Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Avaya Aura® Solution for Midsize Enterprise 6.1 with the AT&T Mobility SIP Trunk Service in Puerto Rico – 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 Aura® SIP-enabled enterprise solution. The Avaya solution consists of a single server containing the Avaya Aura® Solution for Midsize Enterprise 6.1 Template, an Avaya Media Gateway and different types of endpoints.

The AT&T Mobility SIP Trunk Service in Puerto Rico 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 4
2. General Test Approach and Results 4
2.1. Interoperability Compliance Testing 4
2.2. Test Results 5
2.3. Support 6
3. Reference Configuration 6
3.1. Midsize Enterprise Solution Components 8
4. Equipment and Software Validated 10
5. Configure Communication Manager 10
5.1. Licensing and Capacity 11
5.2. System Features 12
5.3. IP Node Names 13
5.4. Codecs 13
5.5. IP Network Region 14
5.6. Signaling Group 15
5.7. Trunk Group 17
5.8. Calling Party Information 19
5.9. Inbound Routing 20
5.10. Outbound Routing 21
6. Configure Avaya Aura® Session Manager 24
6.1. System Manager Login and Navigation 25
6.2. SIP Domains 26
6.3. Locations 27
6.4. Adaptations 29
6.5. SIP Entities 30
6.6. Entity Links 34
6.7. Routing Policies 36
6.8. Dial Patterns 37
7. Configure Avaya Aura® Session Border Controller 39
7.1. Installation Wizard 39
7.1.1. Network Settings 40
7.1.2. Session Border Controller Data 41
7.2. Post Installation Configuration 43
7.2.1. Options Frequency 43
7.2.2. Media Ports 45
7.2.3. Blocked Headers 46
7.2.4. Diversion Header Domain 48
7.2.5. Request URI 52
7.2.6. Refer-to Header 53
7.2.7. Save the Configuration 56
8. AT&T Mobility SIP Trunk Service Configuration 57
9. Verification and Troubleshooting 57

10. Conclusion..... 58
11. References..... 59
Appendix A: Avaya Aura® SBC Configuration File 60

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the AT&T Mobility SIP Trunk Service in Puerto Rico and the Avaya Aura® SIP-enabled enterprise solution. The Avaya solution consists of a HP® Proliant DL360 server running the Avaya Aura® Solution for Midsize Enterprise Template, release 6.1. Multiple Avaya Aura® applications are delivered as part of the Template, running as virtual machines on top of System Platform. An Avaya Media Gateway and various Avaya SIP, H.323, digital and analog endpoints are also part of the solution.

The AT&T Mobility SIP Trunk service in Puerto Rico referenced within these Application Notes is designed for enterprise business customers. Customers using this service with the Avaya Aura® SIP-enabled enterprise solution should be 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 as "AT&T".

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya Aura® Solution for Midsize Enterprise 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.

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 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 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 (1XC) 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 SIP REFER for transfer of inbound call back to 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 in Puerto Rico.
- Inbound toll-free 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:

- **Call Display on PSTN transferred calls:** Call display was not properly updated on the PSTN phone to reflect the true connected party on calls that are transferred to the PSTN from the enterprise. After the call transfer was completed, the PSTN phone showed the party that initiated the transfer instead of the actual connected party.
- **Network Call Redirection**: When a Communication Manager vector is programmed to redirect an inbound call to a PSTN number before answering the call in the vector, AT&T will send an ACK to the "302 Moved Temporarily" SIP message from the enterprise, but it will not redirect the call to the new party in the Contact header of the 302 message. The initiator of the inbound call hears silence. Network call redirection works successfully when the Communication Manager vector is programmed to redirect the inbound call to a PSTN number after answering the call first in the vector (using SIP REFER message for network call redirection instead of the 302 message).
- **Network Call Redirection using REFER with redirected part 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.

- **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.

2.3. Support

At the time of writing these Application Notes, software load 6.1.0.0.2580 of the Midsize Enterprise Solution Template, the Session Border Controller functionality is being introduced by Avaya under a Beta trial program. Customers who want to implement SBC functionality with their Midsize Enterprise Solution server, as described in these Application Notes, should contact Scott Larson with the Avaya Global Product Introduction Team at (303)538-2407 to enroll in this program.

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 the sample Avaya Aura® 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 Public SBC 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.

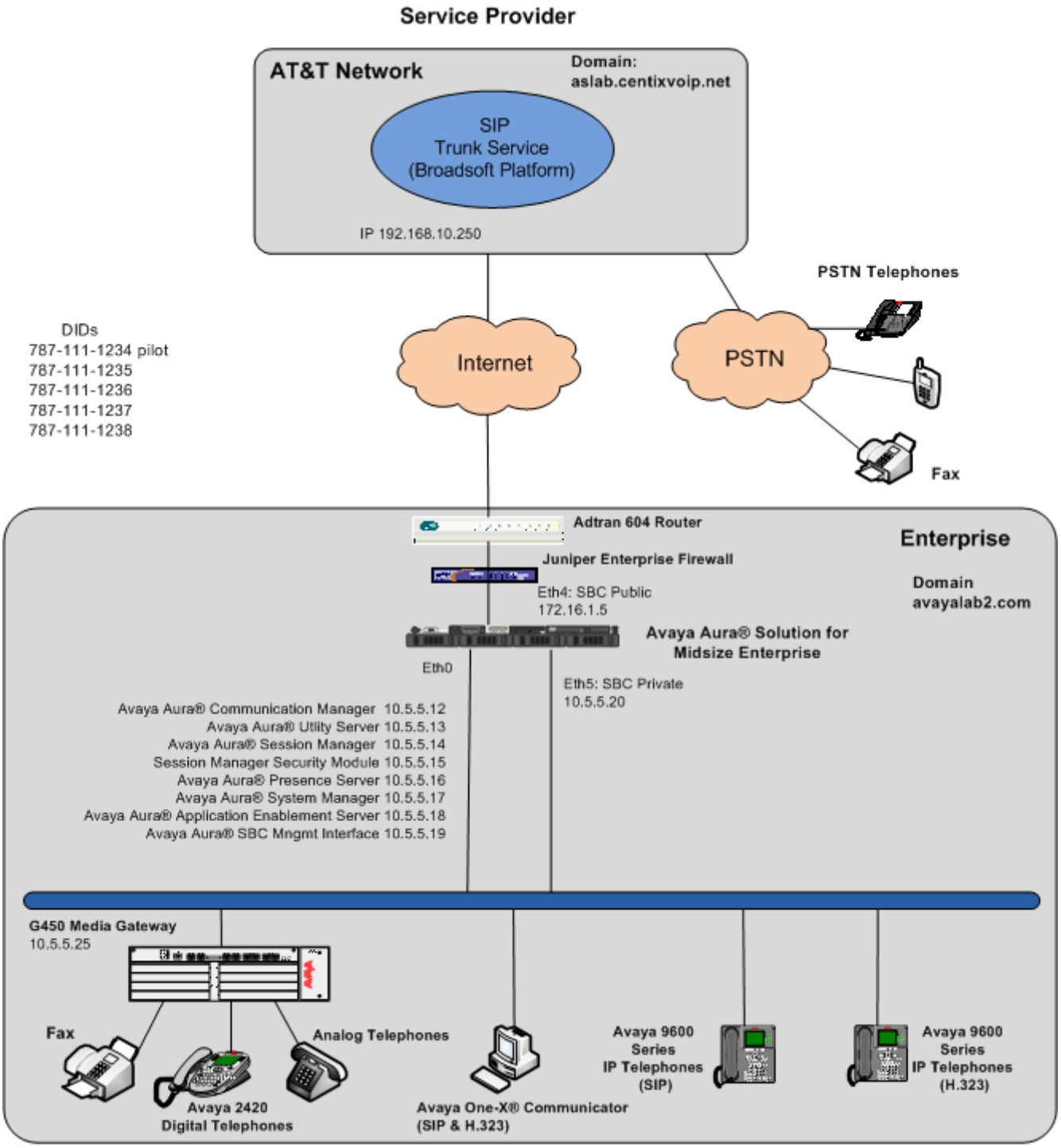


Figure 1: Avaya Aura® SIP Enterprise Solution connecting to AT&T Mobility SIP Trunk Service.

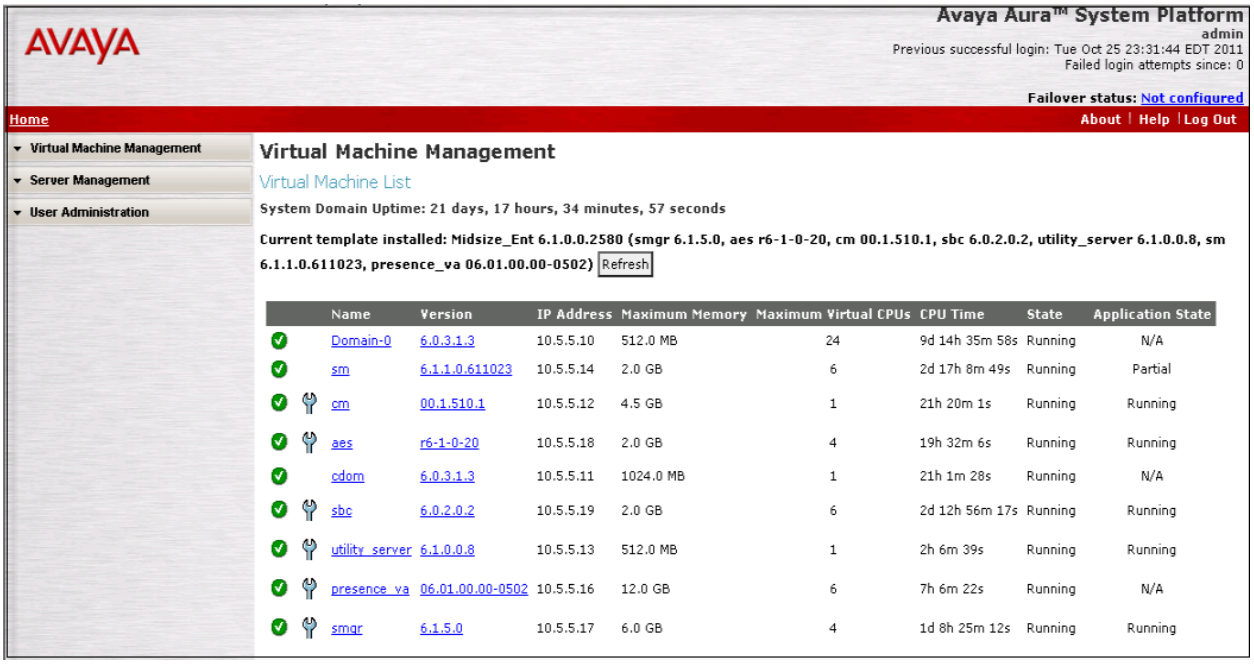
3.1. Midsize Enterprise Solution Components

The Avaya Aura® Solution for Midsize Enterprise Release 6.1 Template delivers the following applications as virtual machines running on System Platform 6.0.3:

- Communication Manager 6.0.1
- Communication Manager Messaging 6.0.1
- Session Manager 6.1
- System Manager 6.1
- Presence Services 6.1
- Utility Services 6.1
- Application Enablement Services 6.1
- Session Border Controller 6.0.2

These Application Notes will not cover the software installation of System Platform and the loading of the Midsize Enterprise Template. For more information and step by step instructions on the software installation of System Platform, the Midsize Enterprise Template and initial configuration, see [1].

The screenshot shows the list of the applications installed and running on the server, as seen from the Virtual Machine Management screen in System Platform.



Note that Application Enablement and Presence Services are installed as part of the Midsize Enterprise Template, but since these applications were not used during the compliance testing, the configuration of these services is not covered in these Application Notes.

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

- Avaya G450 Media Gateway
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones

The public interface of the Avaya Aura® SBC is located at the edge of the Enterprise, connecting to the outside network. The SBC private interface connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC also provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya Aura® SBC and AT&T Mobility across the public IP network is UDP. The transport protocol between the Avaya Aura® SBC and the enterprise Session Manager across the enterprise IP network is TCP.

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

For inbound calls, the calls flow from the service provider to the SBC, then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient of the call, in this case the Communication Manager. 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. The Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the SBC for egress to the AT&T network.

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® Solution for Midsize Enterprise on HP® Proliant DL360 G7 Server.	6.1.0.0.2580 (System Platform 6.0.3)
Avaya Aura® Communication Manager	R016x.00.1.510.1
Avaya Aura® Communication Manager Messaging	vcm-016-00.1.510.1
Avaya Aura® System Manager	6.1.0.0.7345-6.1.5.106
Avaya Aura® Session Manager	6.1.2.0.612004
Avaya Aura® Session Border Controller	6.0.2.0.2
Avaya G450 Media Gateway	31.19.2
Avaya 96xx Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 3.1
Avaya 96xx Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.6.2
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 6.0 SP5
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X® Deskphone Edition SIP 6.0.2
Avaya one-X Communicator (H.323, SIP)	6.1.1.02-SP1-32858
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

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 and administration 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 **12000** licenses are available and **263** 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
                              OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                     Maximum Administered H.323 Trunks: 12000 0
          Maximum Concurrently Registered IP Stations: 18000 2
            Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
             Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 18000 0
                  Maximum Video Capable IP Softphones: 18000 0
                     Maximum Administered SIP Trunks: 12000 263
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                            Maximum TN2501 VAL Boards: 10    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: 300   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? y
                                    Trunk-to-Trunk Transfer: all
                 Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

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



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

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

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

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

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

INTERNATIONAL CALL ROUTING PARAMETERS
                    Local Country Code: 1
               International Access Code: 011
```

5.3. IP Node Names

Use the change node-names ip command to verify that node names have been previously defined for the IP addresses of Communication Manager *(**proc**r*) and the Session Manager Security module (**SM**). 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
Acme_s0p0                 192.168.10.53
SM                        10.5.5.15
default                   0.0.0.0
me-aes                    10.5.5.18
procr                     10.5.5.12
procr6                    ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. 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 Region

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 **avayalab2.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. Note that a Session Manager Adaptation (**Section 6.4**) is used to convert this shared domain name to the specific domain expected by AT&T.
- 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: avayalab2.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: 65535
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
```

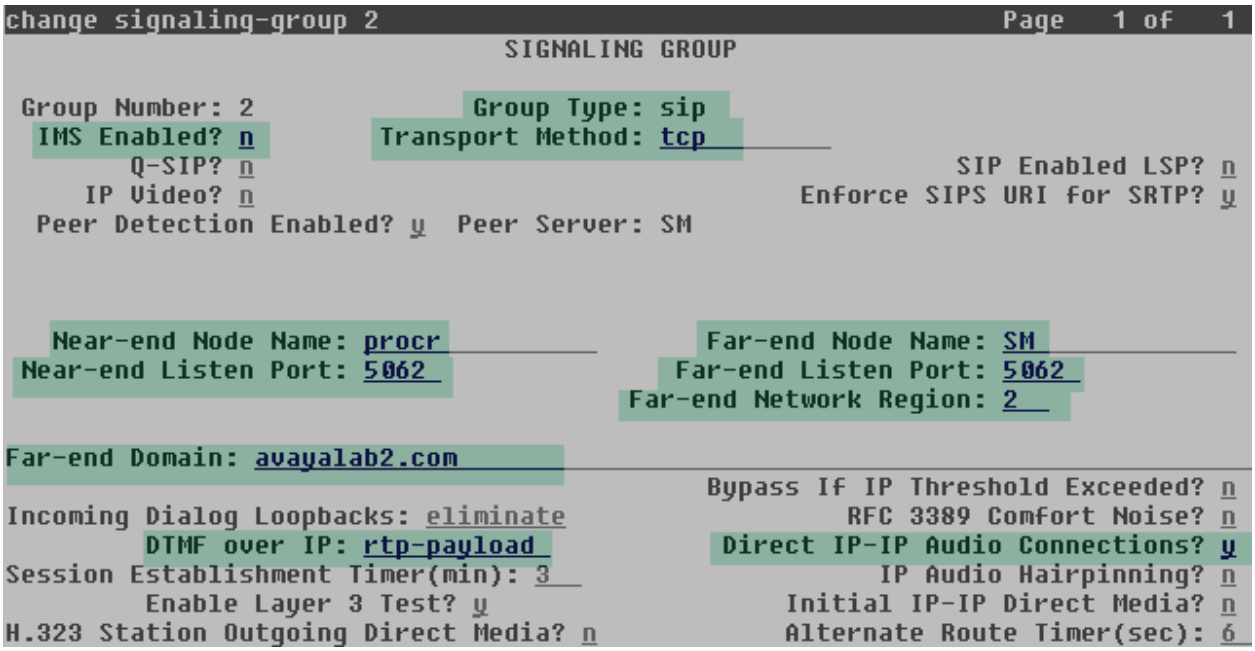
On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows 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
```

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 ***5062***. (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 ***SM***. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.



- Set 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. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- 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 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
```

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, 55001 to 55005. These same 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 5                                    Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext  Ext              Trk        Private          Total
Len  Code             Grp(s)     Prefix           Len
 5   1                                            5     Total Administered: 13
 5   2                                            5        Maximum Entries: 540
 5   5                                            5
 5   55001            2          7871111234       10
 5   55002            2          7871111235       10
 5   55003            2          7871111236       10
 5   55004            2          7871111237       10
 5   55005            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 5-digit extension length, beginning with 5, will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 5                                    Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext  Ext              Trk        Private          Total
Len  Code             Grp(s)     Prefix           Len
 5   5                2          78711            10    Total Administered: 13
                                                          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  55001
 public-ntwrk     10 7871111235        10  55002
 public-ntwrk     10 7871111236        10  55003
 public-ntwrk     10 7871111237        10  55004
 public-ntwrk     10 7871111238        10  55005
 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 78711             5
 public-ntwrk
 public-ntwrk
```

5.10. Outbound Routing

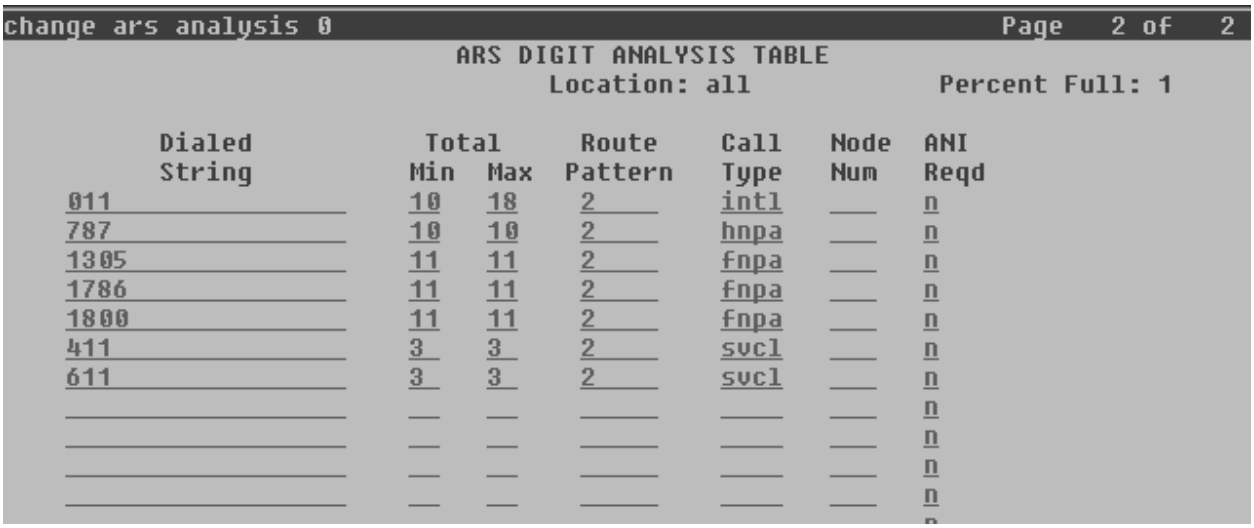
In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration 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
   0        1      attd
   1        5      ext
   2        5      ext
   3        5      ext
   4        5      ext
   5        5      ext
   6        3      dac
   7        5      ext
   8        5      ext
   9        1      fac
   *        3      dac
   #        3      dac
```

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

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

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9    Access Code 2:
                  Automatic Callback Activation: *33   Deactivation: #33
Call Forwarding Activation Busy/DA: *30   All: *31   Deactivation: #30
   Call Forwarding Enhanced Status:    Act:         Deactivation:
                        Call Park Access Code: *40
                      Call Pickup Access Code: *41
```

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**: **none**. If desired, one or more alternate Communication Manager trunks can be listed in the route pattern so that the Look-Ahead Routing (**LAR**) "**next**" setting can route-advance to attempt to complete the call using alternate trunks, should there be no response or an error response is received from the far-end. For the compliance test, since only one trunk group was used, the default value **none** was selected.

```
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   none
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

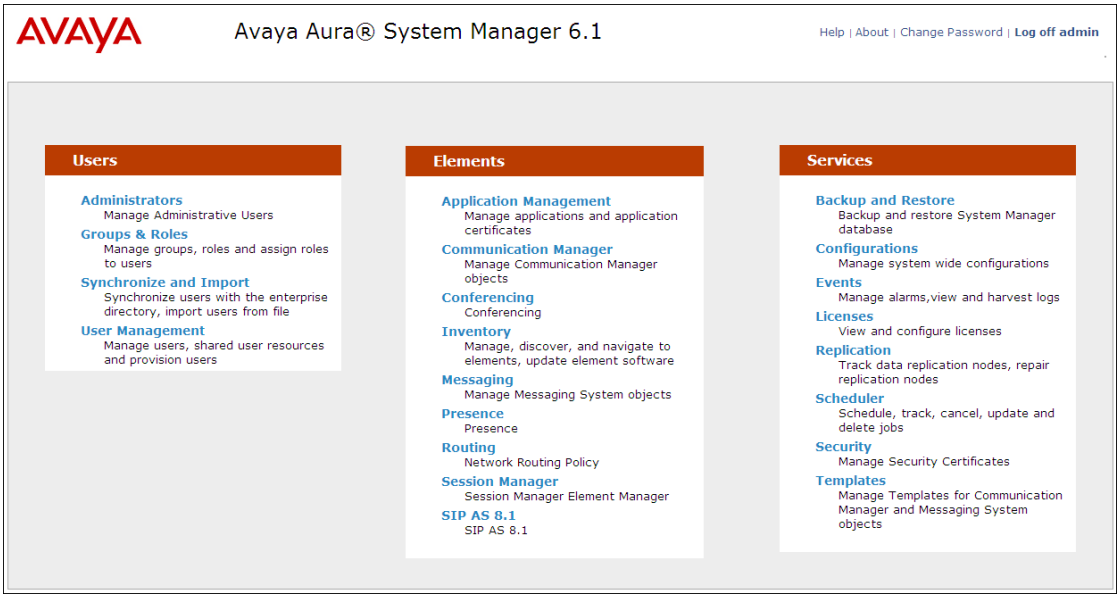
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

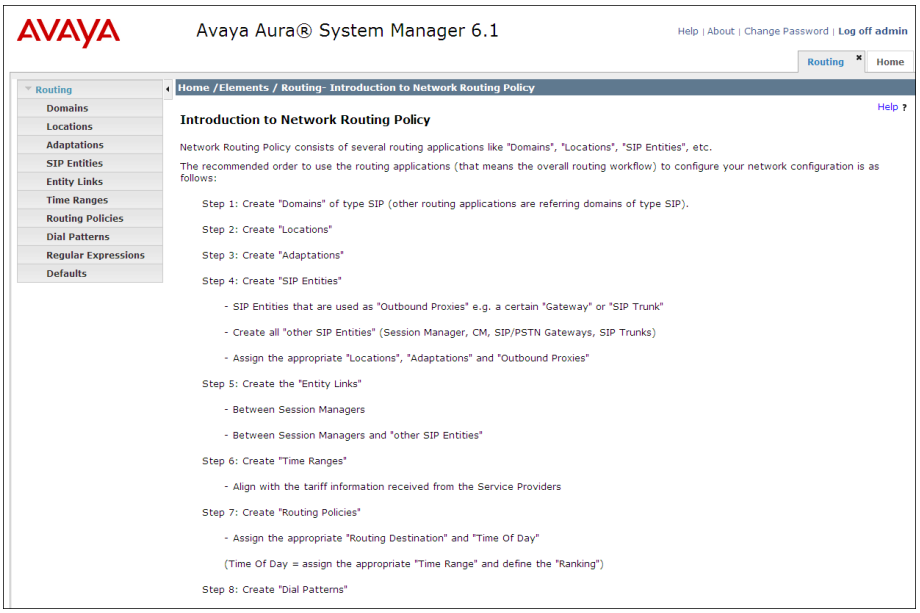
It may not be necessary to create all the items above when creating a connection to the service provider, since some of them would have already been defined as part of the initial Midsize Enterprise Solution template installation. This includes entries such as certain SIP domains, locations, SIP entities, 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.

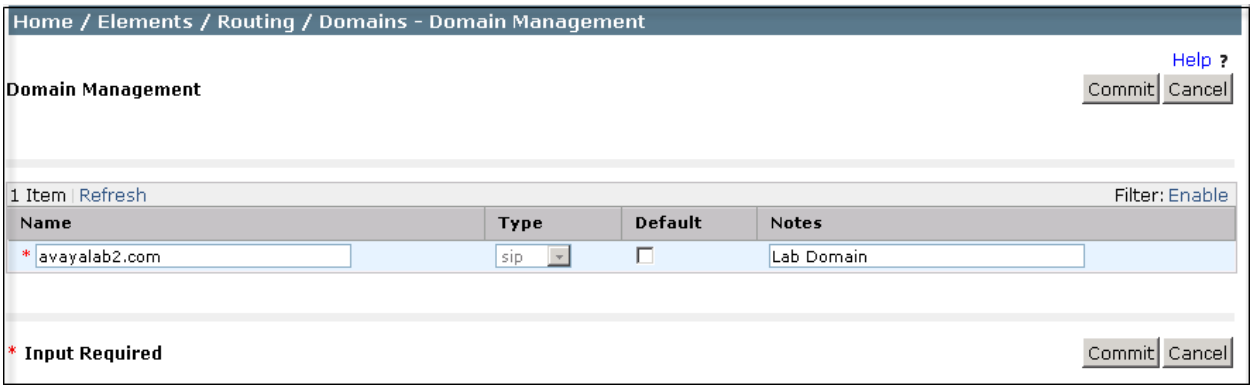


6.2. SIP Domains

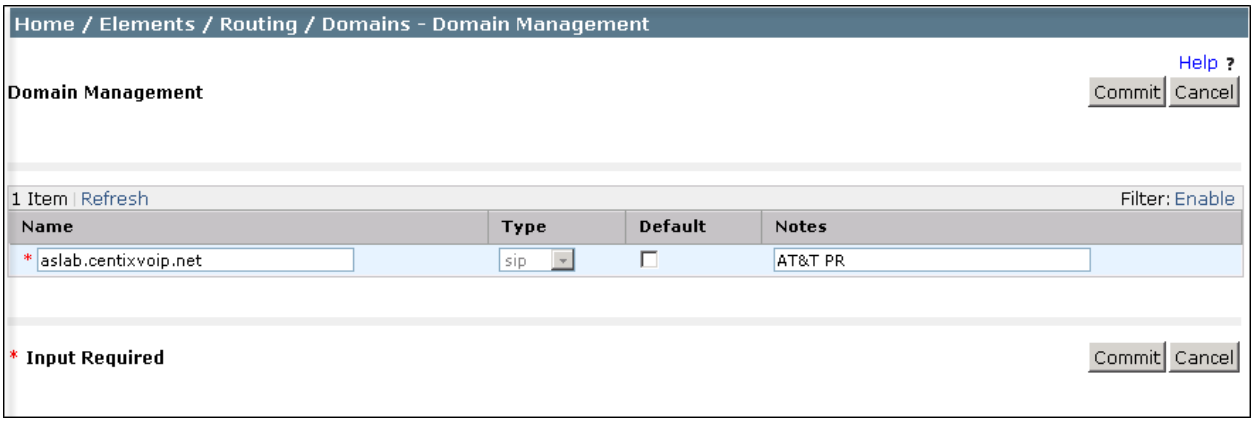
Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain, **avayalab2.com**, and the AT&T domain, **aslab.centixvoip.net**. The enterprise SIP domain was previously created during the Midsize Enterprise template installation, and this entry was already populated. To add the service provider domain, 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

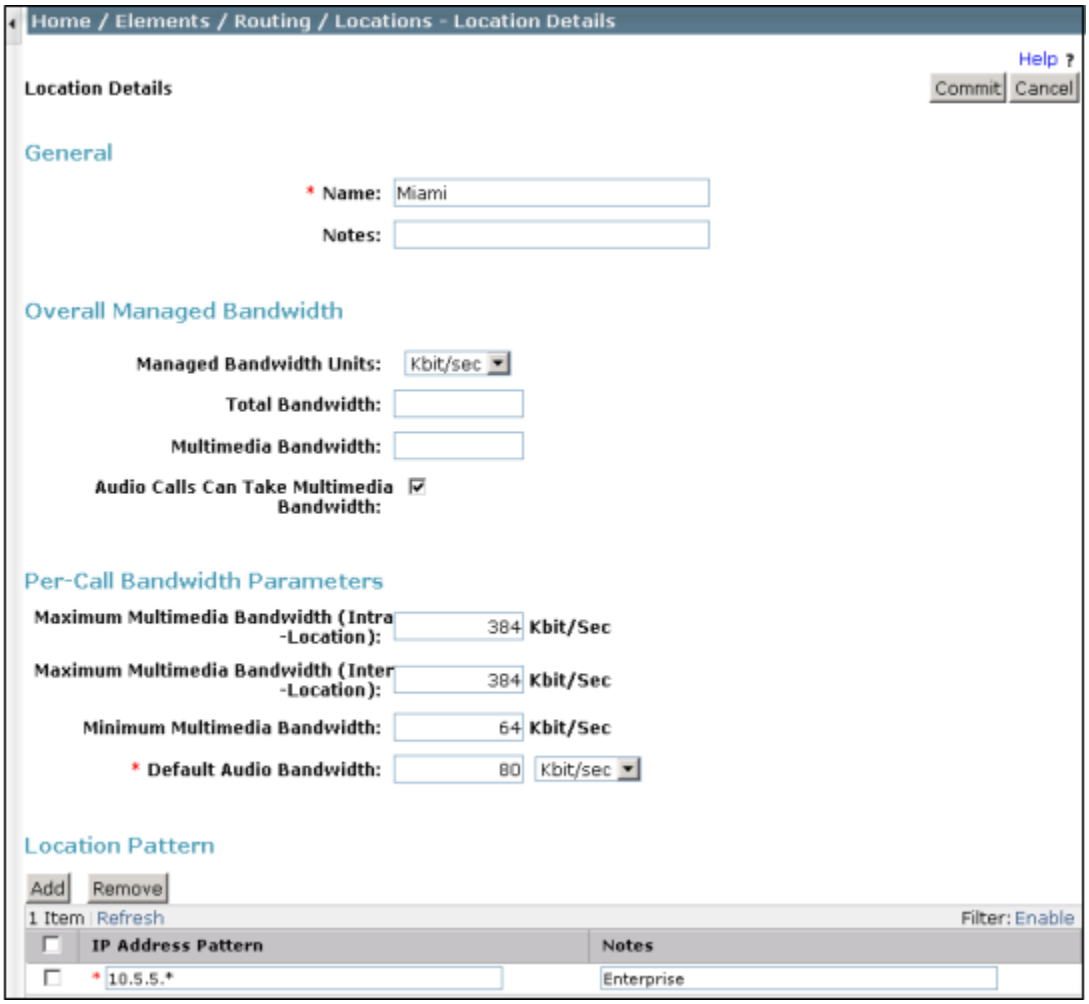
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).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

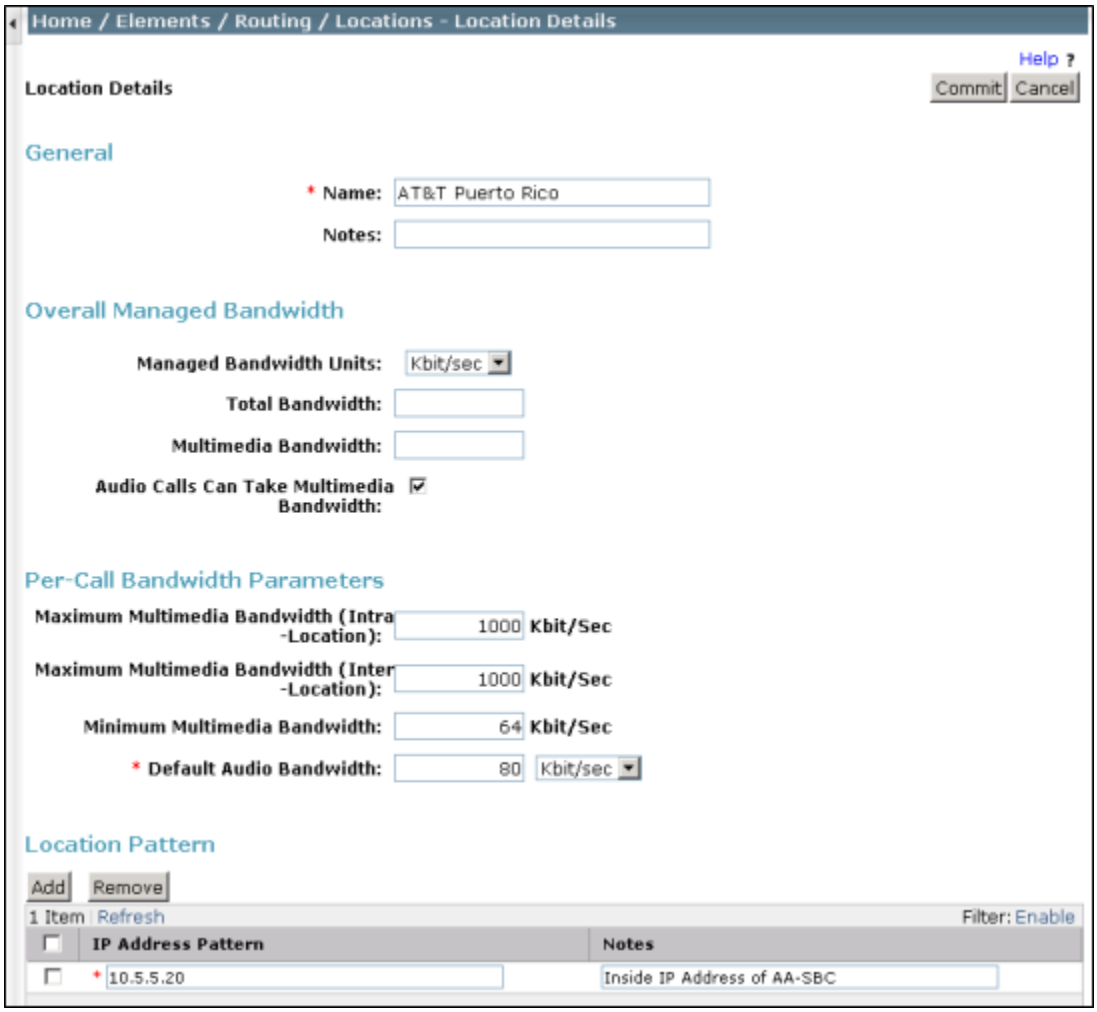
- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

The screen below shows the location **Miami**, created during the template installation. This location includes all equipment on the Enterprise subnet, 10.5.5.0. Click **Commit** to save any changes made, if any.



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 Puerto Rico*** Location, which specifies the inside IP address for the AA-SBC. Click Commit to save.



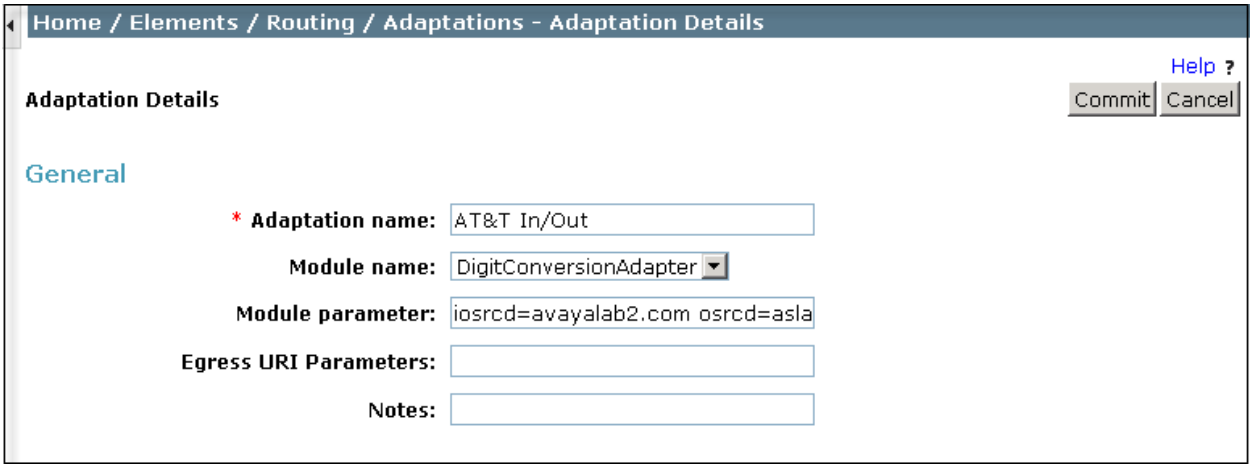
6.4. Adaptations

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

For the compliance test, the adaptation "AT&T In/Out" was created. It will be assigned to the SIP Entity for the Avaya Aura® SBC, later in this document. This adaptation uses the **DigitConversionAdapter** generic module and specifies the following two parameters:

- "**iosrcd=avayalab2.com"**. This parameter replaces the domain of the PAI header on inbound requests with the value of the enterprise domain, "avayalab2.com". This parameter must match the value used for the **Far-end Domain** setting on the Communication Manager signaling group form in **Section 5.6**.
- "**osrcd=aslab.centixvoip.net**". This parameter enables the outbound source domain to be overwritten with "aslab.centixvoip.net". For outbound PSTN calls from the enterprise to AT&T, the domain portion of the PAI header of outgoing requests will now contain "aslab.centixvoip.net", as expected by AT&T.

The screen below shows the adaptation "AT&T In/Out" created for the compliance test. All other fields were left with their default values.

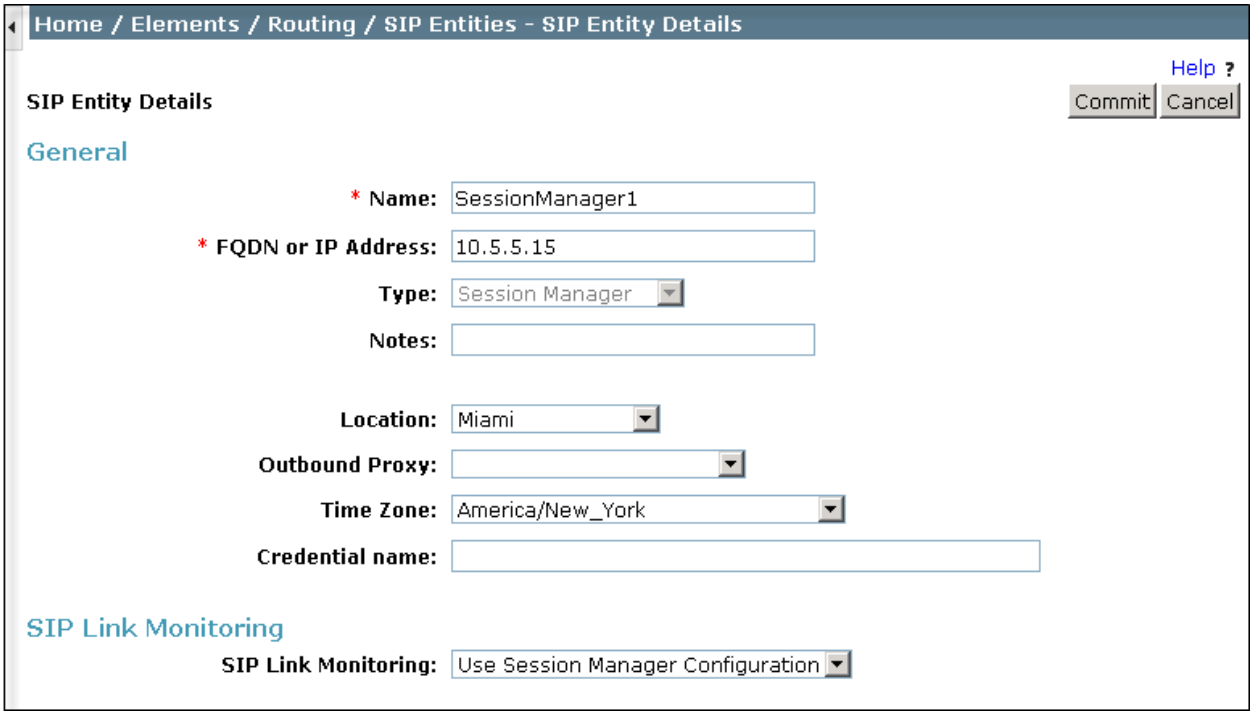


6.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the SBC. 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, **Other** for the SBC.
- **Adaptation:** This field is only present if **Type** is not set to ***Session Manager*** If applicable, select the **Adaptation** name created in **Section 6.4** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

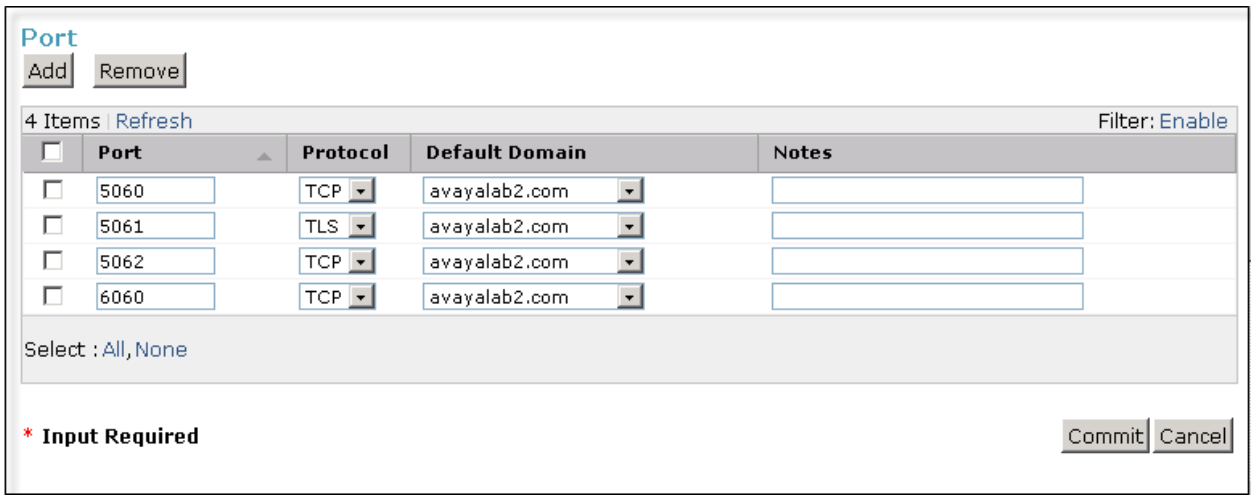
The following screen shows the Session Manager SIP Entity, created during the template installation. The **FQDN or IP Address** is the address of the Session Manager signaling interface (virtual SM-100).



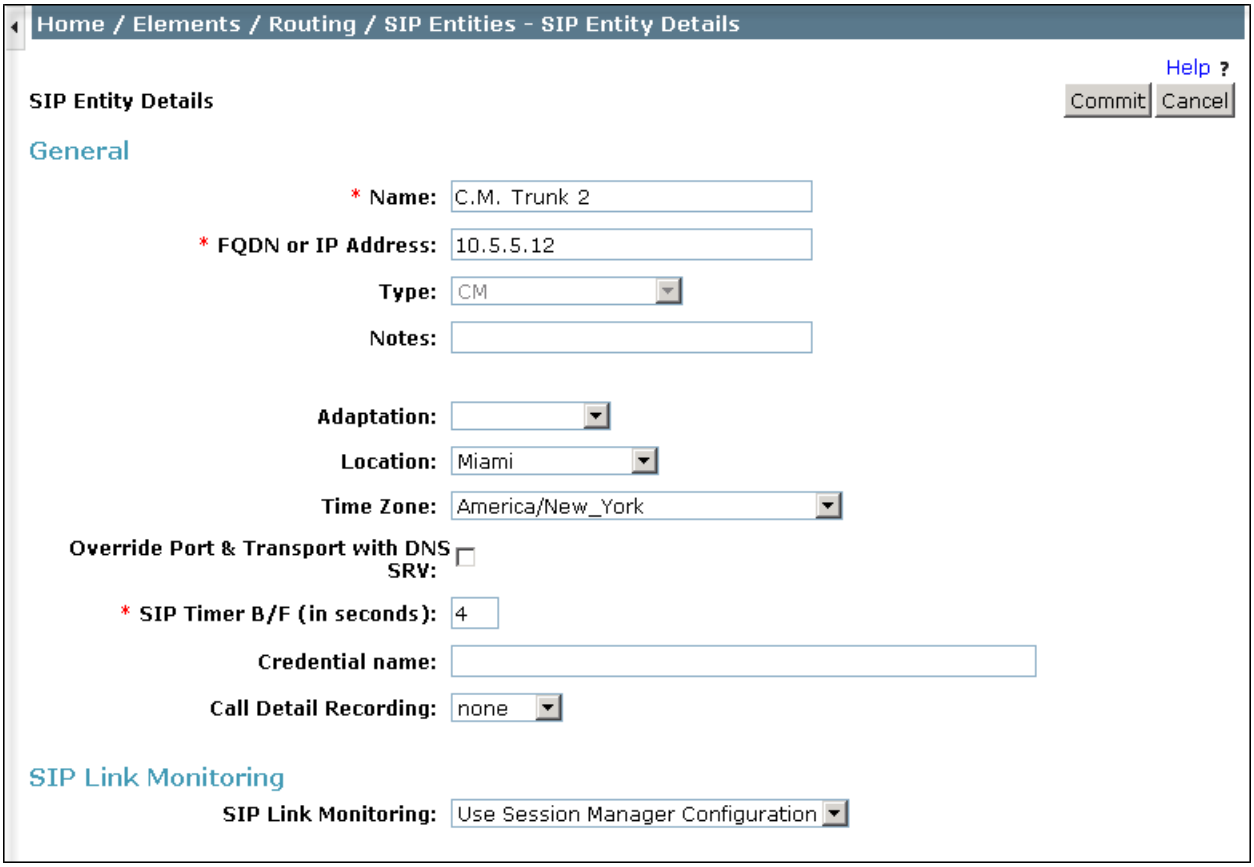
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **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.

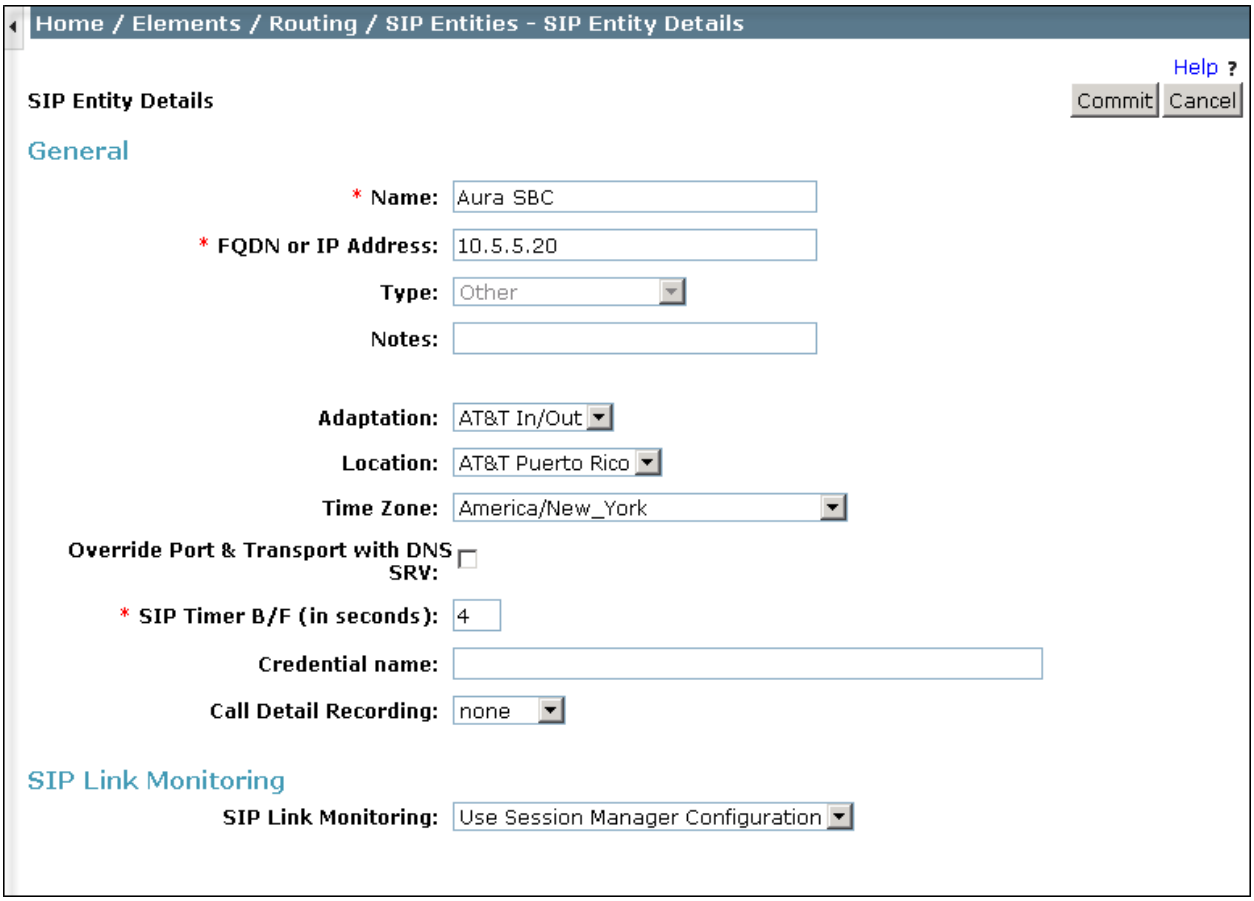
Defaults can be used for the remaining fields. Click **Commit** to save.



The following screen shows the addition of the SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different to the one created during the Template installation for use with all other enterprise SIP traffic. 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 Aura® SBC Entity. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). The location is set to the one defined for SBC in **Section 6.3.** For **Adaptation** field, select the adaptation module "**AT&T In/Out**" previously defined in **Section 6.4**.



6.6. Entity Links

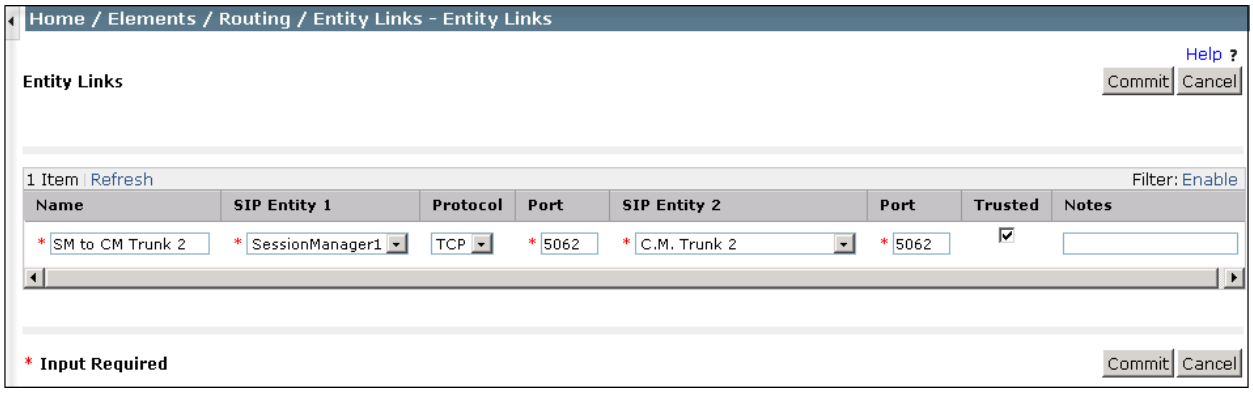
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation 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.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in* ***Section 6.5*** *will be denied.*

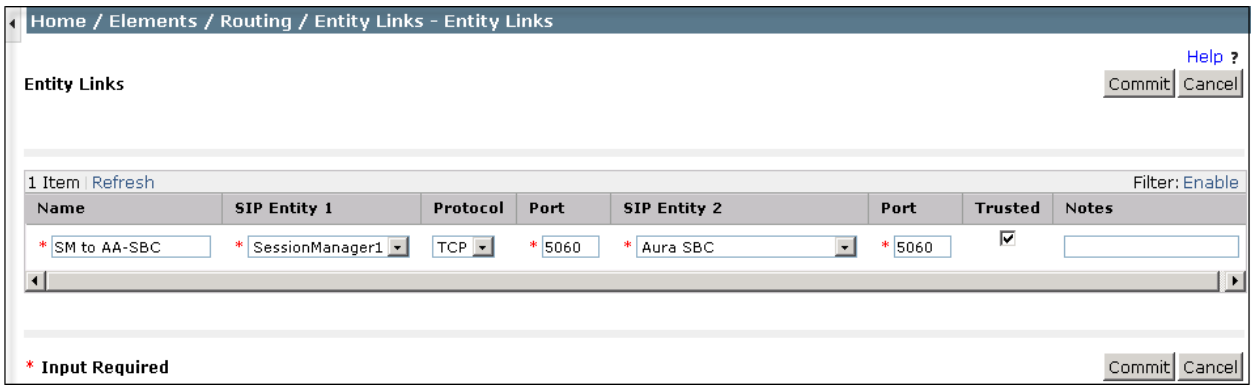
Click **Commit** to save.

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**.

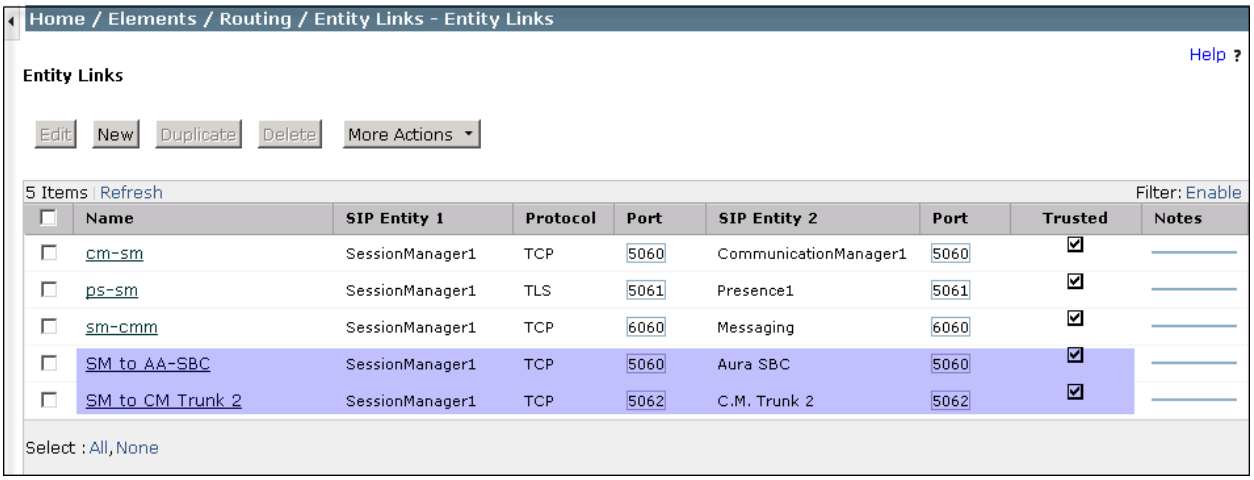
Entity Link to Communication Manager



Entity Link to the SBC:



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. Other links appearing on this screen were automatically created at the time of the Midsize Enterprise template installation.



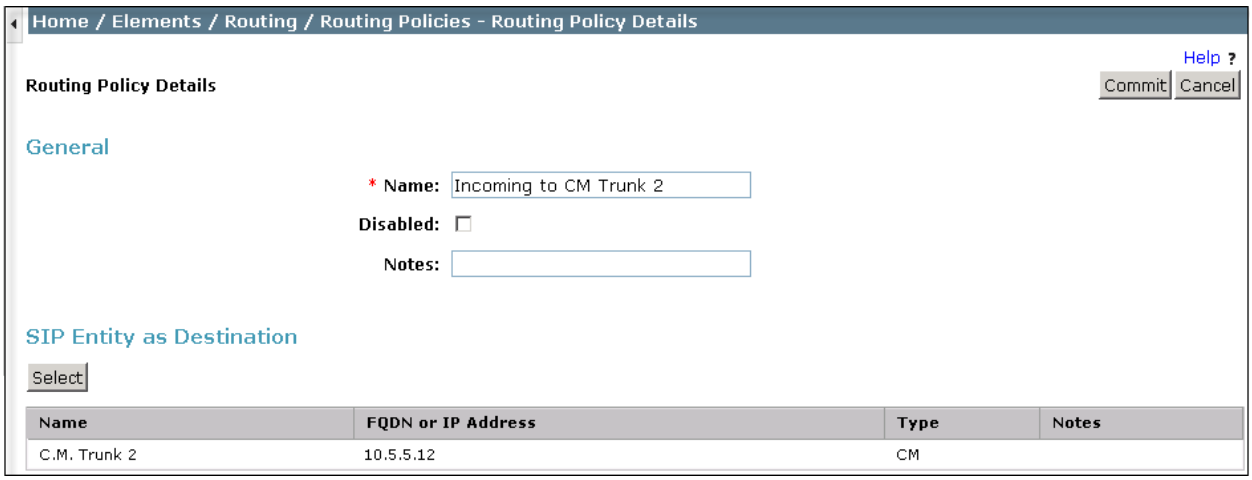
6.7. Routing Policies

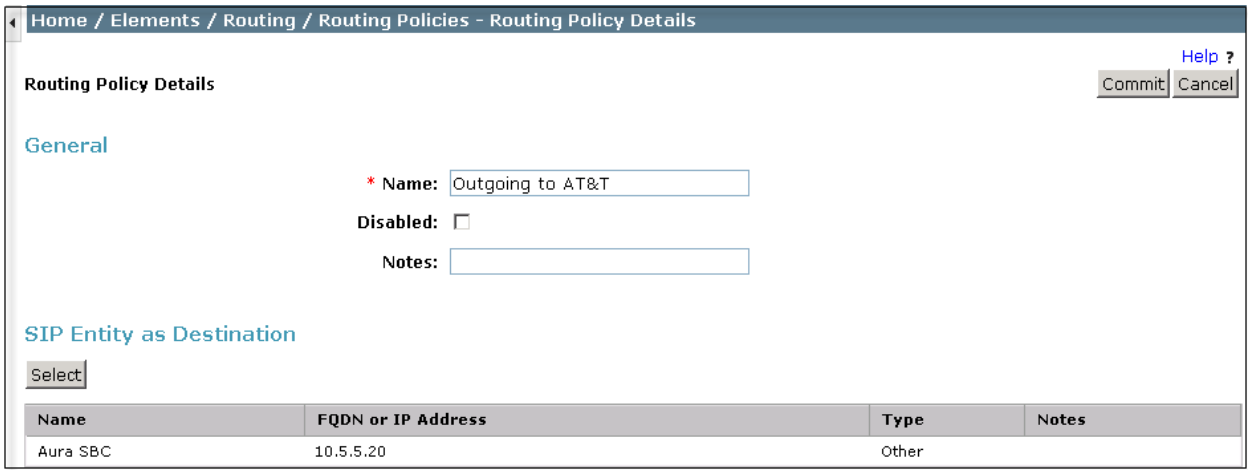
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation 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 SBC.





6.8. 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:

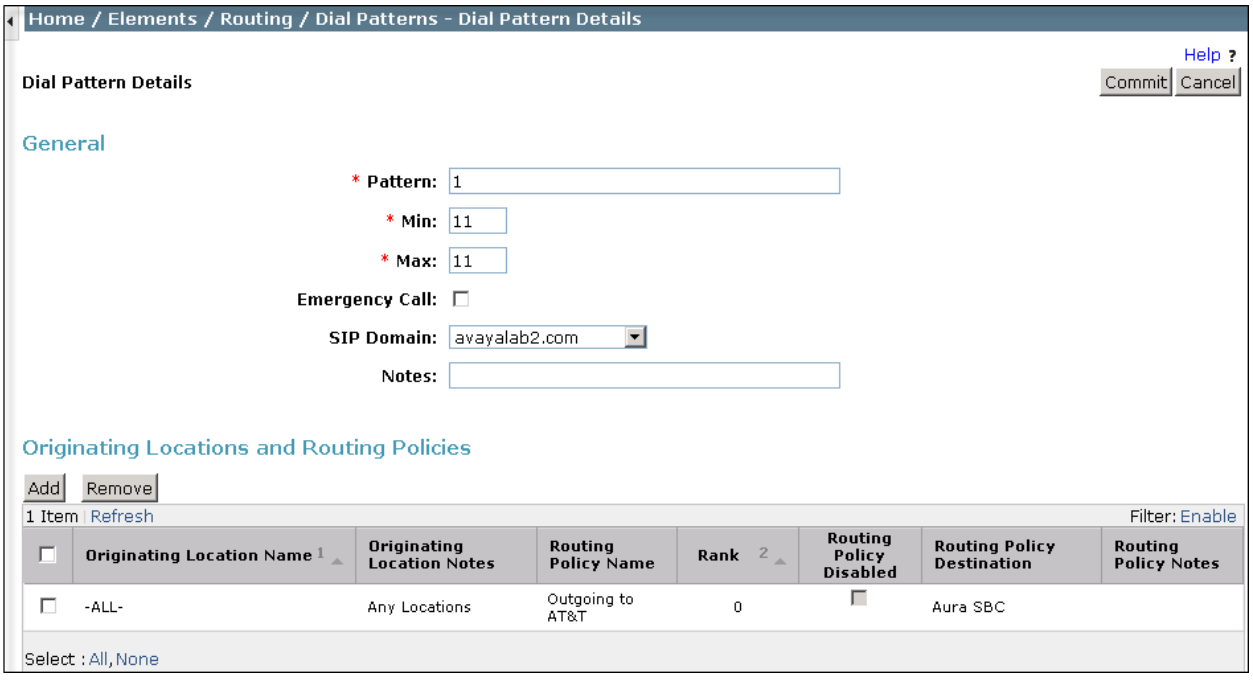
In the **General** section, enter the following values:

- **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).

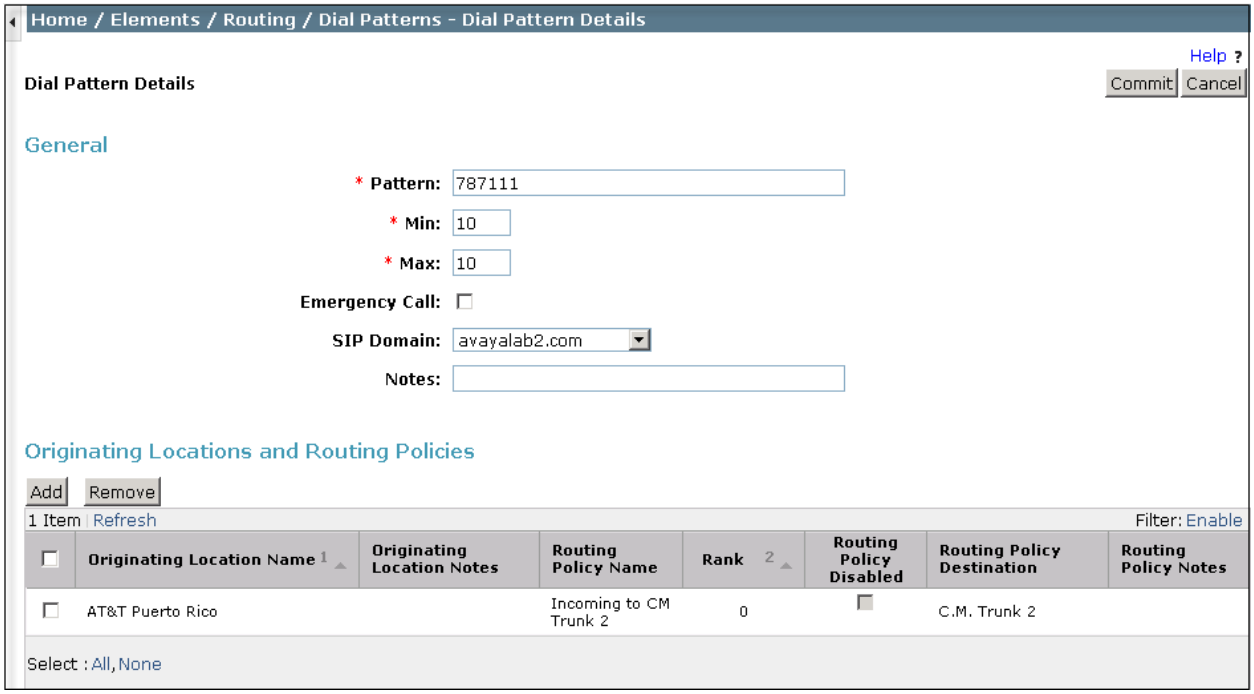
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used 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 "**Outgoing to AT&T**".



The second example shows that a 10 digit number starting with **787111**, to domain **avayalab2.com** and originating from the **AT&T Puerto Rico** location, will use route policy **Incoming to CM Trunk 2**. This number falls in the DID range assigned to the enterprise by AT&T. **AT&T Puerto Rico** is selected for the **Originating Location** because these calls come from the SBC, which resides in that location.



7. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® SBC. This configuration is done in two parts:

- The first part is done during the Avaya Aura® Solution for Midsize Enterprise template software installation via the installation wizard, which is invoked during the loading of the template.
- The second part of the configuration is done after the installation is complete using the SBC web interface.

The resulting SBC configuration file is shown in **Appendix A**.

7.1. Installation Wizard

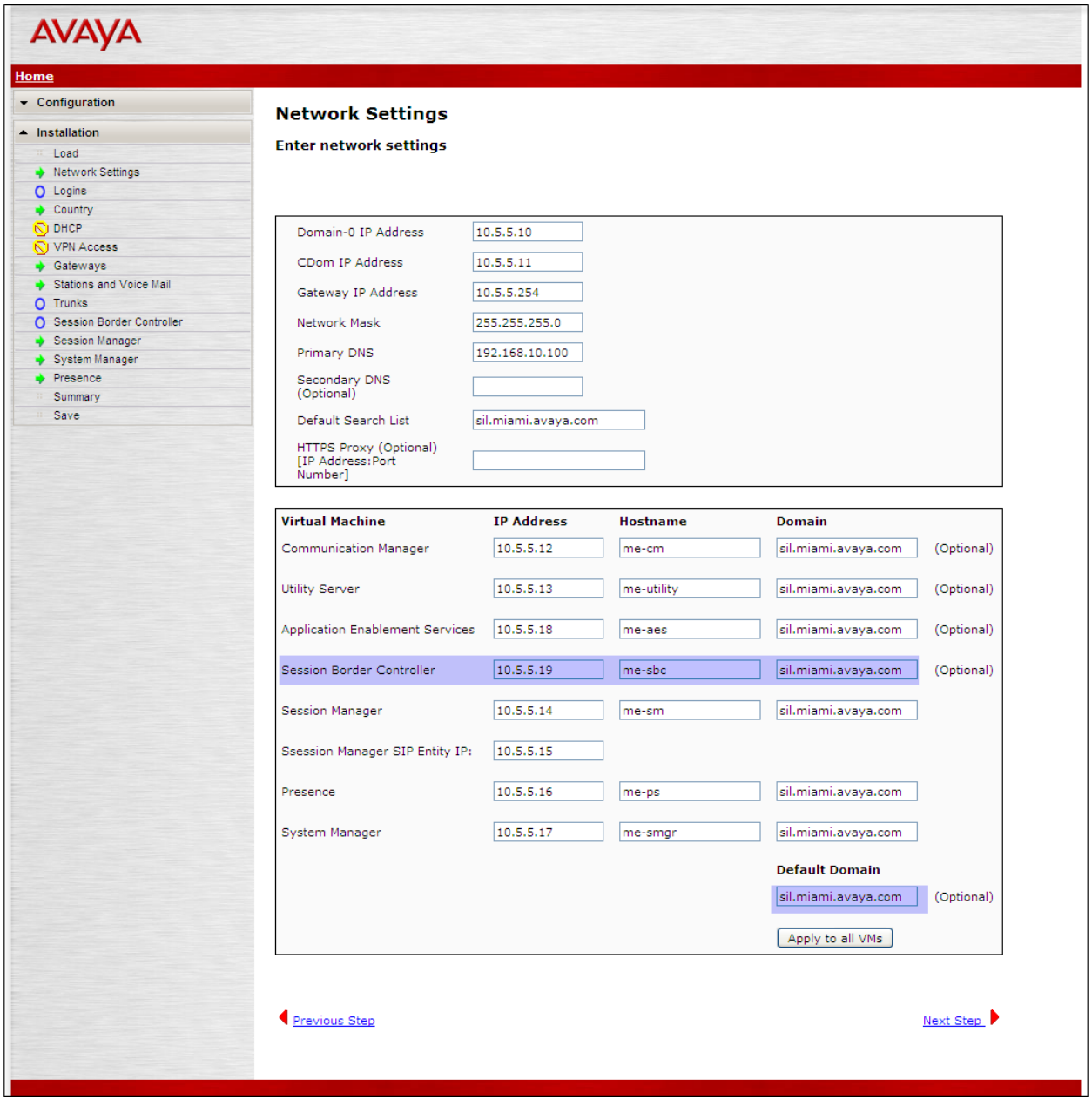
During the installation of the Midsize Enterprise template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the SBC.

These Application Notes will not cover the use of the installation wizard in its entirety, but will include screens that are presented as part of the wizard related to the SBC configuration. For a complete reference in the use of the Midsize Enterprise installation wizard, see [1].

7.1.1. Network Settings

The first screen of the installation wizard is the **Network Settings** screen. Here is where IP Addresses, Hostnames and Domains are assigned to all Virtual Machines. For the Session Border Controller, fill in the fields as described below:

- **IP Address**: Enter the IP address of the SBC management interface (Eth0).
- **Hostname**: Enter a host name for the SBC.
- **Domain**: Enter the enterprise network domain. Note that this could be different, like in the test scenario, than the enterprise SIP domain.



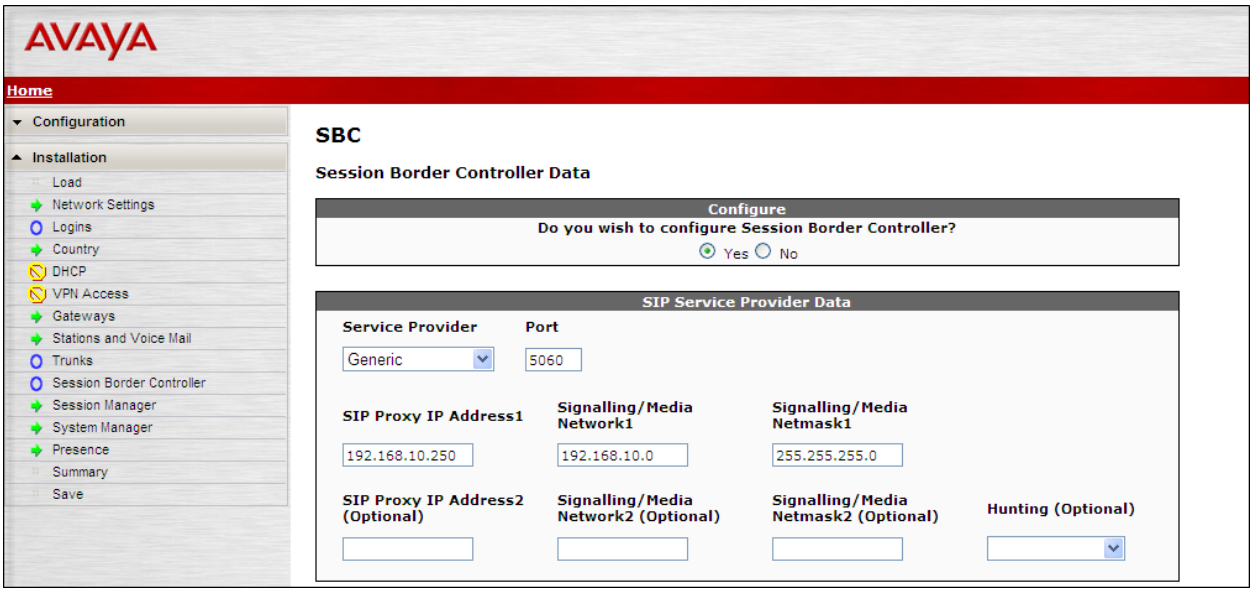
7.1.2. Session Border Controller Data

On the **SBC/Session Border Controller Data** screen, fill in the fields as described below and shown in the following screen:

In the **Configure** section check **Yes** for **Do you wish to configure Session Border Controller?**

In the **SIP Service Provider Data** section:

- **Service Provider**: From the pull-down menu, select the name of the service provider to which the SBC will connect. This will allow the wizard to select a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for AT&T Mobility in Puerto Rico. Thus, **Generic** was chosen instead and further customization was done manually after the wizard was complete.
- **Port**: Enter the port number that the service provider uses to listen for SIP traffic.
- **SIP Proxy IP Address1**: Enter the AT&T provided IP address of the service provider SIP Proxy. If the service provider has multiple proxies, enter the primary proxy on this screen and additional proxies can be added after installation.
- **Signaling/Media Network1:** Enter the AT&T provided subnet where signaling/media traffic will originate. If signaling/media traffic can originate from multiple networks, enter one network address on this screen and additional networks can be added after installation.
- **Signaling/Media: Netmask1:** Enter the netmask corresponding to **Signaling/Media Network1**.

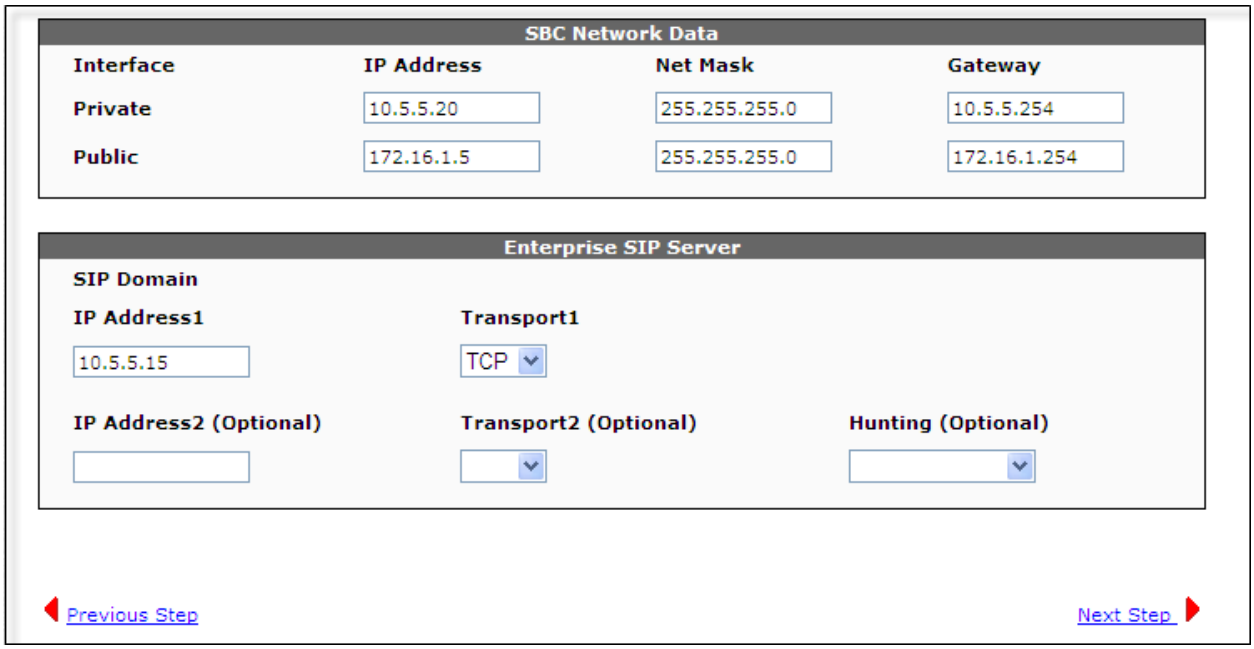


In the **SBC Network Data** section:

- **Private IP Address**: Enter the IP address of the private side of the SBC (Eth5).
- **Private Net Mask**: Enter the netmask associated with the private network to which the SBC connects.
- **Private Gateway**: Enter the default gateway of the private network.
- **Public IP Address**: Enter the IP address of the public side of the SBC (Eth4).
- **Public Net Mask**: Enter the netmask associated with the public network to which the SBC connects.
- **Public Gateway**: Enter the default gateway of the public network.

In the **Enterprise SIP Server** section:

- **IP Address1**: Enter the IP address of the Enterprise SIP Server to which the SBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface.
- **Transport1**: From the pull-down menu, select the transport protocol to be used for SIP traffic between the SBC and Session Manager.



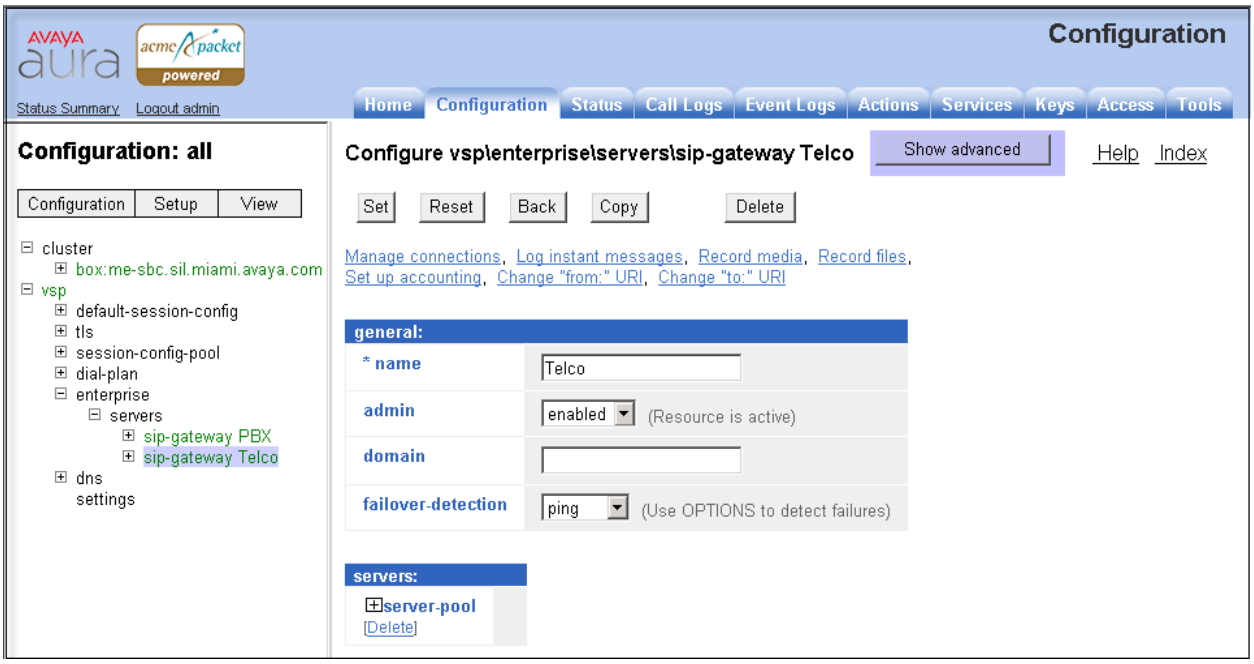
Note: Physical interface Eth5 of the Midsize Enterprise server maps to logical interface Eth1 of the SBC. Similarly, physical interface Eth4 of the server maps to logical interface Eth2 of the SBC.

7.2. Post Installation Configuration

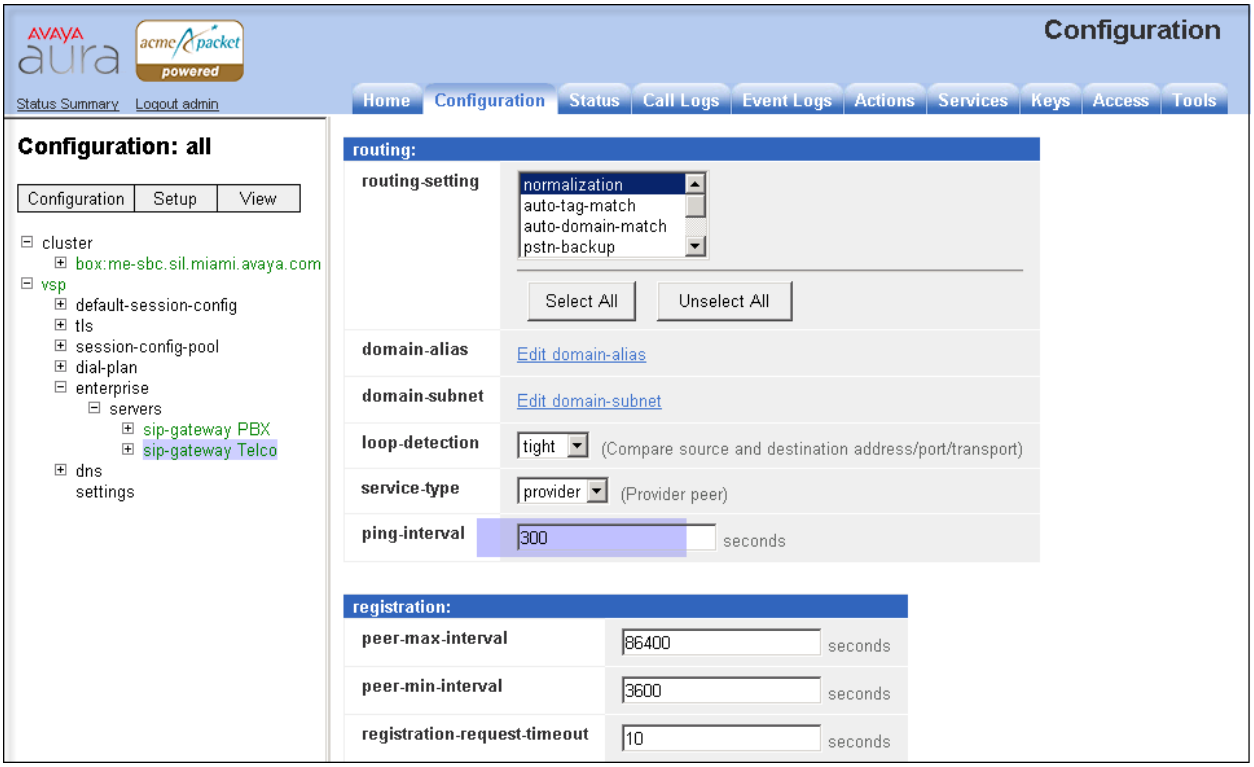
The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 7.1.2**. Since a **Generic** provider was selected in the installation wizard, additional manual changes must also be performed. These changes are performed by accessing the browser-based GUI of the Session Border Controller, using the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured in **Section 7.1.1**. Log in with the proper credentials.

7.2.1. Options Frequency

To set the frequency of the OPTIONS messages sent from the SBC to the service provider, first navigate to **vsp → enterprise → servers → sig-gateway Telco**. Click **Show Advanced.**

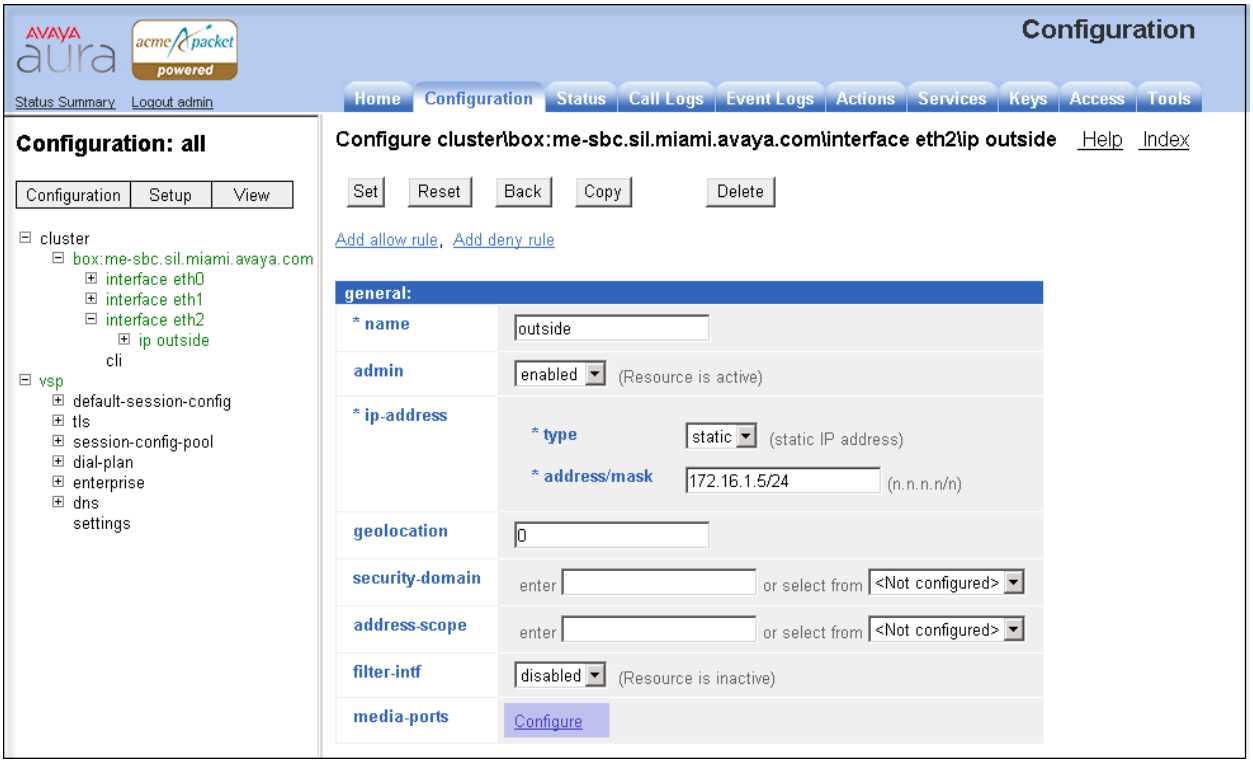


Scroll down to the **Routing** section of the form. Enter the desired interval in the **ping-interval** field. For the compliance test, 300 seconds was used. Click **Set** at the top of the form (shown in previous screen).

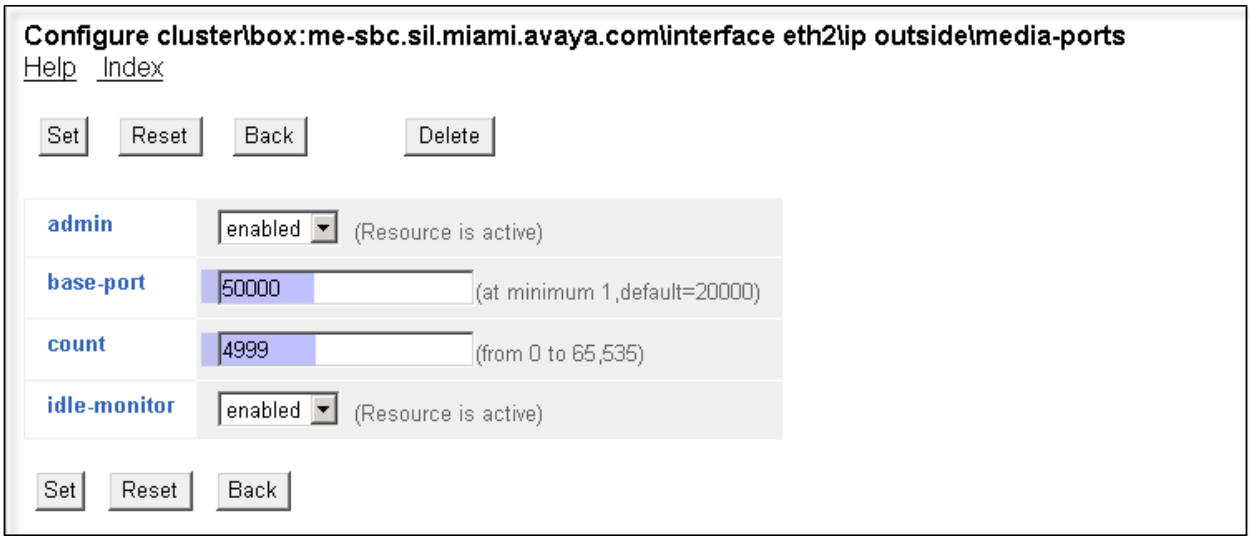


7.2.2. Media Ports

To adjust the port range assigned to media streams leaving the outside interface of the SBC, to match the range specified by AT&T for the compliance test of 50000 to 54999, navigate to **cluster → box → interface eth2 → ip outside**. On the right pane, navigate to **media-ports** and click **Configure**.

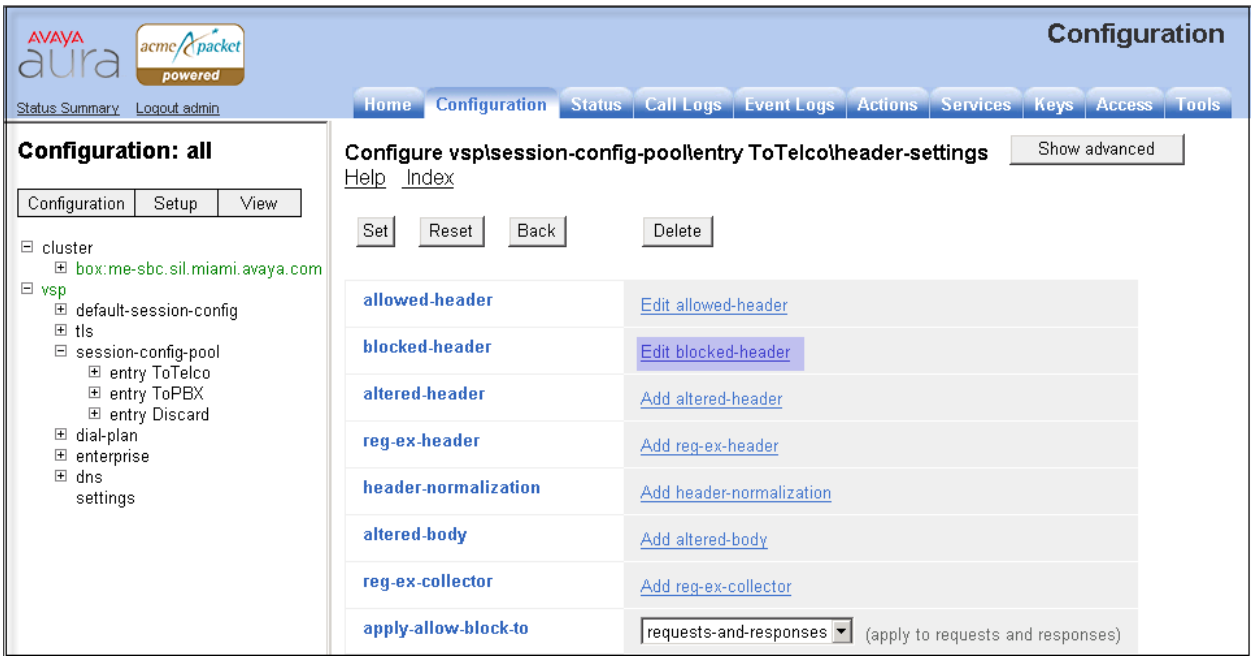


On the next screen, set the value for **base-port** to **50000**, and the **count** to **4999.** Click **Set** to complete the configuration.

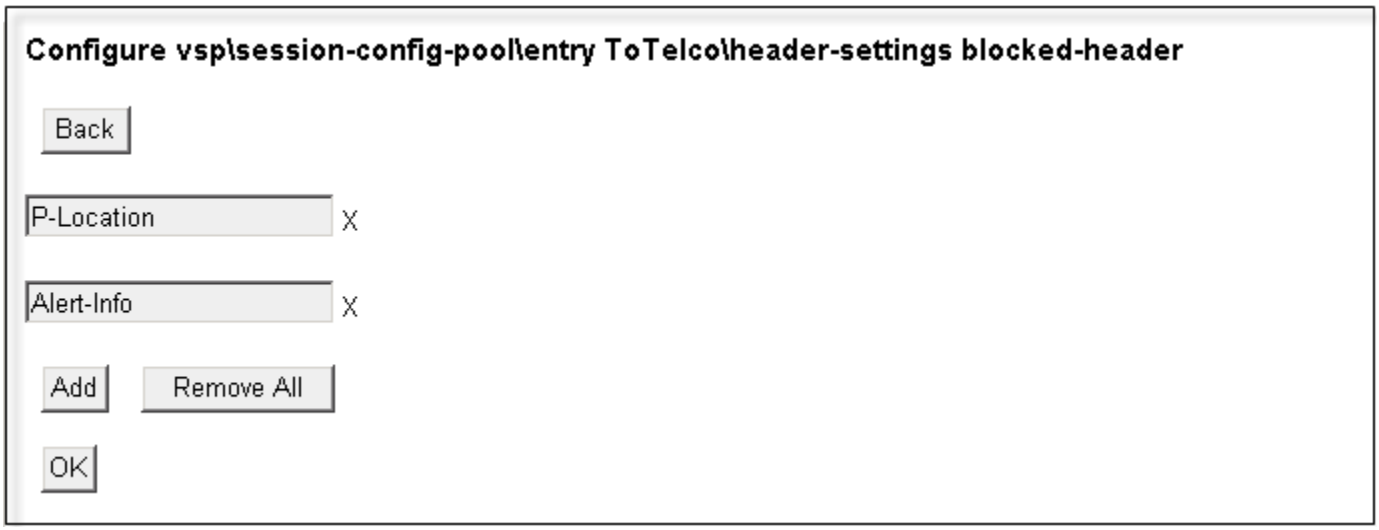


7.2.3. Blocked Headers

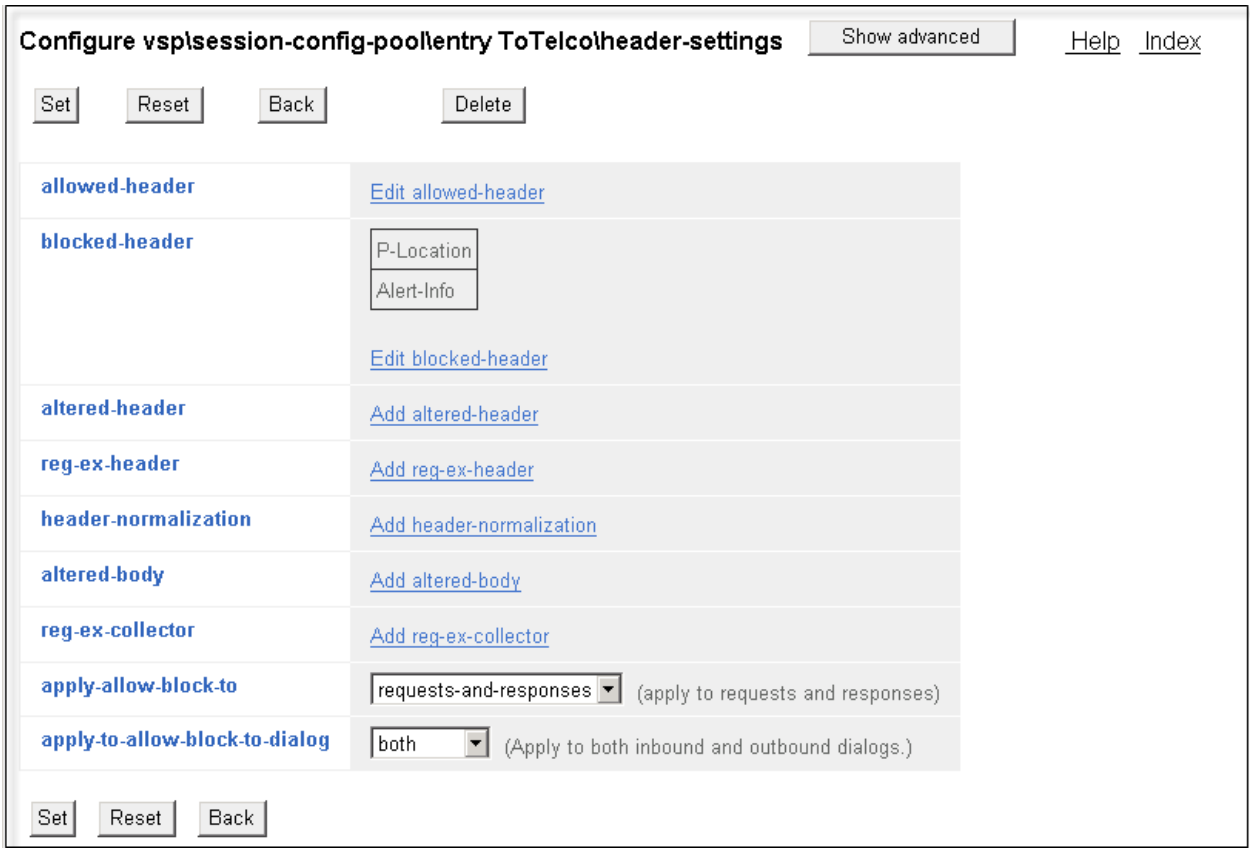
The P-Location and Alert-Info headers are sent in SIP messages from the Session Manager to the AT&T network. These headers contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries. These headers were simply removed (blocked) from both requests and responses for outbound calls. To create a rule for blocking a header on an outbound call, first navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. Click **Edit blocked-header**



In the right pane that appears, click **Add.** In the blank fields, enter the name of the header to be blocked. After all the blocked headers are added, click **OK**. The screen below shows the **P-Location** and the **Alert-Info** headers configured to be blocked for the compliance test.



The list of blocked headers for outbound calls will appear in the right pane as shown below. Click **Set** to complete the configuration.

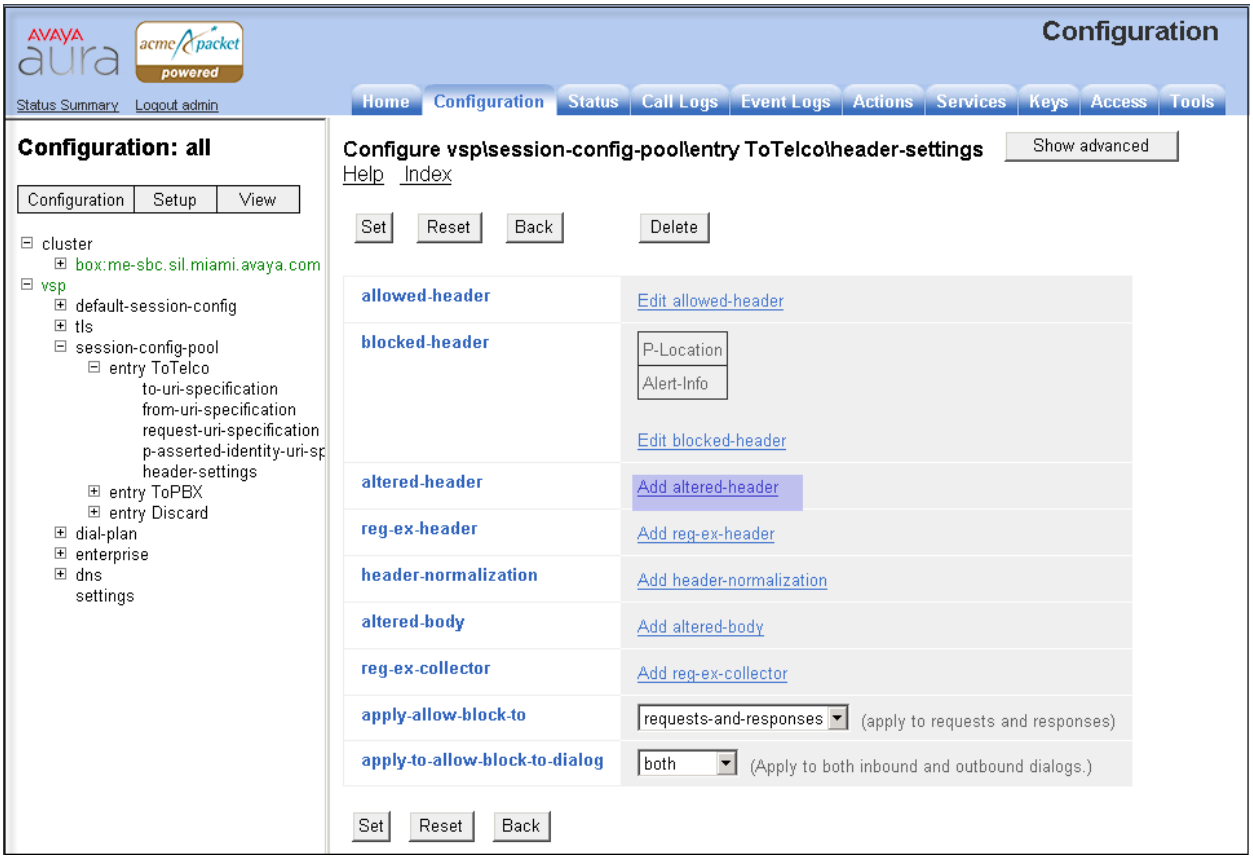


7.2.4. Diversion Header Domain

Avaya Aura® Session Manager can adapt the domain in various SIP headers such as the Request- URI, History-Info and P-Asserted-Identity. As described in these Application Notes, Session Manager was used to adapt the domain in the PAI headers of both incoming and outbound requests, allowing the interoperability between the enterprise domain "avayalab2.com" and the service provider's "aslab.centixvoip.net".

In the sample configuration, the domain portion of the Diversion header was not altered by the Session Manager adaptations. To allow diverted calls to be processed properly, the SBC was used to convert the domain in the Diversion header from the enterprise domain to the AT&T expected "aslab.centixvoip.net".

Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. The screen below shows the configuration before making changes for the Diversion header. Click **Add altered-header**.

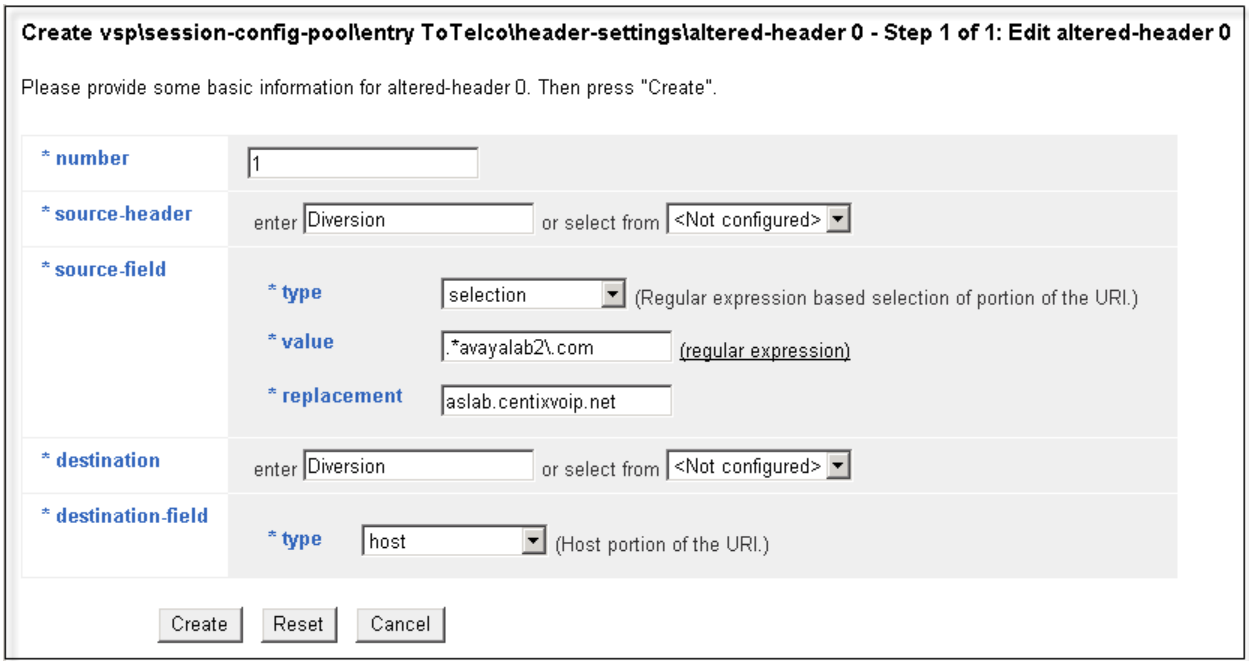


In the **number** field, enter an appropriate unused number. Since this is the first altered-header rule, number 1 was used. For the **source-header** field, enter "**Diversion**".

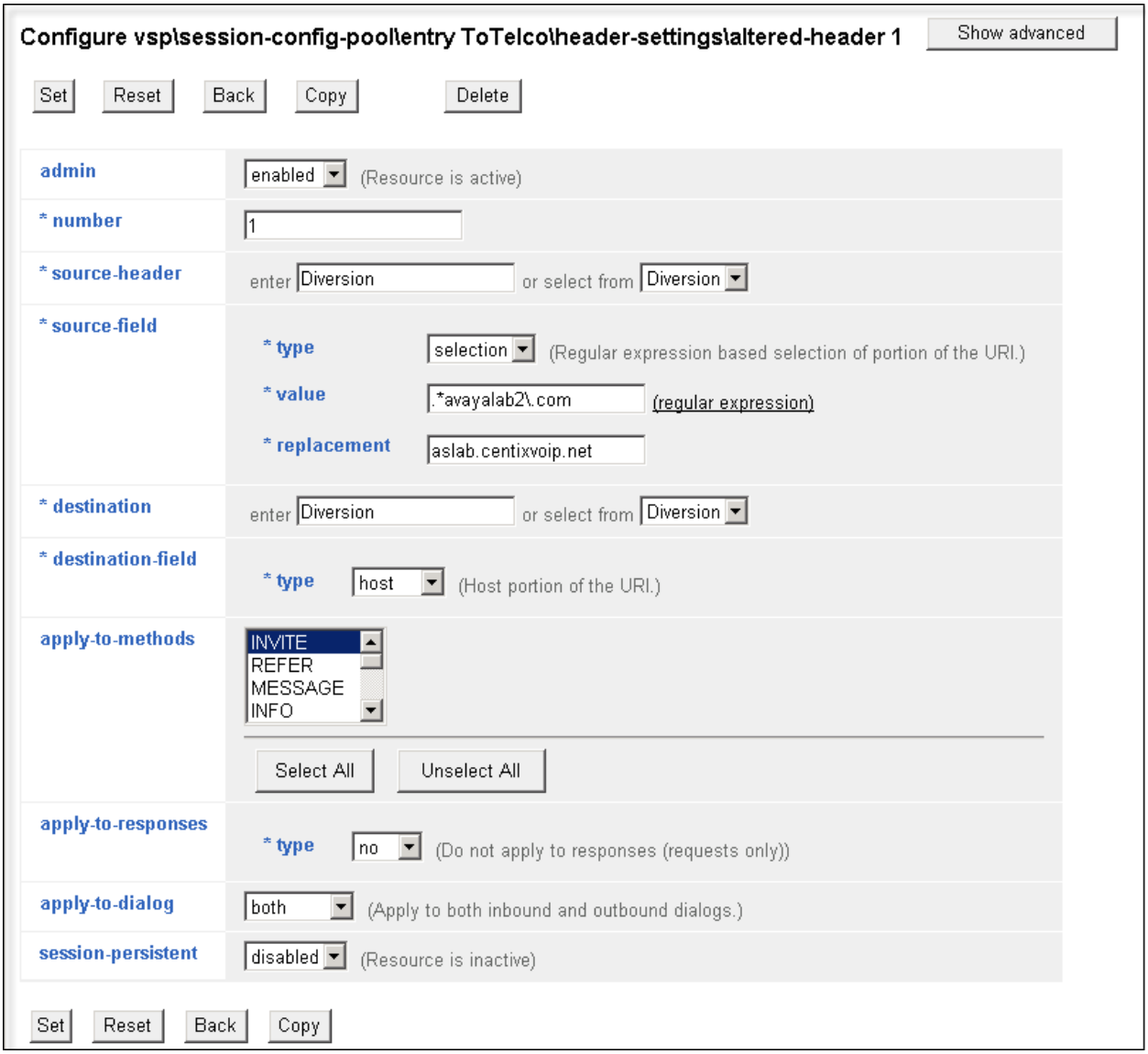
In the source-field area, enter the following:

- **type**: Choose "**selection**" from the drop-down menu
- **value**: Either enter a value to match directly, or click the **regular expression** link for assistance in creating the proper **value**. In the sample configuration, the rule shown will match on "avayalab2.com" appearing in the Diversion header.
- **replacement**: Enter the domain to appear in the host portion of the Diversion header, in place of "avayalab2.com". For the compliance test, AT&T expected "aslab.centixvoip.net".

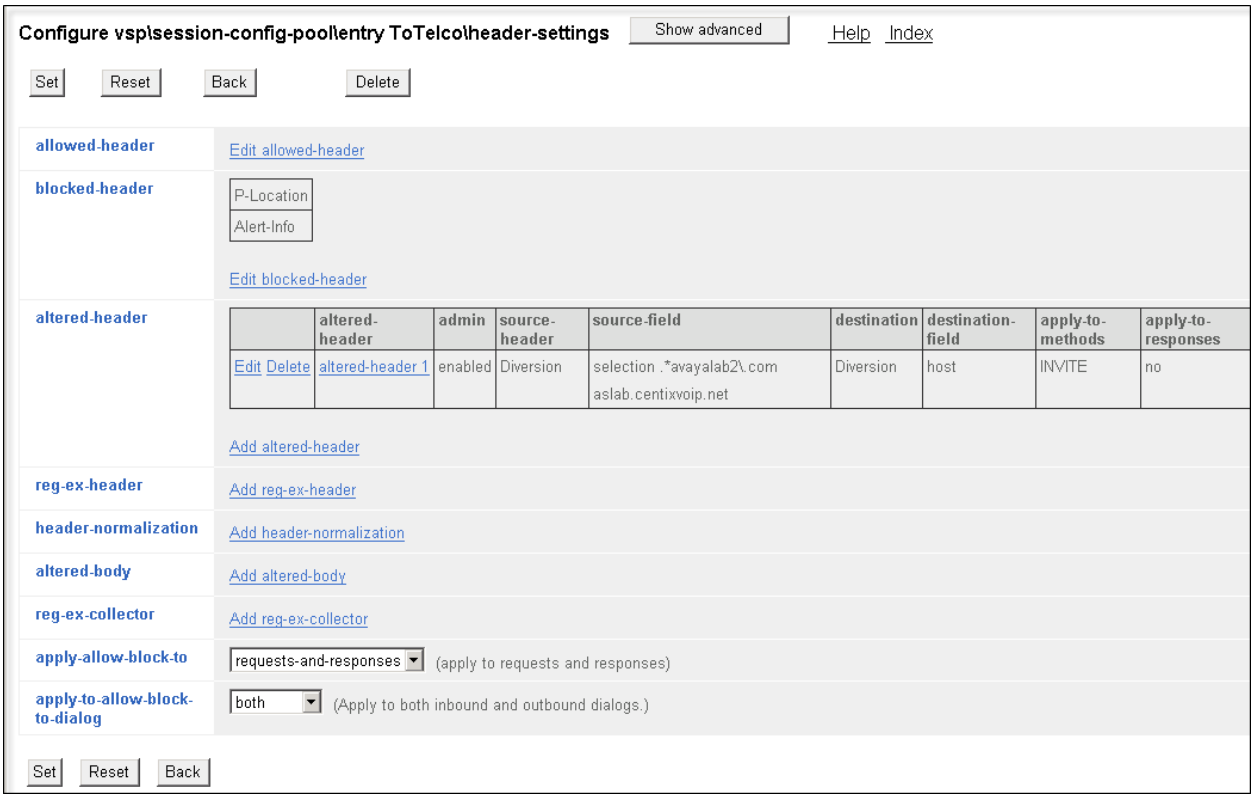
In the **destination** area, enter "**Diversion**". Select "**host**" from the **type** drop-down menu, since it is the host portion of the Diversion header that the rule should replace. Click the **Create** button.



Additional configuration can be applied to the altered-header rule using the screen shown below. In the sample configuration, the defaults were retained. Click the **Set** button.

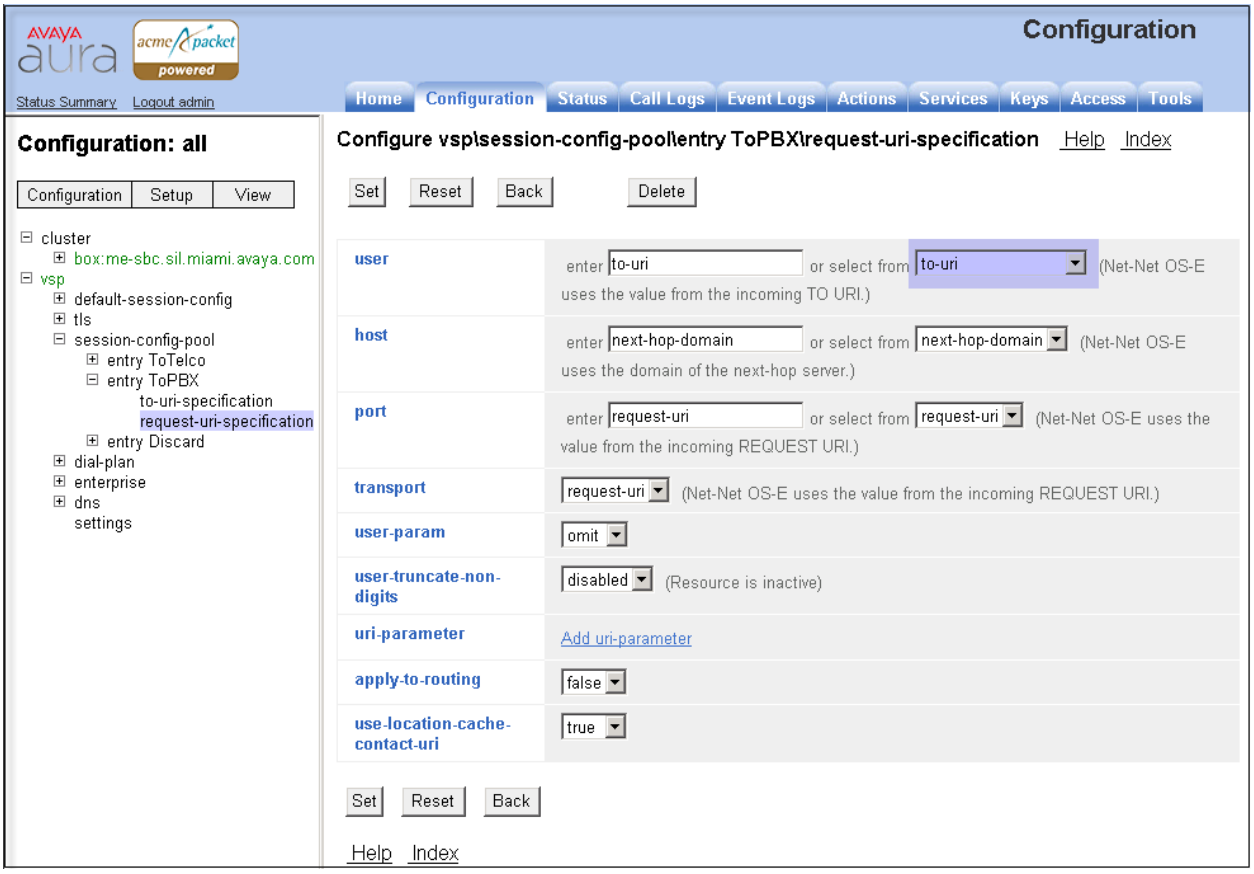


The following screen shows a summary of the altered-header rule configured in this section. It also shows the blocked-header rule configured in **Section 7.2.3**.



7.2.5. Request URI

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 INVITE, 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. Navigate to **vsp → session-config-pool → entry ToPBX.** Click on **request-uri-specification.**

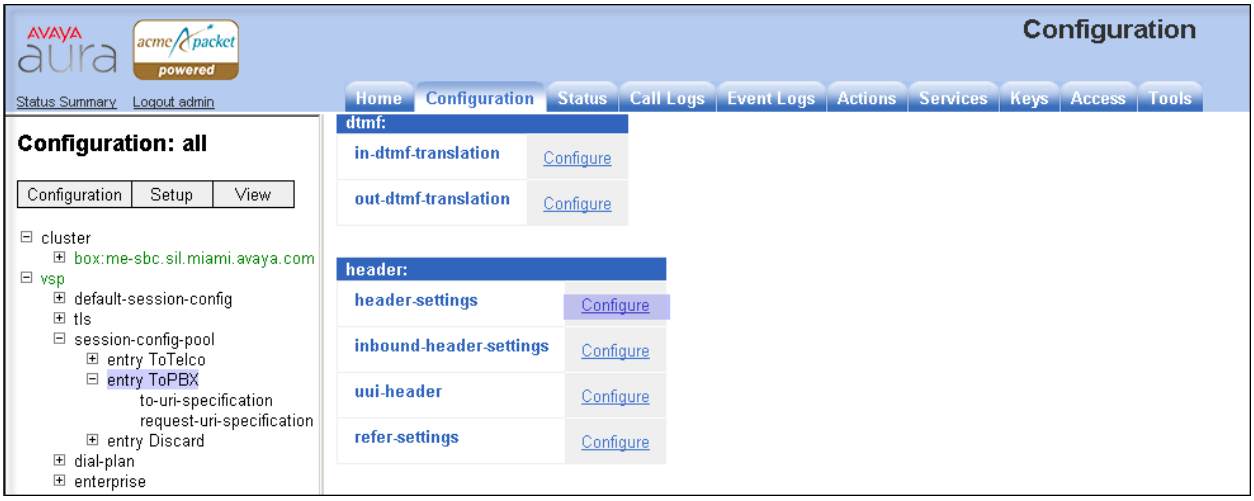


On the **user** field, select "**to-uri**" from the drop-down menu, instead of the default "**request-uri**". By making this change, the call is allowed to be routed to the correct destination by Session Manager, and ultimately by Communication Manager. Click **Set** to complete the configuration

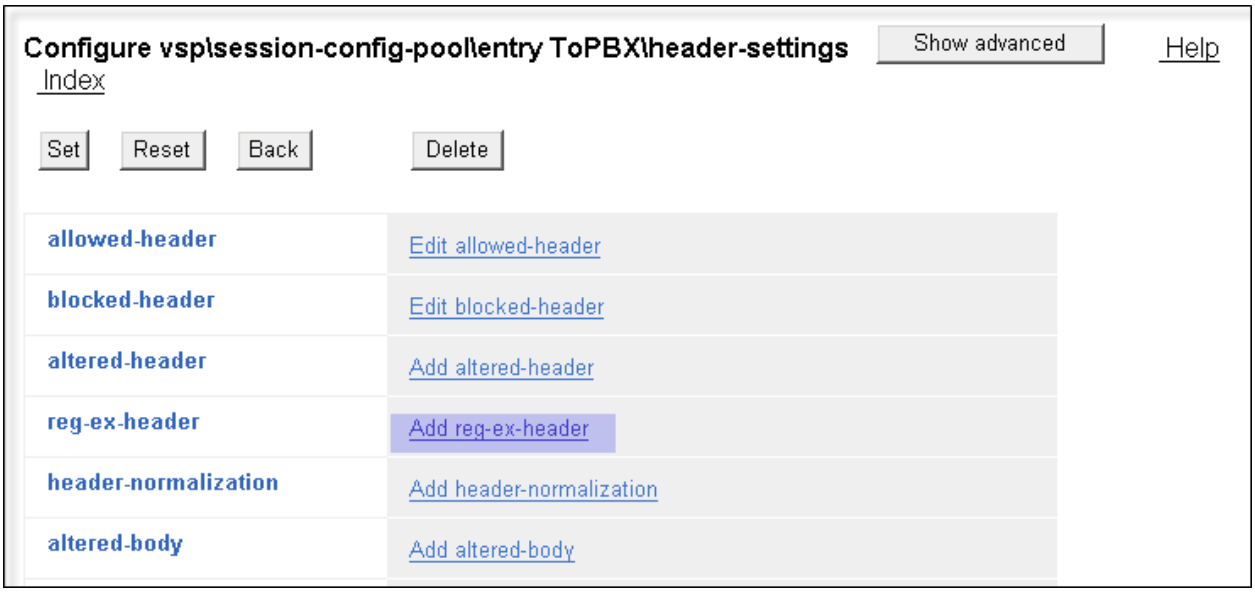
7.2.6. Refer-To Header

This section presents a sample configuration that will cause the SBC to modify the host portion of the Refer-To header in a REFER message, replacing the enterprise domain with the value expected by AT&T. It should be noted that similar results could have been achieved by using additional adaptations at a more global level in Session Manager. Since this manipulation was needed only for specific Network Call Redirection cases, it was implemented here, taking advantage of the SBC granular header modification capabilities.

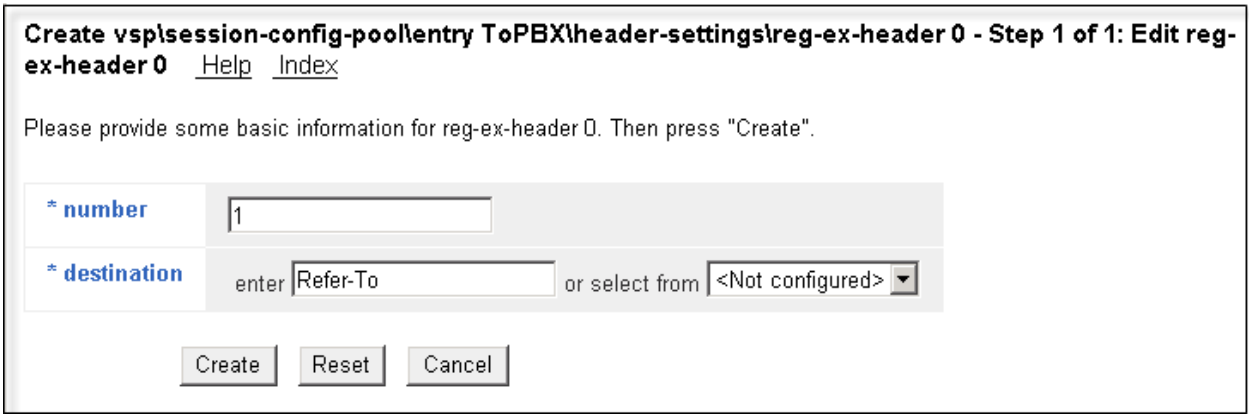
In the left side menu, navigate to **vsp → session-config-pool → entry ToPBX.** Click on **Configure** next to **header-settings**.



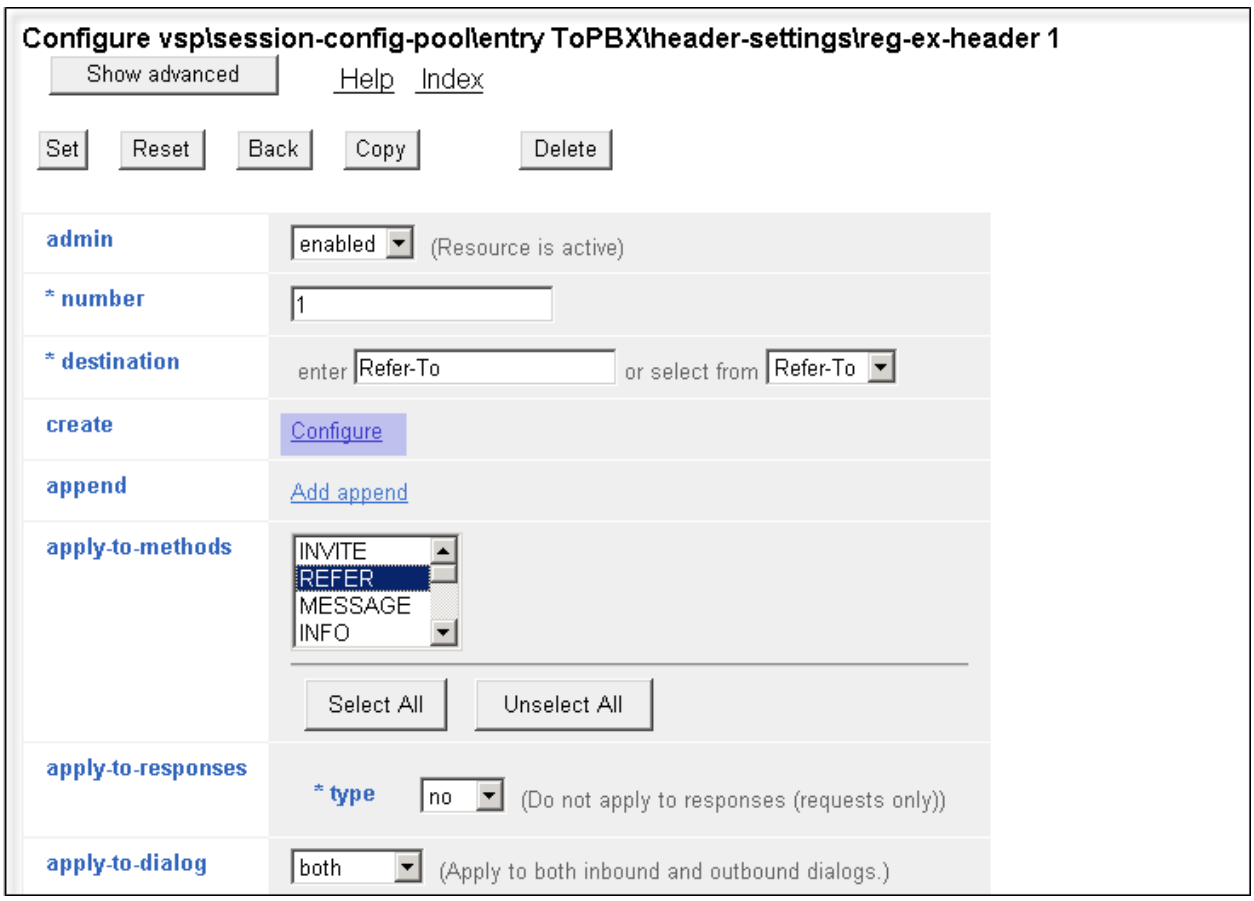
On the right panel, select **Add reg-ex-header** as shown below.



In the new right pane, in the **number** field, since this is the first reg-ex-header rule, **1** was used. Enter "**Refer-To**" in the **destination** field and click **Create.**



On the following screen that is presented, select "REFER" for **apply-to-methods.** Use defaults for all other fields. Click the **Configure** link to the right of **create**.

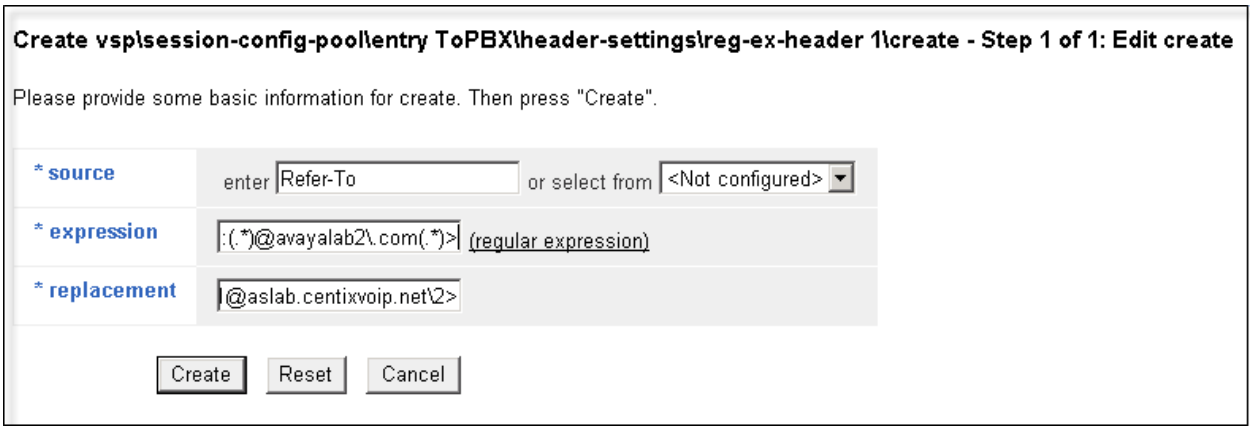


The following screen is presented. In the **source** area, type "**Refer-To**" in the **enter** field.

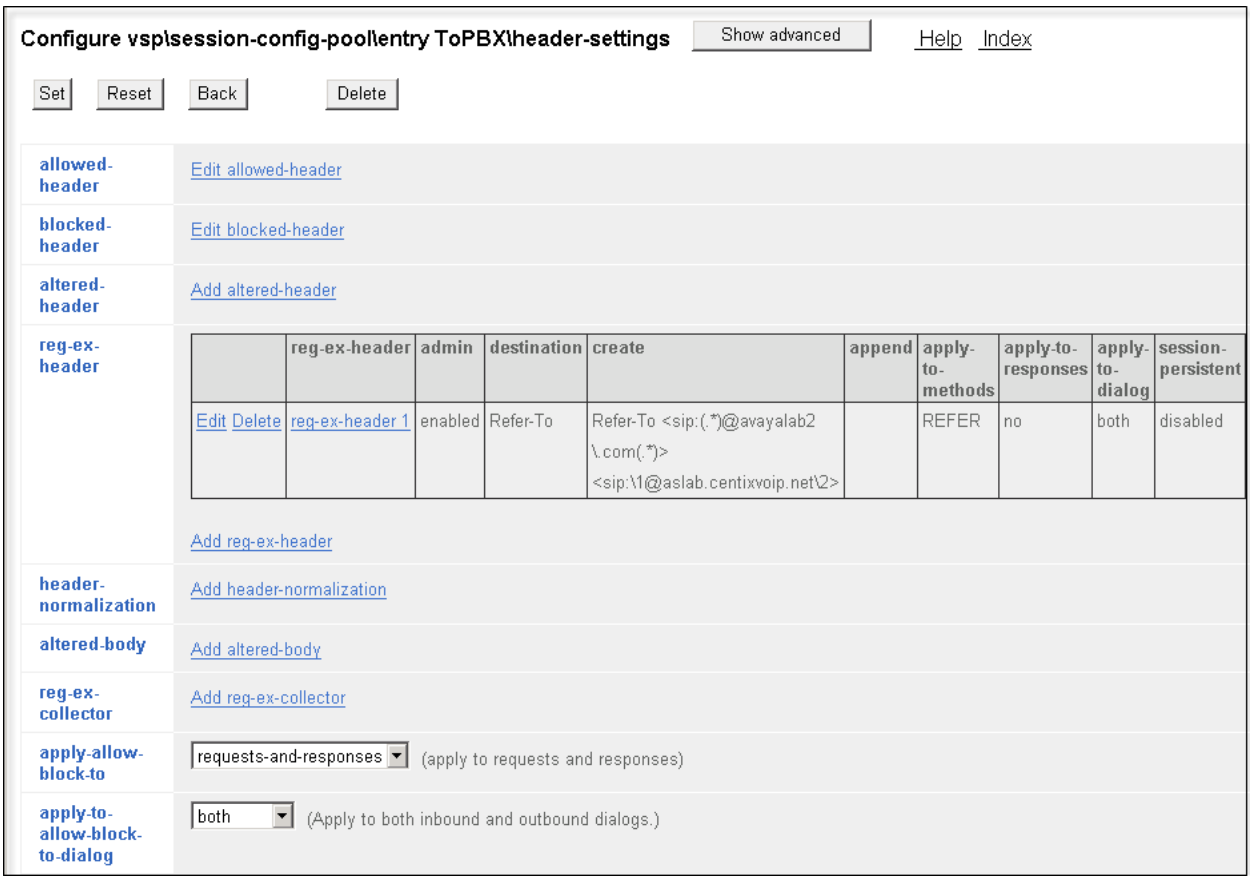
In the **expression** field, enter a regular expression to match. In the sample configuration, "**<sip:(.*)@avayalab2\.com(.*)>**" was entered. In this expression, the first (.*) will match and store any user part of the Refer-To header. The second instance of (.*) matches and stores any UUI if present. The domain "avayalab2.com" is what the AA-SBC would otherwise put in the Refer-To header host part.

In the **replacement** field, "**<sip:\1@aslab.centixvoip.net\2>**" was entered. The variable "\1" is the stored user part from the original Refer-To header containing the Refer-To number, corresponding to the first instance of "(.*)" from the **expression**. The variable "\2" is any stored UUI from the original Refer-To header, corresponding to the second instance of "(.*)" from the **expression**.

After completing the **source**, **expression** and **replacement** fields as appropriate, click **Create**.

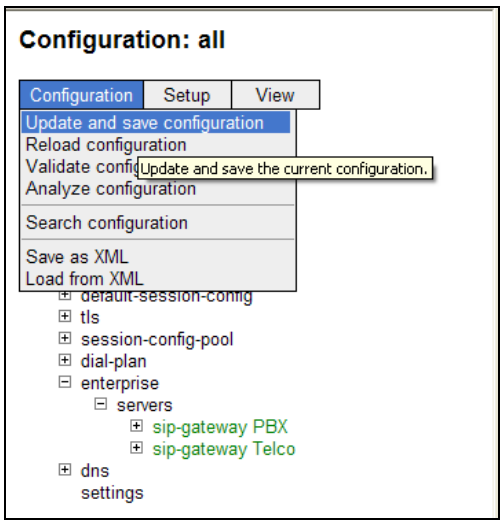


The following screen shows the completed rule. Click **Set** to complete the configuration



7.2.7. Save the Configuration

To save the configuration, begin by clicking on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.



8. AT&T Mobility SIP Trunk Service Configuration

Information about how to establish the AT&T Mobility SIP Trunk Service 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 SBC 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. Session Border Controller:
   - **Call Logs** - On the web user interface of the SBC, the **Call Logs** tab can provide useful diagnostic or troubleshooting information.

2. 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.

3. 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.

10. Conclusion

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

These Application Notes describe the configuration necessary to connect the above service to the Avaya Aura® Solution for Midsize Enterprise 6.1.

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] *Avaya Aura® Solution for the Midsize Enterprise (ME) 6.1 Intelligent Workbook. July 2011.*

[2] *Installing and Configuring Avaya Aura® Solution for Midsize Enterprise, Release 6.1, Issue 3.1, July 2011.*

[3] *Avaya Aura® Solution for the Midsize Enterprise Release Notes, Release 6.1, July 2011.*

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

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

[6] *Administering Avaya Aura® Communication Manager*, *June2010, Document Number 03-300509*.

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

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

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

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

[11] *Avaya Aura® Session Border Controller System Administration Guide, September 2010.*

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

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

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

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

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

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

Appendix A: Avaya Aura® SBC Configuration File

```
#
#  Copyright (c) 2004-2011  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 17:11:58 Wed 2011-10-19
#
config cluster
 config box 1
  set hostname me-sbc.sil.miami.avaya.com
  set timezone America/New_York
  set name me-sbc.sil.miami.avaya.com
  set identifier 00:ca:fe:51:81:77
  config interface eth0
   config ip mgmt
    set ip-address static 10.5.5.19/24
    config ssh
     set mode ssh-2
    return
    config snmp
     set trap-target 10.5.5.11 162
     set trap-filter generic
     set trap-filter dos
     set trap-filter sip
     set trap-filter system
    return
    config web
     set ciphers
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WIT
H_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC
_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_R
SA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA
    return
    config web-service
     set protocol https 8443
     set authentication certificate "vsp\tls\certificate ws-cert"
    return
    config icmp
    return
    config routing
     config route Default
      set gateway 10.5.5.254
     return
     config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.5.5.10
     return
     config route Static1
      set admin disabled
     return
     config route Static2
      set admin disabled
     return
     config route Static3
```

```
     set admin disabled
    return
    config route Static4
     set admin disabled
    return
    config route Static5
     set admin disabled
    return
    config route Static6
     set admin disabled
    return
    config route Static7
     set admin disabled
    return
    config route MgmtDefault
     set gateway 10.5.5.254
    return
   return
  return
 return
 config interface eth1
  config ip inside
   set ip-address static 10.5.5.20/24
   config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
   return
   config icmp
   return
   config media-ports
   return
   config routing
    config route Default
     set gateway 10.5.5.254
    return
   return
  return
 return
 config interface eth2
  config ip outside
   set ip-address static 172.16.1.5/24
   config sip
    set udp-port 5060 "" "" any 0
   return
   config media-ports
    set base-port 50000
    set count 4999
   return
   config routing
    config route Default
     set admin disabled
    return
    config route external-sip-media-1
     set destination network 192.168.10.0/24
     set gateway 172.16.1.254
```

```
     return
    return
    config kernel-filter
     config allow-rule allow-sip-udp-from-peer-1
      set destination-port 5060
      set source-address/mask 192.168.10.0/24
      set protocol udp
     return
     config deny-rule deny-all-sip
      set destination-port 5060
     return
    return
   return
  return
  config cli
   set prompt me-sbc.sil.miami.avaya.com
  return
 return
return

config services
 config event-log
  config file access.log
   set filter access info
   set count 3
  return
  config file system.log
   set filter system info
   set count 3
  return
  config file general.log
   set filter general info
   set count 3
  return
  config file error.log
   set filter all error
   set count 3
  return
  config file db.log
   set filter db debug
   set filter dosDatabase info
   set count 3
  return
  config file management.log
   set filter management info
   set count 3
  return
  config file peer.log
   set filter sipSvr info
   set count 3
  return
  config file dos.log
   set filter dos alert
   set filter dosSip alert
   set filter dosTransport alert
   set filter dosUrl alert
```

```
   set count 3
  return
  config file krnlsys.log
   set filter krnlsys debug
   set count 3
  return
 return
return

config master-services
 config database
  set media enabled
 return
return

config vsp
 set admin enabled
 config default-session-config
  config media
   set anchor enabled
   set rtp-stats enabled
  return
  config sip-directive
   set directive allow
  return
  config log-alert
  return
  config third-party-call-control
   set handle-refer-locally disabled
  return
 return
 config tls
  config default-ca
   set ca-file /cxc/certs/sipca.pem
  return
  config certificate ws-cert
   set certificate-file /cxc/certs/ws.cert
  return
  config certificate aasbc.p12
   set certificate-file /cxc/certs/aasbc.p12
   set passphrase-tag aasbc-cert-tag
  return
 return
 config session-config-pool
  config entry ToTelco
   config to-uri-specification
    set host next-hop
   return
   config from-uri-specification
    set host local-ip
   return
   config request-uri-specification
    set host next-hop
   return
   config p-asserted-identity-uri-specification
   return
```

```
   config header-settings
    set blocked-header P-Location
    set blocked-header Alert-Info
    config altered-header 1
     set source-header Diversion
     set source-field selection ".*avayalab2\.com" aslab.centixvoip.net
     set destination Diversion
     set destination-field host
    return
   return
  return
  config entry ToPBX
   config to-uri-specification
    set host next-hop-domain
   return
   config request-uri-specification
    set user to-uri
    set host next-hop-domain
   return
   config header-settings
    config reg-ex-header 1
     set destination Refer-To
     set create Refer-To "<sip:(.*)@avayalab2\.com(.*)>"
"<sip:\1@aslab.centixvoip.net\2>"
     set apply-to-methods REFER
    return
   return
  return
  config entry Discard
   config sip-directive
   return
  return
 return
 config dial-plan
  config route Default
   set priority 500
   set location-match-preferred exclusive
   set session-config vsp\session-config-pool\entry Discard
  return
  config source-route FromTelco
   set peer server "vsp\enterprise\servers\sip-gateway PBX"
   set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
   set peer server "vsp\enterprise\servers\sip-gateway Telco"
   set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
 return
 config enterprise
  config servers
   config sip-gateway PBX
    set domain avayalab2.com
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
```

```
     config server PBX1
      set host 10.5.5.15
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set failover-detection ping
    set ping-interval 300
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
     config server Telco1
      set host 192.168.10.250
     return
    return
   return
  return
 return
 config dns
  config resolver
   config server 192.168.10.100
   return
  return
 return
 config settings
  set read-header-max 8191
 return
return

config external-services
return

config preferences
 config gui-preferences
  set enum-strings SIPSourceHeader Diversion
  set enum-strings SIPSourceHeader Refer-To
 return
return

config access
 config permissions superuser
  set cli advanced
 return
 config permissions read-only
  set config view
  set actions disabled
 return
 config users
  config user admin
   set password 0x00d8b88dfc7517d214bd8c404489c41bf575547211ad1a7521c05d24f5
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x0069d2a6686bb2d23563e1e4cd90275bd1735222619152e9d64ac2385c
   set permissions access\permissions read-only
```

```
  return
  config user init
   set password 0x002ca274c8fd8f18d046301ba7127d77562fd2391e039de0735b0dd7b9
   set permissions access\permissions superuser
  return
  config user craft
   set password 0x006caa3956d62ee91793108eb4b2a4fa4c6fc08f9e16c9bcbc163bd22e
   set permissions access\permissions superuser
  return
  config user dadmin
   set password 0x00d4041dc8a804e2c42bacc8258c9ee9c757b0797d4c8019ddc4f90926
   set permissions access\permissions read-only
  return
 return
return

config features
return
```

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.