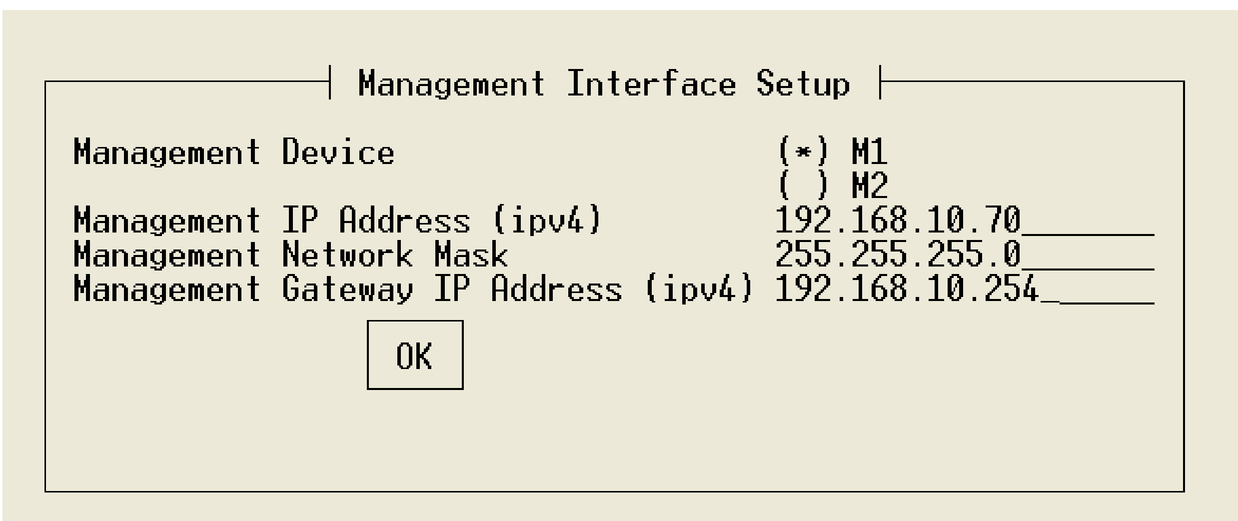
On the next screen, the EMS+UC-Sec Provisioning screen, select **EMS+UC- SEC Appliance Configuration.** Press **Select.**



Enter the required information into the appropriate fields. Click **OK**.



Back at the EMS+UC-Sec Provisioning screen shown in the previous page, select **Management Interface Setup** and press **Select**. Select the **M1 Management Device**, and enter the IP address, Netmask and Gateway to be used to manage the SBC on the network. Click **OK**.

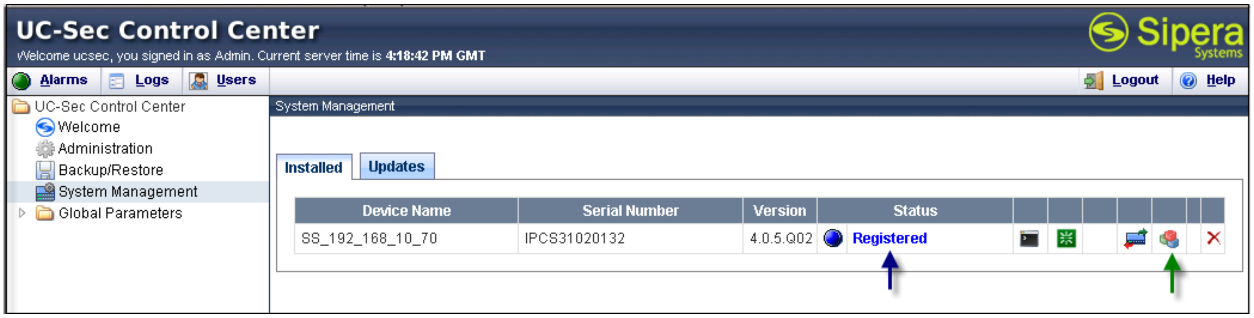


Press **Back** at EMS+UC-Sec Provisioning screen. This will bring up the Top Level Provisioning screen. Select **Done**.

At this point the initial configuration is complete and the SBC is ready to be administered via the browser through the Management Interface.

7.2. Install Device

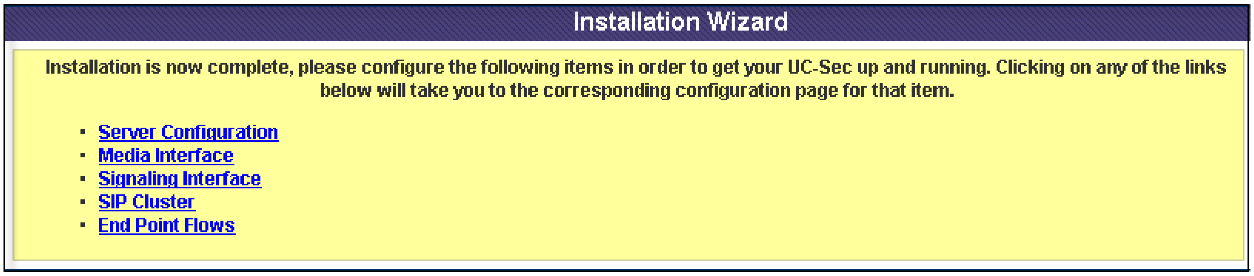
Logon to the SBC web interface pointing a browser to the previously configured management interface address. For the Compliance Test, this was **https://192.168.10.70.** Click the **UC-Sec Control Center** box. Login using the proper credentials (the GUI default password for the account "ucsec" is "ucsec"). Once in the UC-Sec Control Center home page, on the left hand side navigation panel select **System Management.** Select the **Installed** tab.



After the SBC has been initially installed and connected to the network, it will show the status of **Registered**. In addition, the **Install Device** icon, marked with a green arrow on the screen capture, is displayed only for the devices which have not yet been configured.

Click the **Install Device** icon. On the Installation Wizard that follows, fill the required information for the Appliance Name, DNS servers and the Private (A1) and Public (B1) interfaces of the SBC as shown. Click **Finish** when done.

The last screen in the Wizard is a basic reminder of topics that need to be visited in order to complete the configuration. Close this window.



7.3. Global Profiles

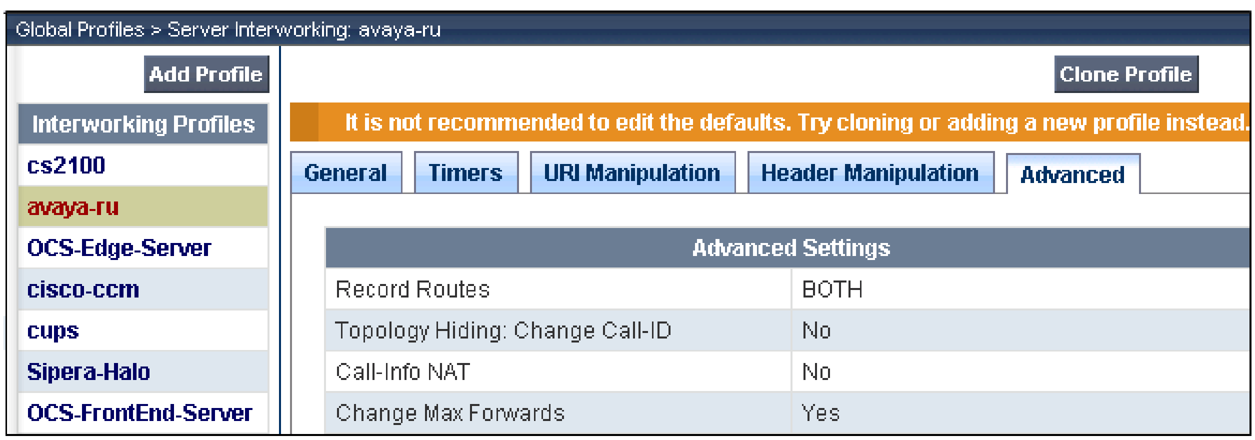
The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the EMS control.

7.3.1. Server Interworking

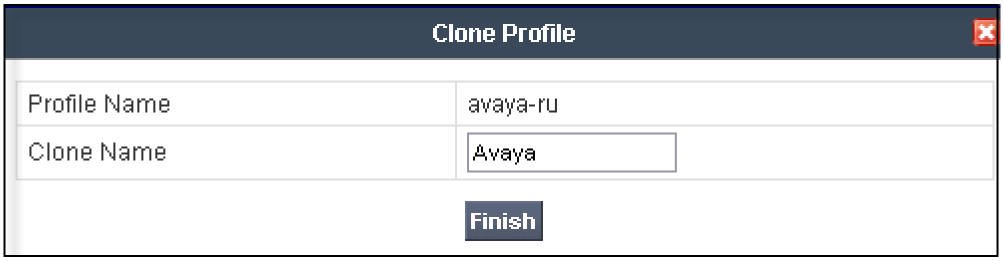
Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since modifying a default profile is generally not recommended, the default **avaya-ru** profile was duplicated, or "cloned". That way if modifications are needed in the future, they will not affect the default.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone Profile.**

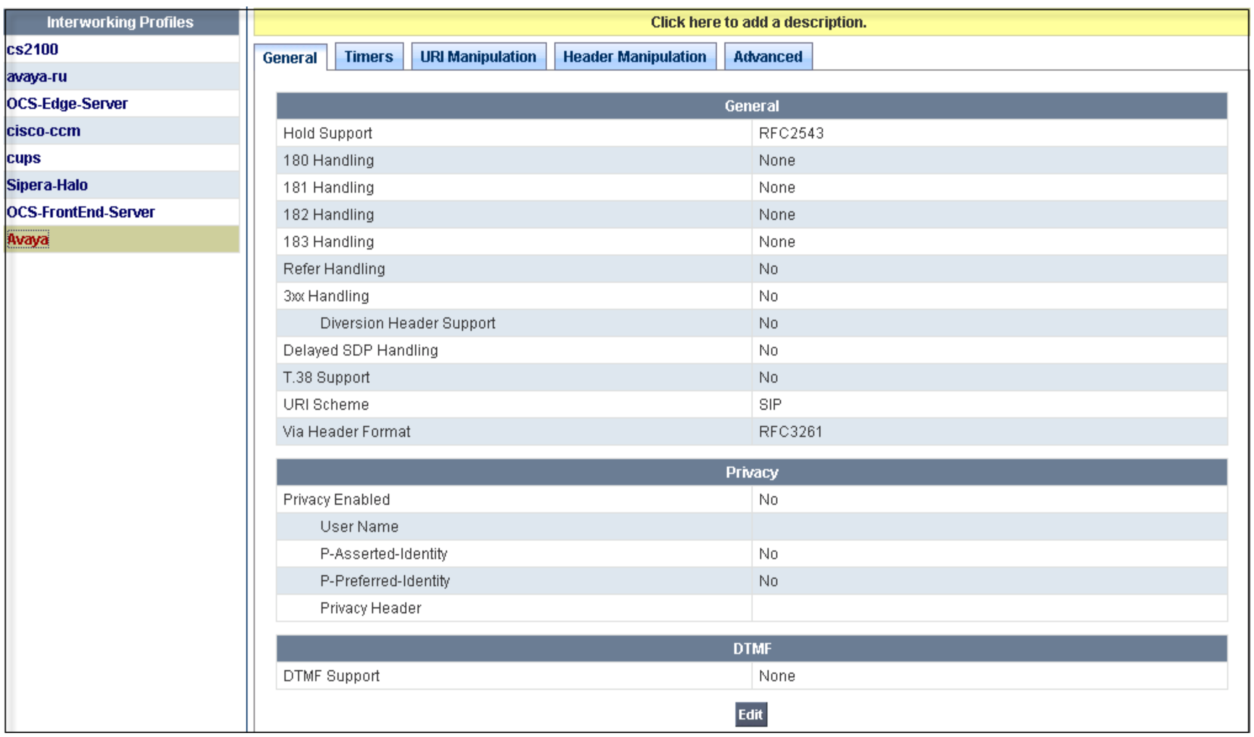


Enter the new profile name in the **Clone Name** field. Click **Finish**.



For the newly created Avaya profile, click **Edit** at the bottom of the General tab:

- Verify that for **Hold Support**, **RFC2543** is selected.
- Leave other fields with their default values.
- Click **Next**.



Click **Next** on the **Privacy** tab (not shown) and **Finish** on the **Advanced** tab to save and exit.

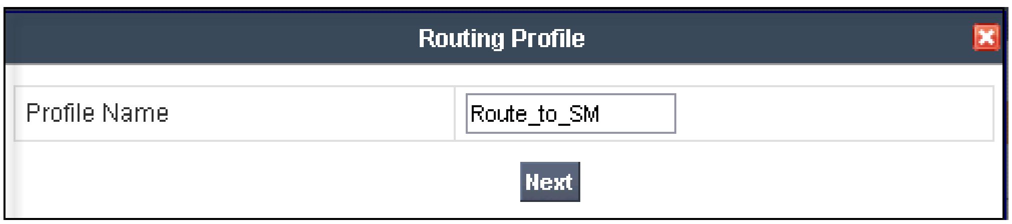
7.3.2. Routing Profiles

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

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

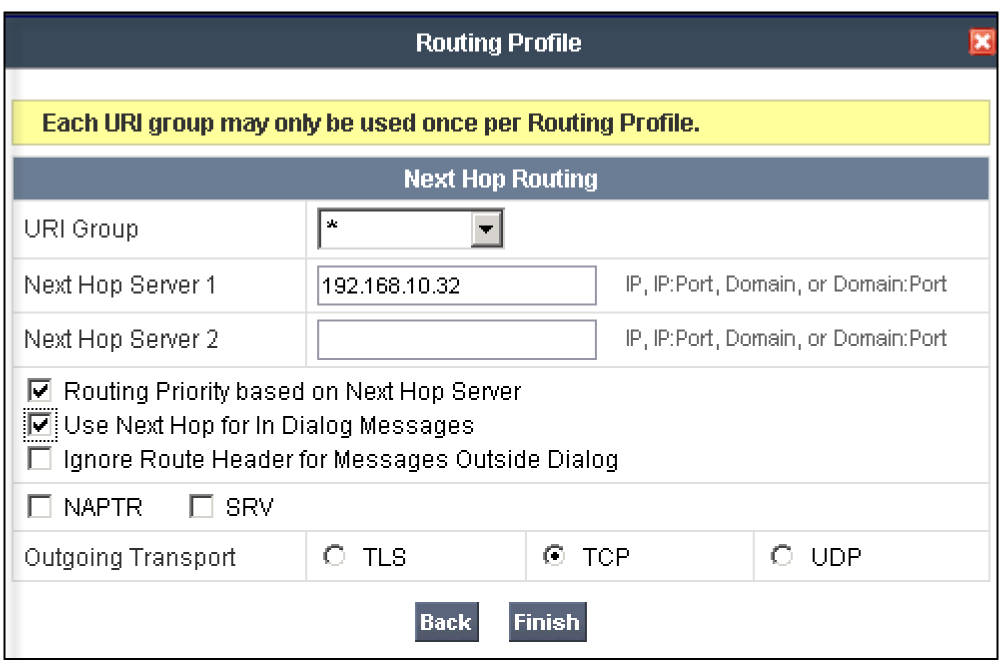
To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select the **Routing** tab.
- Select **Add Profile.**
- Enter Profile Name: **Route_to_SM.** Click **Next.**

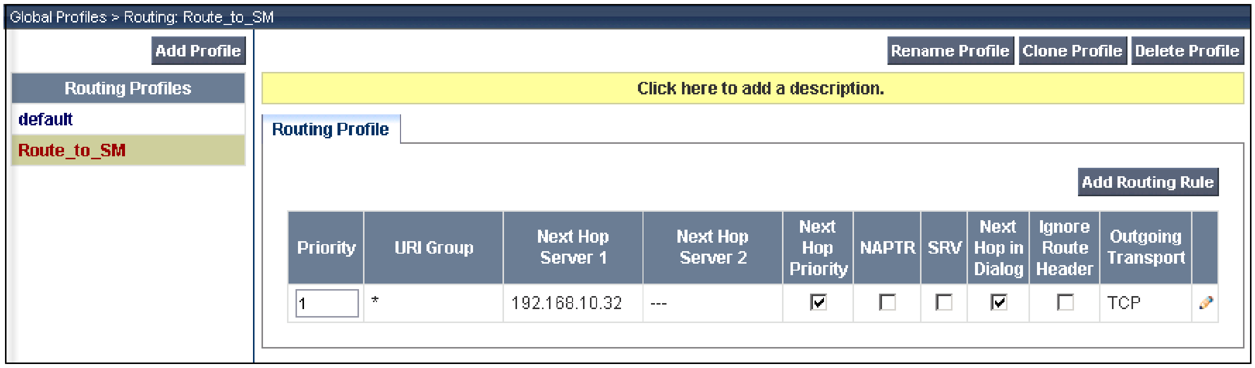


On the next screen, complete the following:

- **Next Hop Server 1: 192.168.10.32** (Session Manager IP address)
- Check **Routing Priority Based on Next Hop Server**
- Check **Use Next Hop for In-Dialog Messages**
- **Outgoing Transport: TCP**

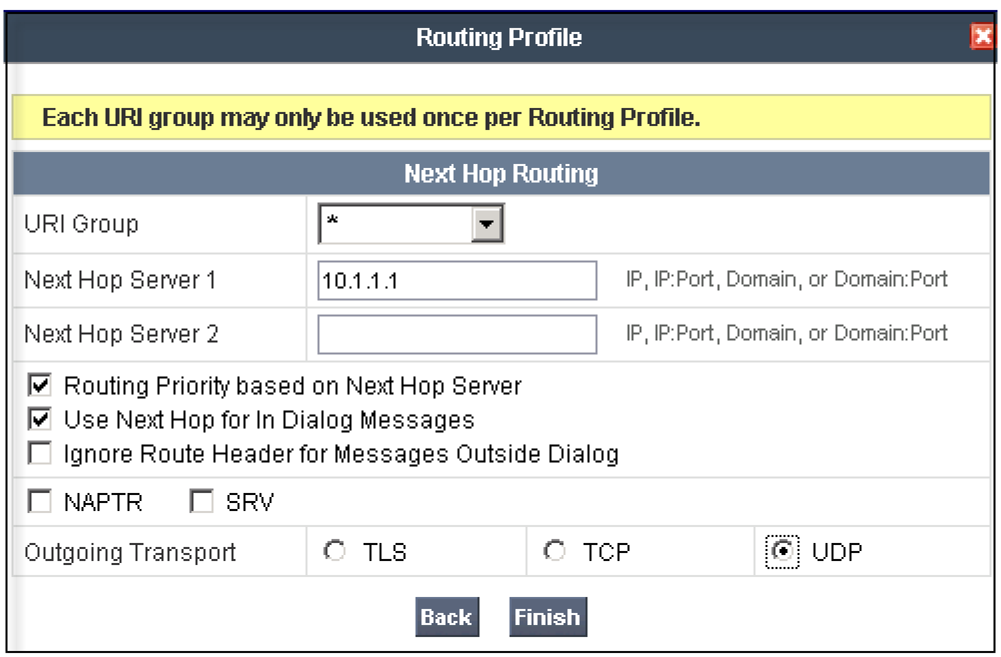


- Click **Finish**

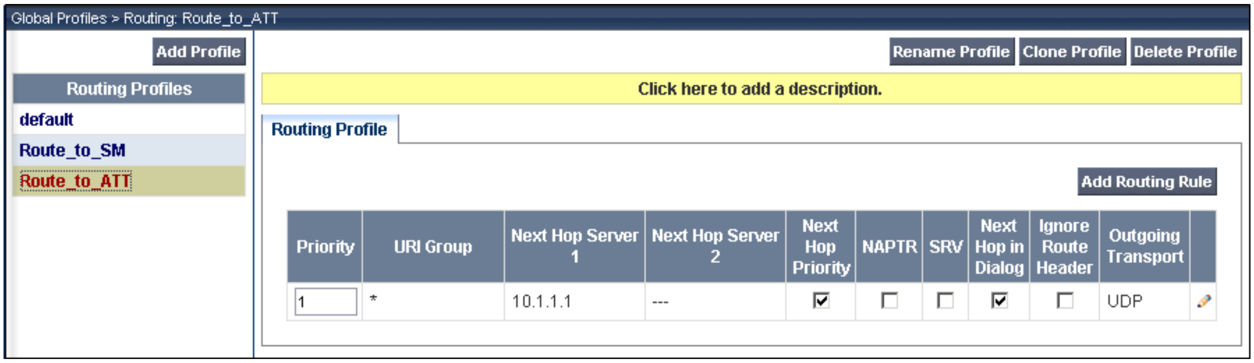


Similarly, for the outbound route:

- Select **Add Profile.**
- Enter Profile Name: **Route_to_ATT**
- Click **Next.**
- **Next Hop Server 1: 10.1.1.1** (service provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server**
- Check **Use Next Hop for In-Dialog Messages**
- **Outgoing Transport: UDP**



- Click **Finish**



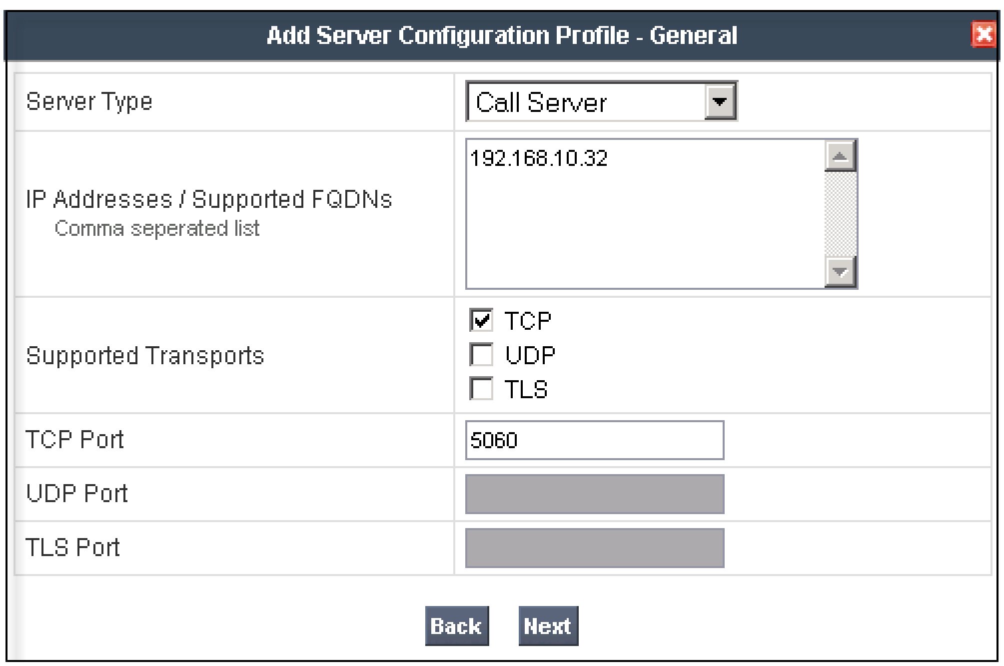
7.3.3. Server Configuration

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

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

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

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

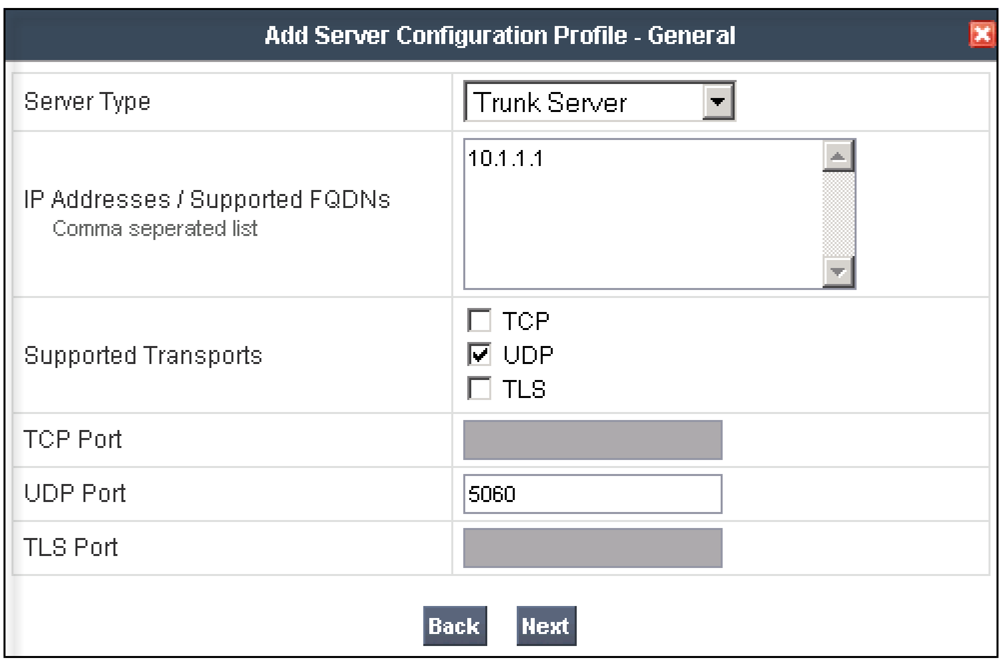


- Click **Next** on the **Authentication** tab
- Click **Next** on the **Heartbeat** tab
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None** for now. This field will be revisited and assigned a different value later in the configuration process.
- Click **Finish.**

To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** and enter the profile name: **ATT_Puerto_Rico.**

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

- Select **Server Type: Trunk Server**
- **IP Address: 10.1.1.1** (service provider's SIP Proxy IP address)
- **Supported Transports**: Check **UDP**.
- **UDP Port:5060**
- Click **Next**



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

7.3.4. Topology Hiding

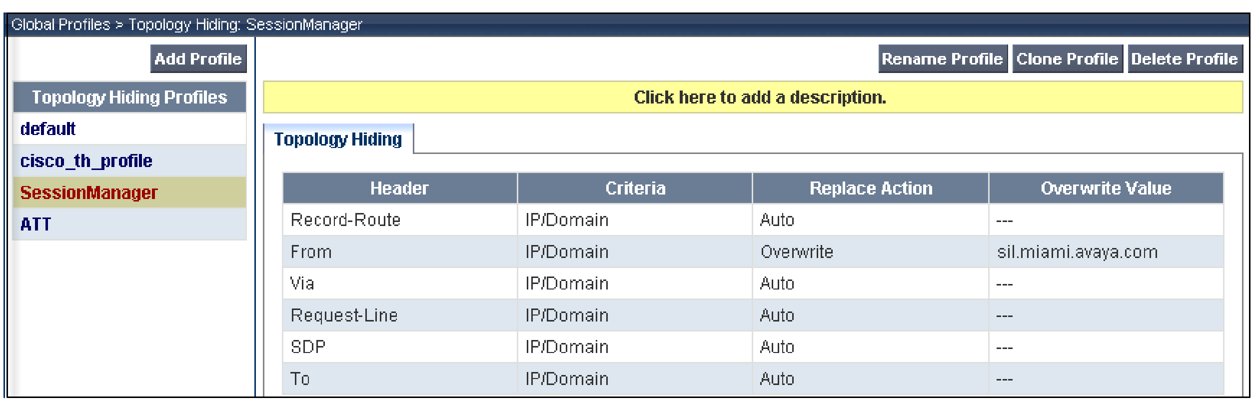
Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

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

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

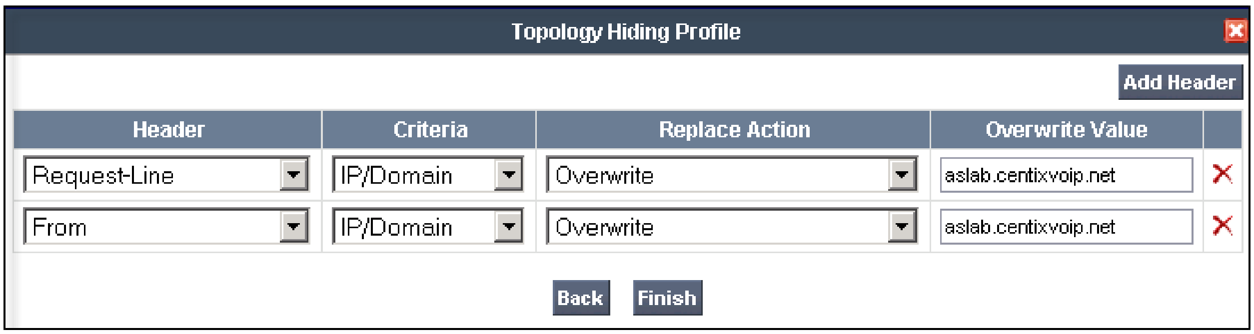
To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

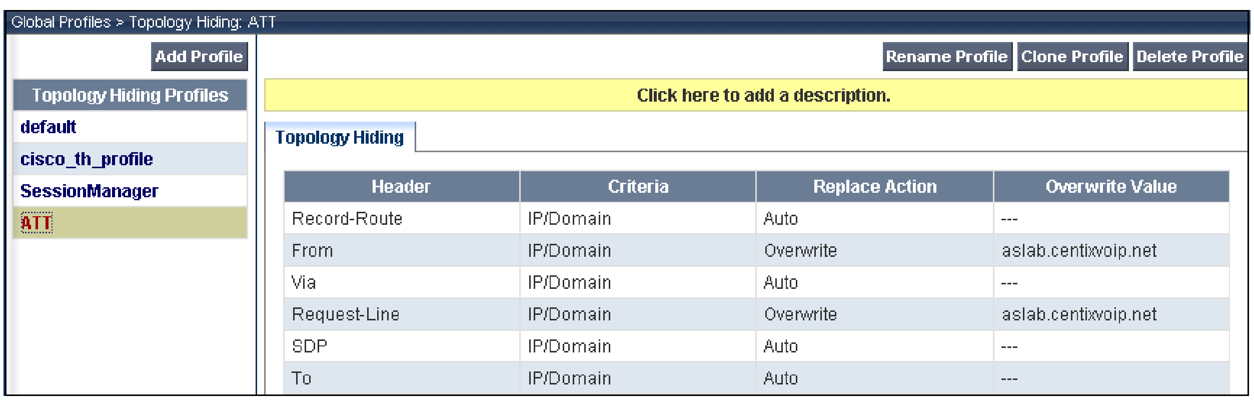
- Click **Add Profile**
- Enter the **Profile Name**: **SessionManager**. Click **Next.**
- In the **Header** column, select **From**.
- In the **Criteria** column, select **IP/Domain**
- In the **Replace Action** column, select**: Overwrite**
- In the **Overwrite Value** column, enter **sil.miami.avaya.com**, the SIP domain of the enterprise.
- Click **Finish**.



To add the Topology Hiding Profile in the SIP trunk direction:

- Click **Add Profile**
- Enter the **Profile Name**: **ATT**. Click **Next.**
- In the **Header** column, select **Request-Line**.
- In the **Criteria** column, select **IP/Domain**
- In the **Replace Action** column, select**: Overwrite**
- In the **Overwrite Value** column, enter **aslab.centixvoip.net**, the AT&T SIP domain used for the compliance test.
- Click **Add Header**.
- Select **From** in the **Header** column.
- Repeat the values shown above for **Criteria, Replace Action** and **Overwrite Value**.
- Click **Finish**





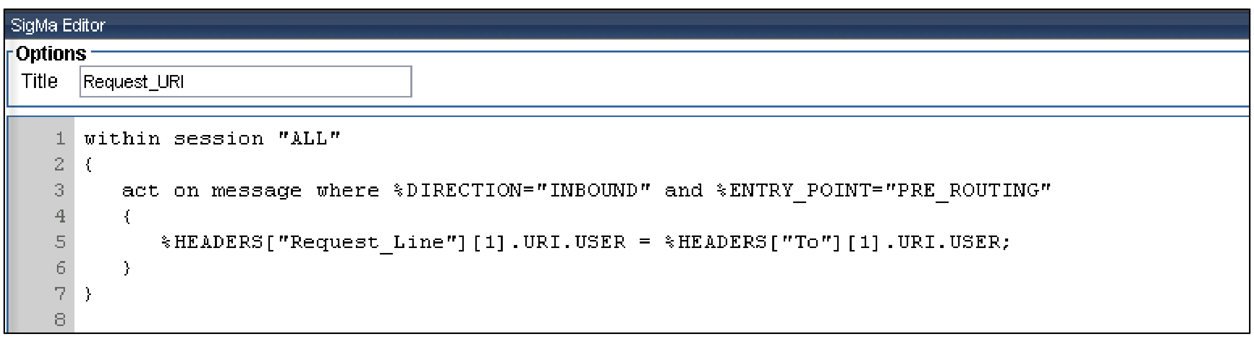
7.3.5. Signaling Manipulation

On incoming calls to the enterprise, AT&T will always send the same “pilot” DID number on the user portion of the Request-Line of any incoming request, and the actual number dialed in the user portion of the “To” header. Since Session Manager routes the calls based on the number contained in the Request-URI, it is necessary to modify the user portion of the Request-URI sent to Session Manager, to replace the “pilot” number with the actual number being called, extracted from the “To” header.

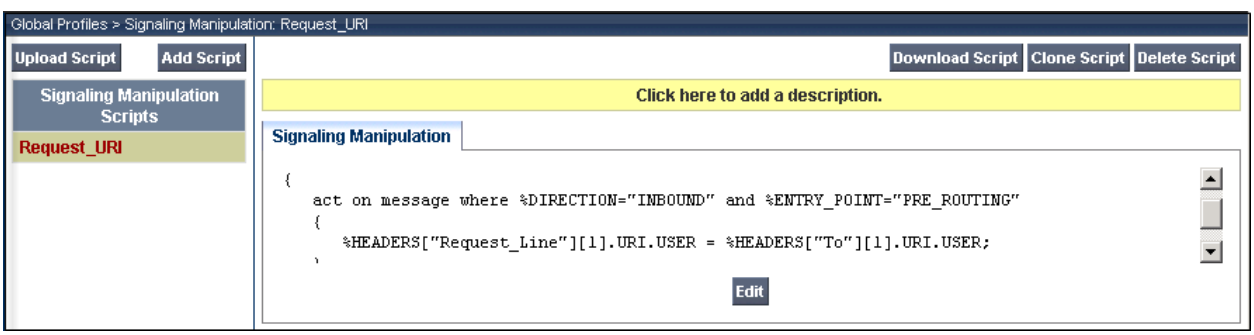
The Avaya SBCE addresses this type of granular header manipulation, which is not possible to achieve directly by configuration on the web interface, by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described above.

For more information on the structure of the SigMa Scripting Language and details on its use, see **[9]**.

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click on **Add Script** to open the SigMa Editor screen. On the **Title**, enter **Request_URI**. Enter the script as shown on the screen below:

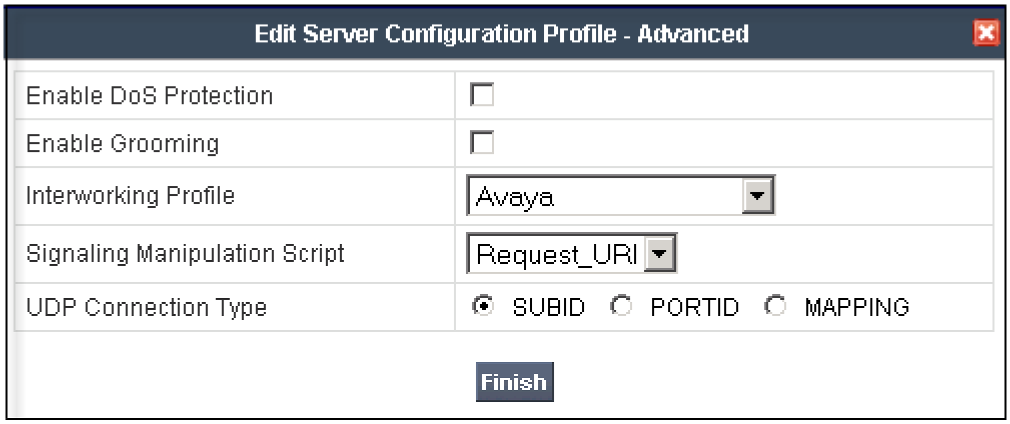


Once all the lines have been entered, click **Save** (not shown).



After the Signaling Manipulation Script is created, it should be applied to the **ATT_Puerto_Rico** Server Profile previously created in **Section 7.3.3.**

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



7.4. Domain Policies

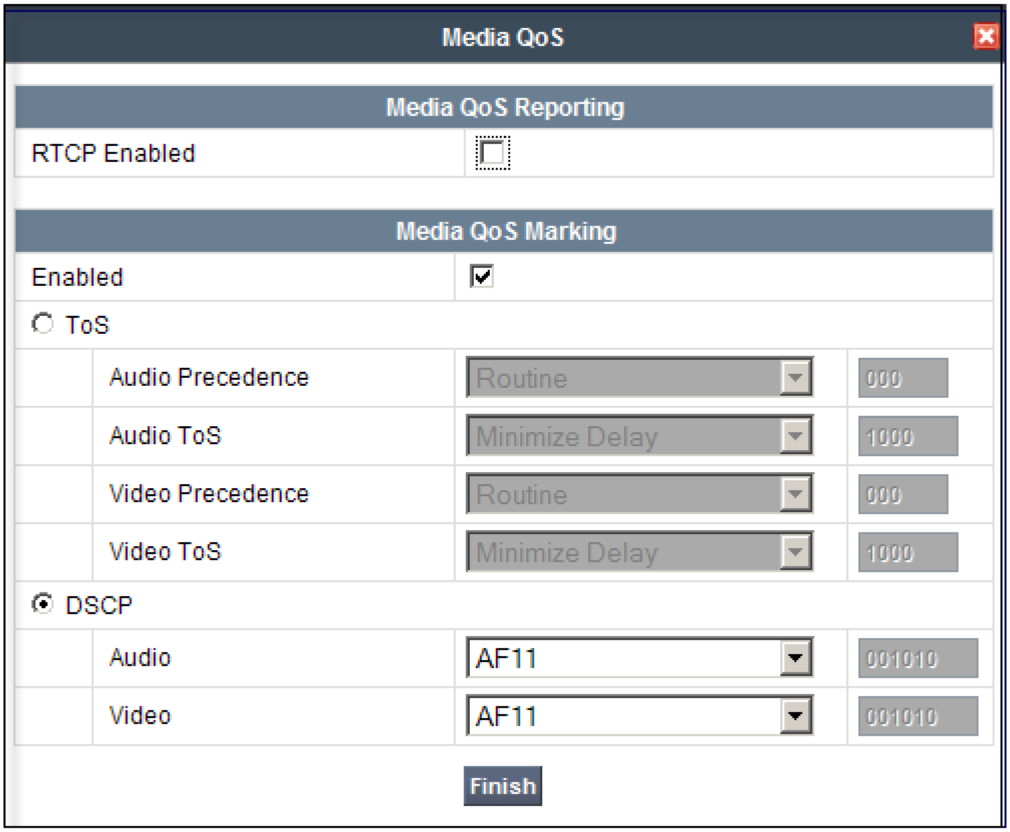
Domain Policies allow one to configure, manage and apply various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.4.1. Media Rules

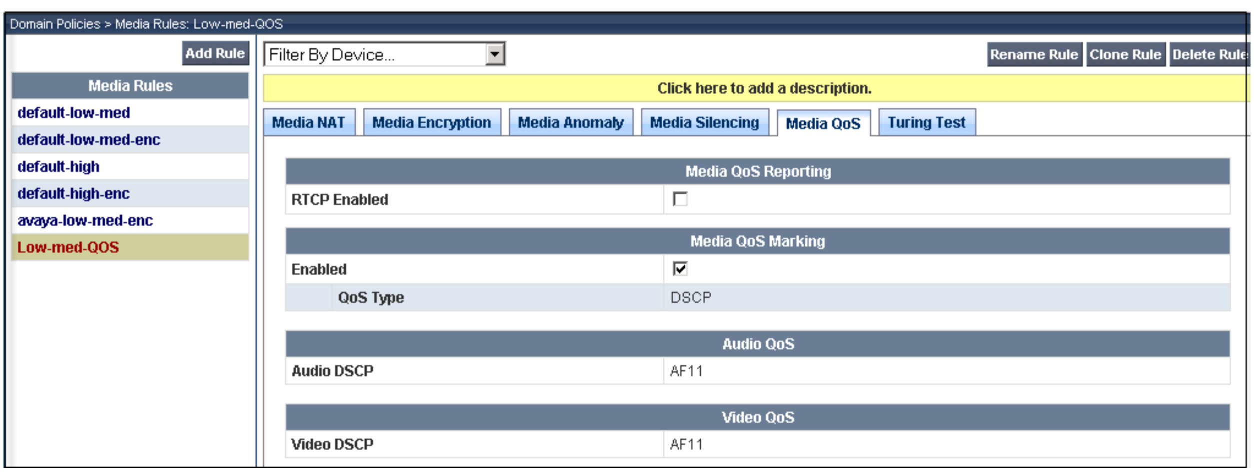
For the compliance test, a Media Rule was created to enable Quality of Service tagging of media packets. For the test, the DSCP value AF11 (Priority Traffic, High Throughput) was agreed with the service provider. On a real customer environment, this value needs to be verified and set accordingly to match the customer and service provider's requirements.

From the **Domain Policies** menu on the left-hand side, select **Media Rules.**

- Select the **default-low-med** rule from the Media Rules list.
- Select **Clone Rule** button
- Enter the **Clone Name: Low-med-QOS**
- Click **Finish**
- Highlight the rule just created: **Low-med-QOS**
- Select the **Media QOS** tab
- Click the **Edit** button
- Under **Media QOS Marking,** check the **Enabled** box.
- Check the **DSCP** box
- **Audio:** Select **AF11** from the drop-down
- **Video**: Select **AF11** from the drop-down



Click **Finish** to save the rule.



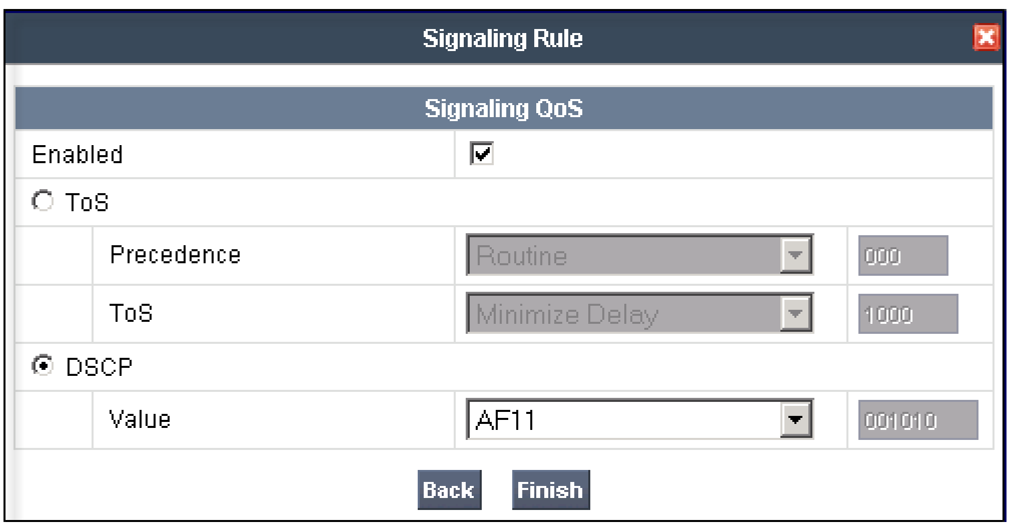
7.4.2. Signaling Rules

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

The Alert-Info and P-Location headers are sent in SIP messages from the Session Manager to the SBC and the AT&T network. They contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries. These headers need to be removed (blocked) from both requests and responses for outbound calls.

Two Signaling Rules were specified, each to be later applied in the direction of the enterprise or the SIP Trunk. To create a rule selecting the QoS type, and to block the Alert-Info and P-Location headers coming from Session Manager from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**, then **Add Rule**:

- Enter a name: **Remove_headers**. Click **Next**.
- On the next page, leave sections **Inbound**, **Outbound** and **Content-Type Policies** with their default values. Click **Next**.
- On the **Signaling QoS** screen shown below, select **DSCP** and **Value AF11** from the drop-down menu.
- Click **Finish**.

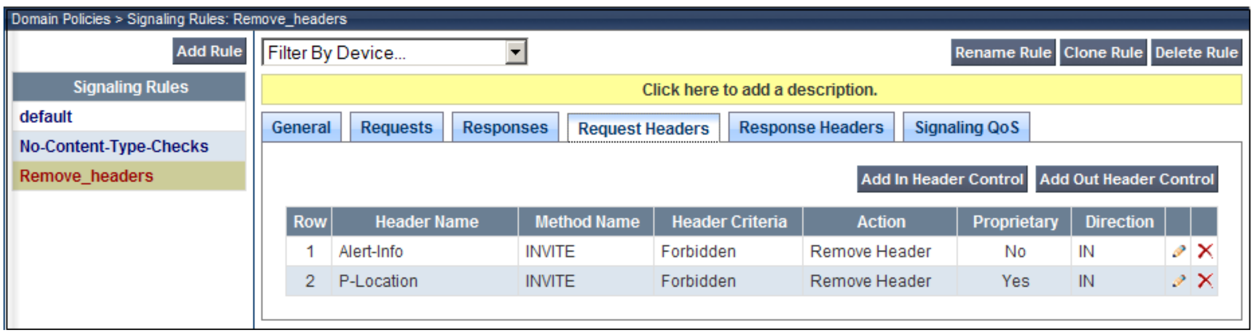


Select the **Request Headers** tab of the newly created Signaling Rule.

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

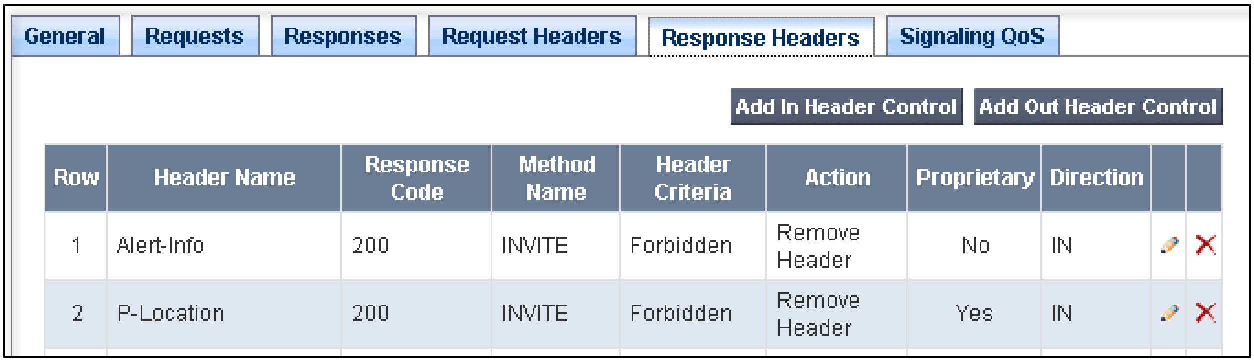
To add the P-Location header:

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



Select the **Response Headers** tab.

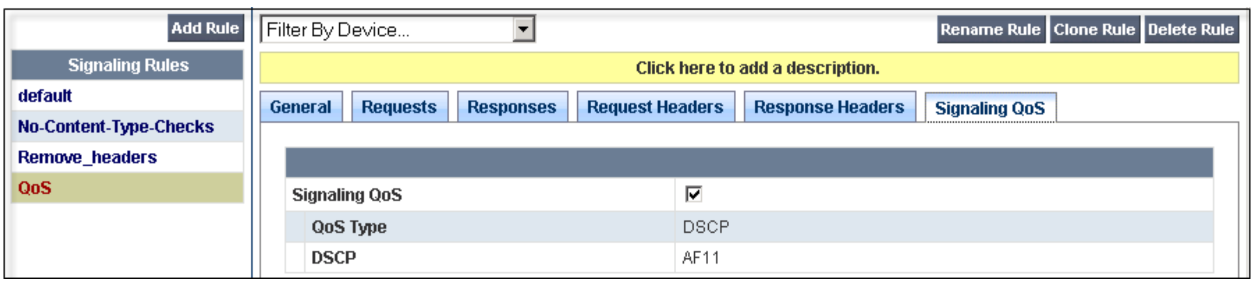
- Select **Add in Header Control**
- **Header Name: Alert-Info**
- **Response Code: 200**
- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**
- Select **Add in Header Control** one more time.
- Check the **Proprietary Request Header** box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



A second Signaling Rule was created with the purpose of defining the proper QoS type of the signaling packets traveling to the AT&T SIP Trunk.

Select **Domain Policies → Signaling Rules →Add Rule**:

- Enter a name: **QoS**. Click **Next**.
- On the next page, leave sections **Inbound**, **Outbound** and **Content-Type Policies** with their default values. Click **Next**.
- On the **Signaling QoS** screen, select **DSCP** and **Value AF11** from the drop-down menu.
- Click **Finish**.

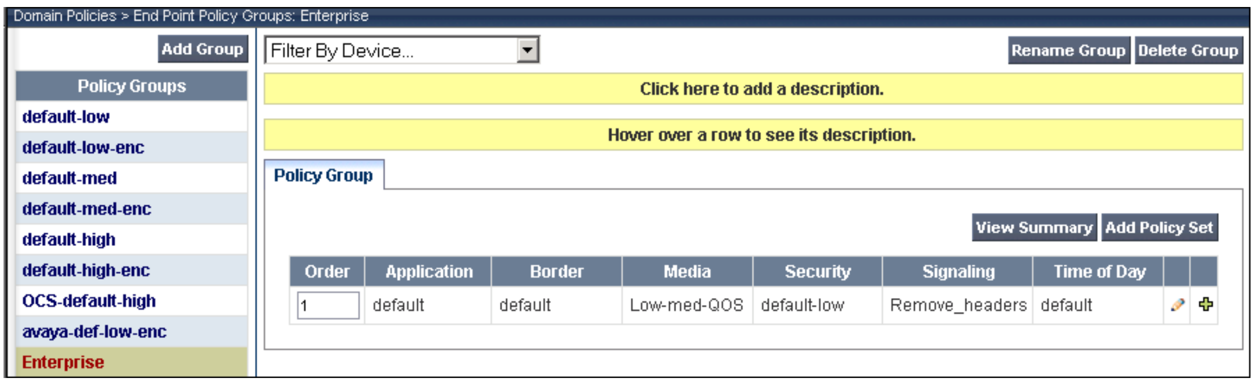


7.4.3. End Point Policy Groups

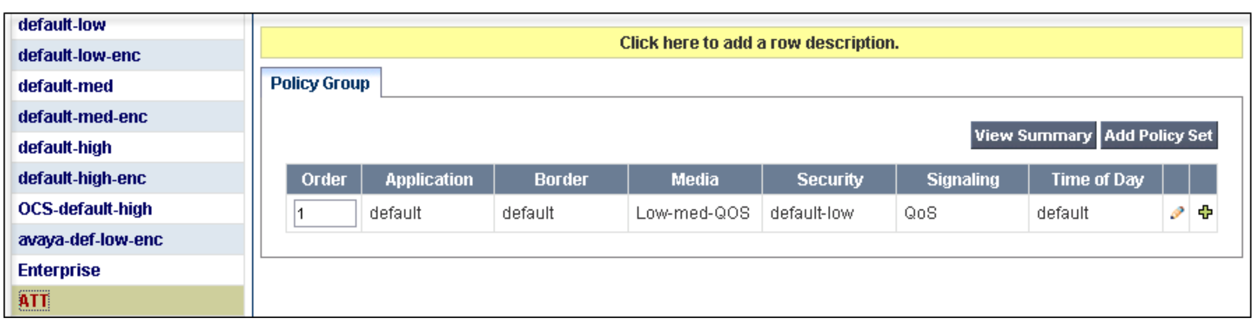
End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the SBC.

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

- **Group Name: Enterprise**.
- **Application Rule: default**
- **Border Rule: default**
- **Media Rule: Low-med-QOS**
- **Security Rule: default-low**
- **Signaling Rule: Remove_headers**
- **Time of Day: default**
- Click **Finish**.



- To create an End Point Policy Group for the AT&T SIP Trunk, select **Add Group**.
- **Group Name: ATT**.
- **Application Rule: default**
- **Border Rule: default**
- **Media Rule: Low-med-QOS**
- **Security Rule: default-low**
- **Signaling Rule: QoS**
- **Time of Day: default**
- Click **Finish**.

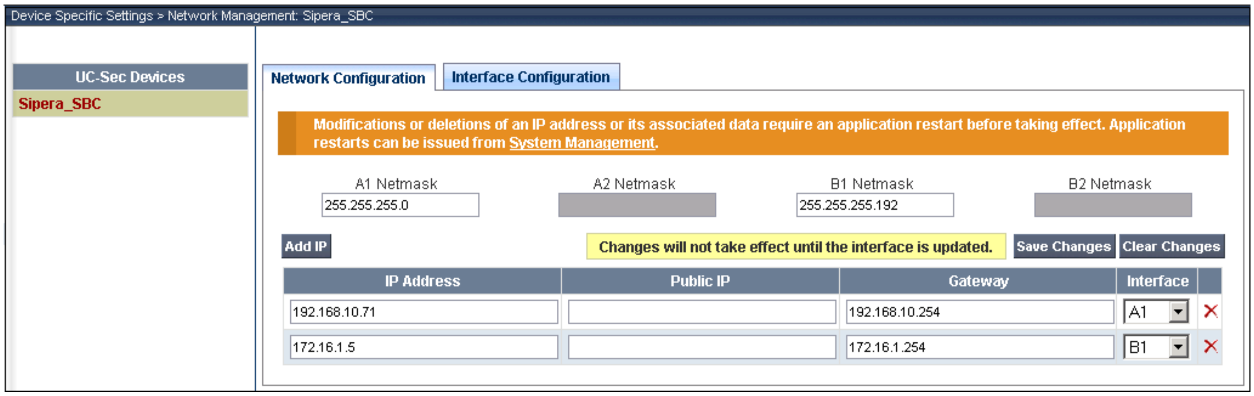


7.5. Device Specific Settings

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

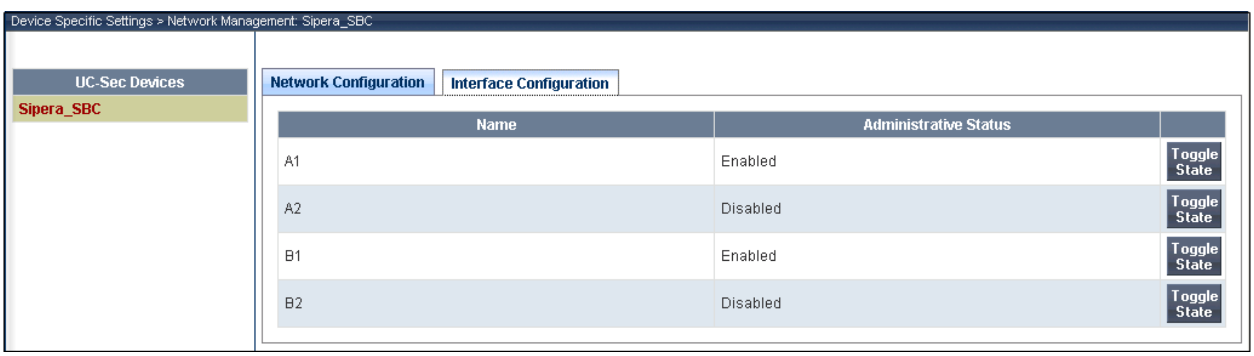
7.5.1. Network Management

The network information should have been previously completed in **Section 7.2**. To verify the network configuration, from the **Device Specific Menu** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.



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

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

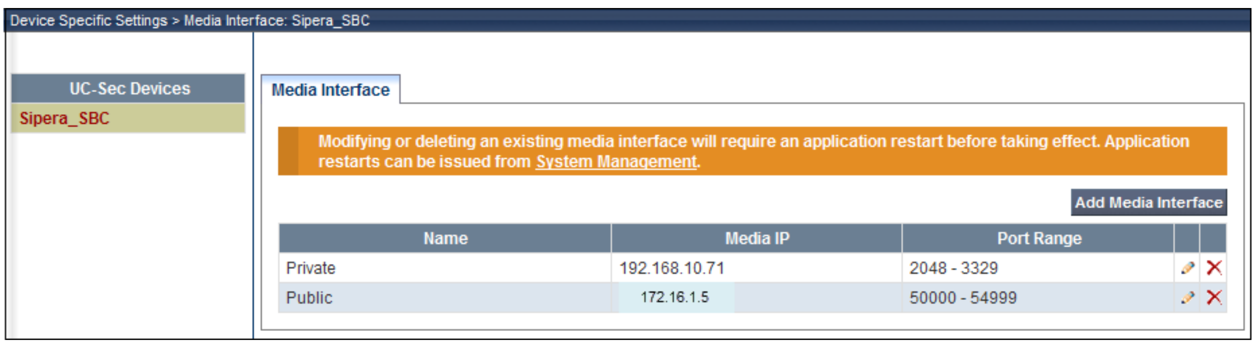


7.5.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the SBC. The Private interface of the SBC was made to match the range specified in the IP-Network-Region in Communication Manager of 2048 to 3349, and the Public interface to match the range specified by AT&T for the compliance test of 50000 to 54999.

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

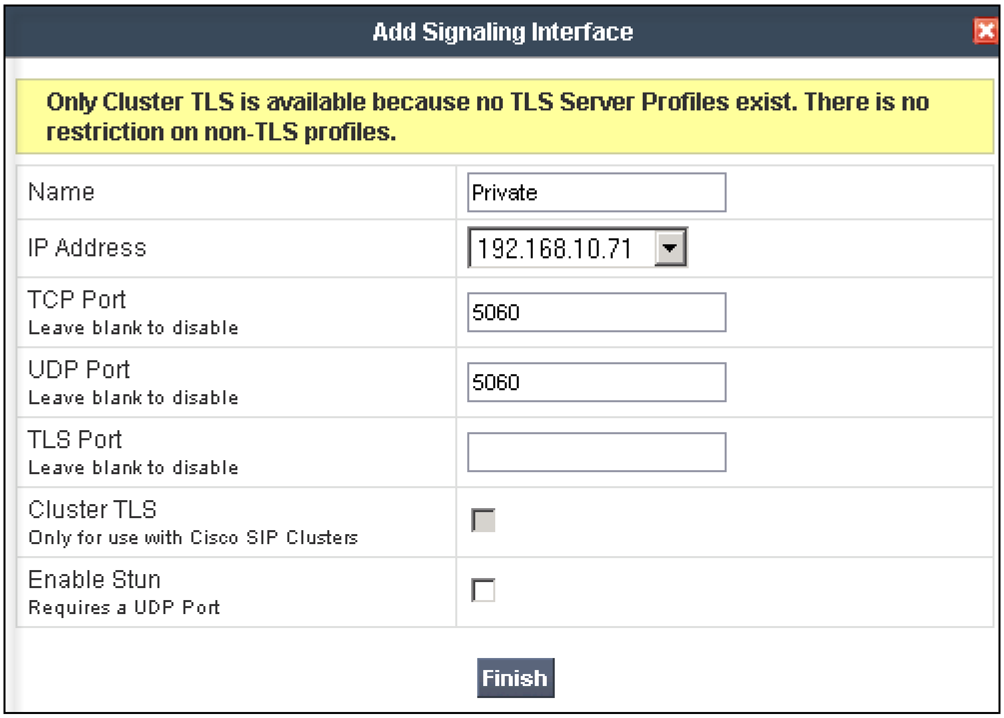
- Select **Add Media Interface**
- **Name: Private**
- **IP Address: 192.168.10.71** (Inside IP Address of the SBC, toward Session Manager)
- **Port Range: 2048-3329**
- Click **Finish**
- Select **Add Media Interface**
- **Name: Public**
- **IP Address: 172.16.1.5** (Outside IP Address of the SBC, toward AT&T)
- **Port Range: 50000-54999**
- Click **Finish.**



7.5.3. Signaling Interface

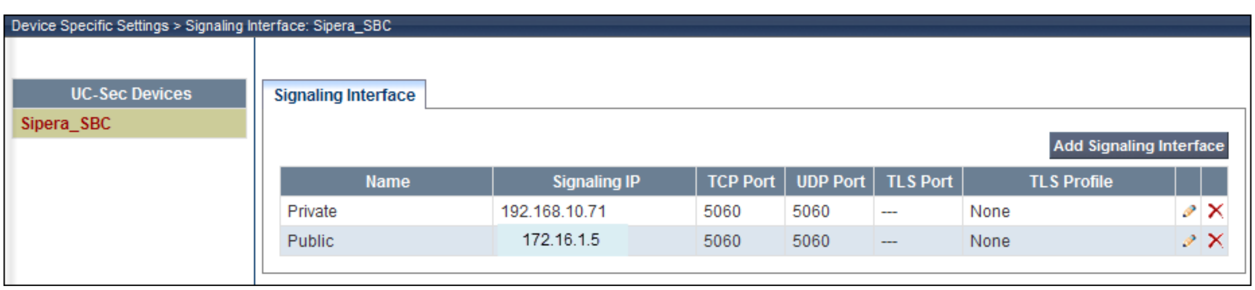
To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**, then **Add Signaling Interface**:

- **Name: Private**
- **IP Address: 192.168.10.71** (Inside IP Address of the SBC, toward Session Manager)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**



Similarly, to add the Signaling Interface toward the AT&T SIP Trunk:

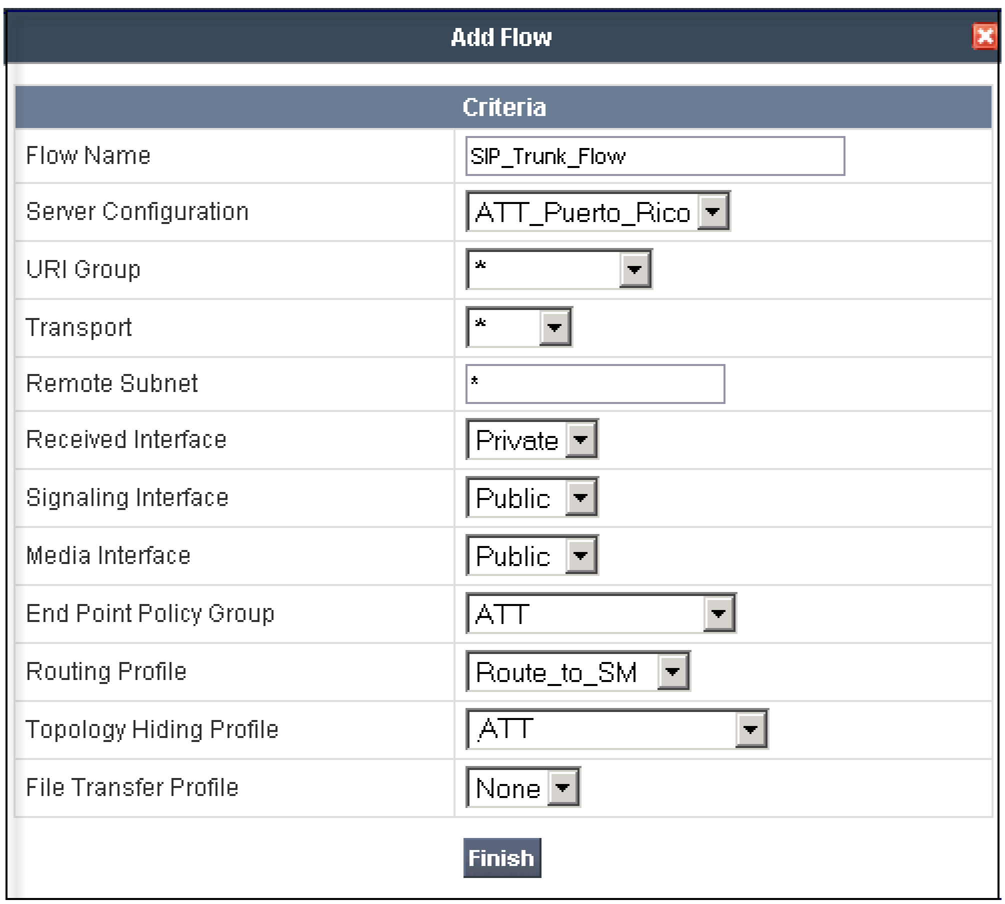
- Click **Add Signaling Interface**:
- **Name: Public**
- **IP Address: 172.16.1.5 (**Outside IP Address of the SBC, toward AT&T)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**



7.5.4. End Point Flows

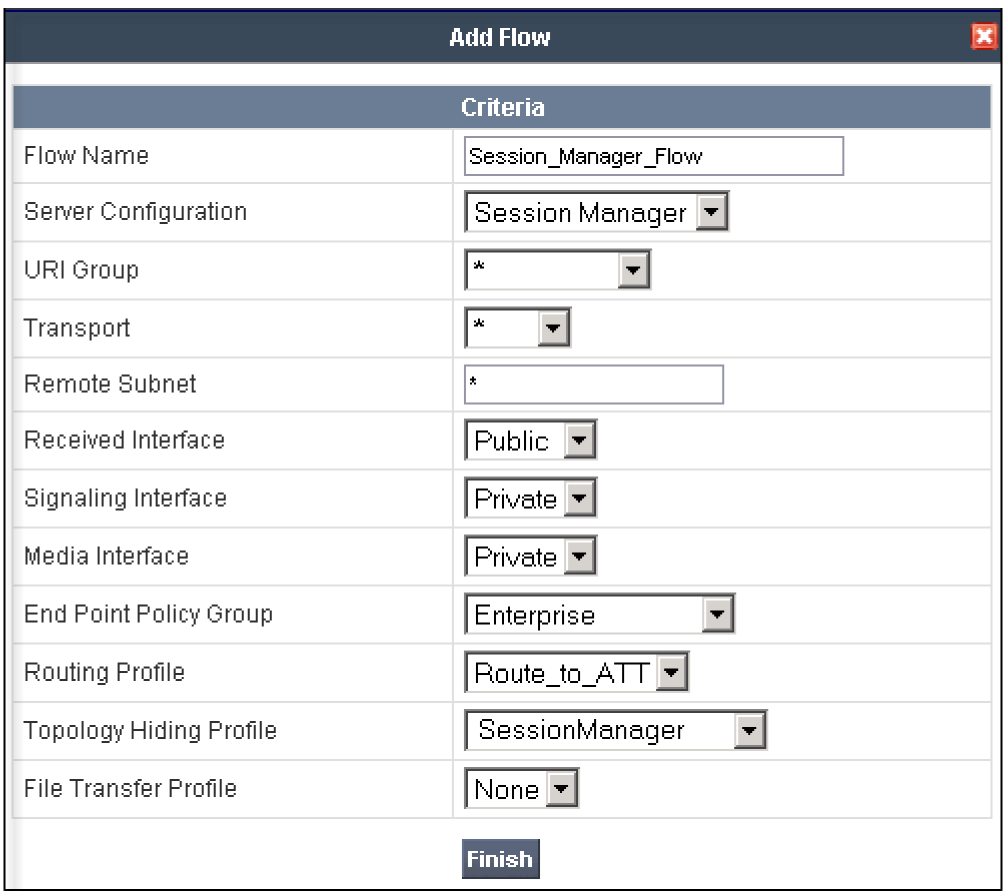
To create the call flow toward the AT&T SIP trunk, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add Flow**.

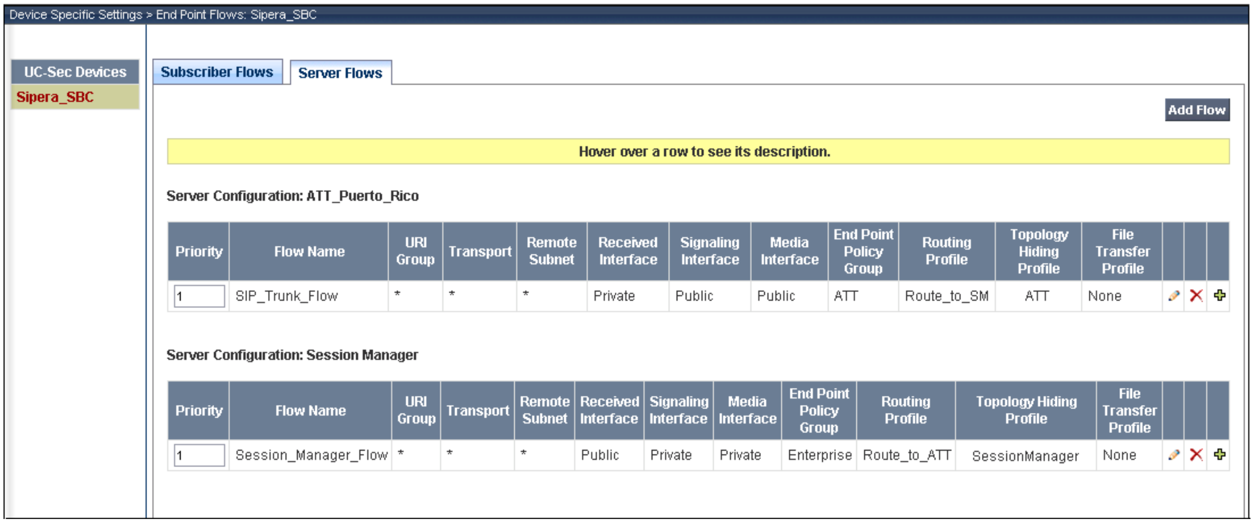
- **Name: SIP_Trunk_Flow**
- **Server Configuration**: **ATT_Puerto_Rico**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private**
- **Signaling Interface: Public**
- **Media Interface**: **Public**
- **End Point Policy Group: ATT**
- **Routing Profile: Route_to_SM**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



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

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





8. AT&T Mobility SIP Trunk Service Configuration

Information about how to establish the SIP Trunk Service with AT&T Mobility in Puerto Rico can be obtained by contacting an AT&T Mobility sales representative.

AT&T Mobility is responsible for the configuration of the AT&T Mobility SIP Trunk service in their network. To establish service, the customer will need to provide AT&T with the IP address used to reach the SBC at the enterprise. AT&T will provide the customer with the necessary information to configure the SIP connection from the enterprise site to the AT&T network, including:

- IP address of the AT&T SIP proxy.
- AT&T SIP domain.
- CPE SIP domain.
- Supported codecs.
- DID numbers
- Port numbers used for signaling and media.

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

9. Verification and Troubleshooting

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

Verification Steps:

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

Troubleshooting:

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

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

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

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

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

10. Conclusion

AT&T Mobility in Puerto Rico SIP Trunk Service passed compliance testing.

These Application Notes describe the configuration necessary to connect the above service to Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller for Enterprise.

The AT&T Mobility SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. AT&T Mobility SIP Trunk Service provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, *Release 6.0.3, February 2011*.

[2] *Administering Avaya Aura® System Platform*, *Release 6.0.3, February 2011*.

[3] *Administering Avaya Aura® Communication Manager*, *June 2010, Document Number 03-300509*.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation, June 2010,* Document *Number 555-245-205.*

[5] *Installing and Upgrading Avaya Aura® System Manager, Release 6.1*, *November 2010*.

[6] *Installing and Configuring Avaya Aura® Session Manager*, *April 2011, Document Number 03-603473.*

[7] *Administering Avaya Aura® Session Manager*, *November 2010, Document Number 03-603324*.

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

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

[10] *Sipera Systems E-SBC Release Notes. Release 4.0.5.Q02. November 2011.*

[11] *Avaya one-X® Deskphone H.323 Administrator Guide Release 6.1, May 2011, Document Number 16-300698.*

[12] *Avaya one-X® Deskphone SIP Administrator Guide Release 6.1, December 2010, Document Number 16-603838.*

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

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

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

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

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