Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller 6.0 to support Alestra Enlace IP SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between the service provider Alestra in Mexico and Avaya SIP enabled enterprise solution. The Avaya SIP enabled enterprise solution consists of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Session Border Controller, and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya Aura® Session Border Controller or Avaya Aura® Session Manager. The official name of Alestra's SIP Trunk offering is **"Enlace IP"**.

Alestra Enlace IP SIP Trunk Service provides PSTN access via SIP trunks between the enterprise and Alestra's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Service provider Alestra in Mexico is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) Trunking between the service provider Alestra in Mexico and an Avaya SIP enabled enterprise solution.

In the sample configuration, the Avaya SIP enabled enterprise solution consists of an Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Session Border Controller, and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya Aura® Session Border Controller or Avaya Aura® Session Manager.

Customers using Avaya SIP-enabled enterprise solution with Alestra Enlace IP SIP Trunk service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional analog trunks and/or PSTN trunks such as ISDN-PRI. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting an Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to Alestra Enlace IP SIP Trunk service via the public internet, as depicted in **Figure 1.**

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability, the following areas were tested for compliance:

- Static IP.
- SIP OPTIONS messages.
- Incoming calls from the PSTN were routed to the DID numbers assigned by Alestra. Incoming PSTN calls were terminated to the following end points: Avaya 9640 SIP Telephones, Avaya 9620 IP Telephones (H.323), Avaya 2420 Digital Telephones, Avaya one-X® Communicator (H.323 and SIP modes), Analog Telephones and Fax machines.
- Outgoing calls to the PSTN were routed via Alestra GSX9000 Sonus network to the various PSTN destinations. A local PSTN extension in Monterrey, Mexico & Telephones in the Test Lab connected to the PSTN in the U.S. were used as PSTN end points.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect during normal active call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (w/voice mail off).
- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Note: Testing was done with Codec’s G.729(a) and G.711-Alaw as requested by Alestra (common codec’s used in Mexico).
- No matching codec’s.

- Voice mail and DTMF tone support (Leaving voice mail, retrieving voice mail, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Outbound/Inbound local calls.
- International calls.
- Calls to special numbers (Alestra information: 040, etc.).
- Calling number blocking to and from the PSTN.
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call transfers.
- Station Conference.
- T.38 faxing support (inbound and outbound).
- EC500.
- Simultaneous active calls.
- Long duration calls (> one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

Items not supported or not tested included the following:

- Network Call Redirection using the SIP REFER method was not tested.
- Inbound toll-free calls were not tested.
- 0, 0+10, 411,911, etc. are calls types not supported in Mexico. Instead, calls to special numbers in Mexico were tested (e.g., information: 040, Denuncia: 089, etc.)

2.2. Test Results

Interoperability testing of Alestra Enlace IP SIP trunk service with Avaya SIP-enabled enterprise solution was completed successfully with the following observations/limitations.

- **DTMF digits detection**: In the sample configuration Alestra was sending DTMF digits, both, in-band as audible tones and out-of-band as RTP events (RFC2833) and the two were not precisely aligned. The Avaya G450 Gateway was detecting the in-band and out-of-band digits as two separate digits instead of the same digit sent two ways, and this was causing problems with voice mail retrieval during the login process to the voice mail system. For interoperability, Alestra must disable the sending of in-band digits and only send DTMF digits as out-of-band RTP events. Alestra technician must disable this at the time of service activation. Otherwise, the detection of incoming DTMF digits from the network is unreliable. In-band tones must be disabled when using either the G.711A or G.729A codec. In rare cases if problems persist, the workaround described in **Appendix B** can also be applied. However, this is not recommended unless **absolutely** necessary since it burdens the media resources of the Communication Manager with additional processing.

- **Call Display on transferred calls to PSTN** – Caller ID display is not updated on PSTN phones involved with call transfers from Avaya Aura® Communication Manager to the PSTN. On Call Transfers from Avaya Aura® Communication Manager to the PSTN, after the call transfer is completed, the PSTN phone does not display the actual connected party but instead shows the ID of the host extension that initiated the call transfer. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/Alestra solution. It is listed here simply as an observation.

- **EC500 Mobility Feature** Certain EC500 features rely on verification that the calling number matches the configured mobile number on the **off-pbx-telephone station-mapping** form. Alestra was populating the From header in the inbound INVITE with a number that was not routable, the number contained 81 (e.g., 8112343093). The solution was to normalize the calling number contained in the From header to a routable number. Normalization was done in the Avaya Aura® SBC (see **Section 7.2.6**).

- **Outbound Calling Party Number (CPN) Block**: To support outbound privacy calls (calling party number blocking), Avaya Aura® Communication Manager sends "anonymous" as the calling number in the SIP From header, uses the P-Asserted-Identity (PAI) header to pass the actual calling party number and includes "Privacy: id" in the INVITE. During testing Alestra's network (Sonus) was configured to ignore the SIP From header for this purpose thus the Calling Party Number (CPN) was not blocked. Changes to Alestra's network are needed in order to block the Calling Party Number (CPN).

- **Outgoing G.711-A-law fax calls fail to connect**. The problem is **only** seen with **Outgoing** Fax calls (Communication Manager → PSTN) **and** with **T.38** Interworking with **G.711-Alaw**, incoming fax calls (PSTN → Communication Manager) work fine. Also, **T.38** interworking with **G729(a)** works in both directions (Communication Manager → PSTN and PSTN → Communication Manager). Traces captured indicate successful conversion from **G.711-Alaw** to **T.38** but the "modem connection" fail to be established and the attempt times out. Both fax machines show "connecting", the tone is heard and the attempt is made to scan the 1st page but fails resulting in time out.

  The work around is to use **G.729(a)** as the voice codec prior to the transition to **T.38.**

- Calls originating from PSTN telephones in the U.S. to Mexico DIDs assigned to Avaya Aura® Communication Manager will display **Restricted/Unavailable**; this is a PSTN restriction for **all** calls from the U.S. to Mexico. For testing, Alestra provided a local PSTN number in Monterrey, Mexico. A SIP based Softphone was registered to this local PSTN number and was used to originate and terminate calls to and from the Mexican PSTN to Avaya Aura® Communication Manager. Alestra also provided access to a WEB based GUI allowing feature changes to this local PSTN number.

Note: International long distance call to Mexico always will be presented without a Caller ID. – International Rule between carriers.

2.3. Support

2.3.1. Avaya

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

2.3.2. Alestra

For technical support on Alestra Enlace IP SIP Trunk service offer visit the online support site at http://www.alestra.com.mx/negocios.asp?id=206

3. Reference Configuration

Figure 1 below illustrates the test configuration used. The test configuration simulates an enterprise site with Avaya SIP-enabled enterprise solution connected to Alestra Enlace IP SIP trunk service through the public internet.

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

- Avaya S8300 Server running Avaya Aura® Communication Manager.
- Avaya G450 Media Gateway.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® Session Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® System Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® SBC.
- Avaya 9620-Series IP Telephones (H.323).
- Avaya 9640 Telephones (SIP).
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya 2420 Digital telephones.
- Analog Telephones.
- Fax machines
- Desk top with administration interfaces
- Lap-top with SIP Softphone connected to the local PSTN in Monterrey, Mexico.

Located at the edge of the enterprise is the Avaya Aura® SBC. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya Aura® SBC. In this way, the Avaya Aura® SBC can protect the enterprise against any SIP-based attacks. The Avaya Aura® SBC provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya Aura® SBC and Alestra across the public IP network is SIP over UDP. The transport protocol between the Avaya Aura® SBC and Avaya Aura® Session Manager across the enterprise IP network is SIP over TCP. The transport protocol between Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the enterprise IP network is SIP over TLS. For ease of troubleshooting during testing, the compliance test was conducted with the Transport Method set to **tcp** between Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

For security reasons, any actual public IP addresses used in the configuration have been masked. Similarly, any references to real routable PSTN numbers have also been masked to numbers that cannot be routed by the PSTN.

One SIP trunk group was created between the Avaya Aura® Communication Manager and the Avaya Aura® Session Manager to carry the traffic to and from the service provider (two-way trunk group). To separate the codec settings required by the service provider from the codec used by the telephones, two IP network regions were created, each with a dedicated signaling group. For inbound calls, the calls flowed from the service provider to Avaya Aura® SBC then to Avaya Aura® Session Manager. Avaya Aura® Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Avaya Aura® Communication Manager) and on which link to send the call. Once the call arrived at Avaya Aura® Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions could be performed.

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

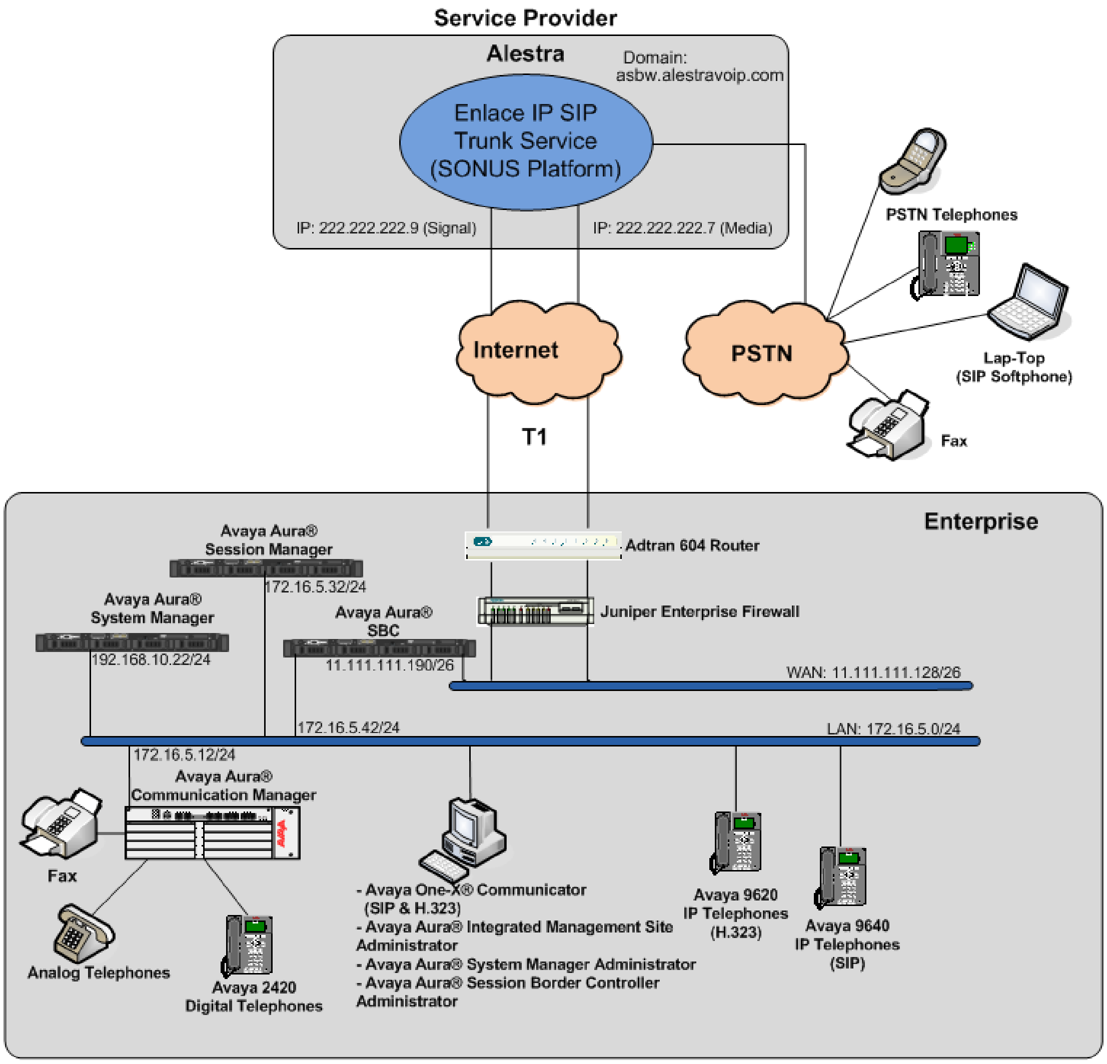

Service Provider
Alestra
Domain: asbw.alestravoip.com
Enlace IP SIP Trunk Service (SONUS Platform)
IP: 222.222.222.9 (Signal)
IP: 222.222.222.7 (Media)
PSTN Telephones
Internet
PSTN
Lap-Top (SIP Softphone)
Fax
T1
Enterprise
Avaya Aura® Session Manager
172.16.5.32/24
Adtran 604 Router
Avaya Aura® System Manager
Avaya Aura® SBC
Juniper Enterprise Firewall
192.168.10.22/24
11.111.111.190/26
WAN: 11.111.111.128/26
172.16.5.42/24
LAN: 172.16.5.0/24
172.16.5.12/24
Avaya Aura® Communication Manager
Fax
Analog Telephones
Avaya 2420 Digital Telephones
- Avaya One-X® Communicator (SIP & H.323)
- Avaya Aura® Integrated Management Site Administrator
- Avaya Aura® System Manager Administrator
- Avaya Aura® Session Border Controller Administrator
Avaya 9620 IP Telephones (H.323)
Avaya 9640 IP Telephones (SIP)

Figure 1: Avaya SIP enabled enterprise solution and Alestra Enlace IP SIP Trunk Service

3.1. DIDs and client types used for testing

The following DIDs client types were used for testing (DID Numbers in Monterrey, Mexico)

DID Number	Client Type	Registered with
(81) 1234-3040	Avaya 9620 IP Telephone (H323)	Avaya Aura® Communication Manager
(81) 1234-3041	Avaya 9620 IP Telephone (H323)	Avaya Aura® Communication Manager
(81) 1234-3042	Avaya 9620 IP Telephone (H323)	Avaya Aura® Communication Manager
(81) 1234-3043		Used for EC500 (Idle Appearance)
(81) 1234-3044	Avaya one-X® Communicator (SIP)	Avaya Aura® Session Manager
(81) 1234-3045	2500 (Pots)	Avaya Aura® Communication Manager
(81) 1234-3046	Avaya 2420 Digital Telephone	Avaya Aura® Communication Manager
(81) 1234-3047	Avaya 9640 Telephone (SIP)	Avaya Aura® Session Manager
(81) 1234-3048	Avaya one-X® Communicator (H.323)	Avaya Aura® Communication Manager
(81) 1234-3049	Not Used	---
(81) 1234-3093	SIP Softphone	Local PSTN in Monterrey, Mexico
1-555-123-0788	Avaya 9641G IP Telephone	Behind a PBX in the U.S.
1-555-123-0772	Analog Line/Phone	Connected to the Local PSTN in the U.S.

Table 1 – DID and client Types used for testing

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager running on a HP® Proliant DL360 G7 Server.	6.0.1 SP3 (R016x.00.1.510.1)
G450 Media Gateway	30.12.1
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.1 service pack 3 (ASM 6.1.3.0.613006)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.1 Service Pack 3 Build No. 6.1.0.0.7345-6.1.5.112
Avaya Aura® Session Border Controller running on a HP® Proliant DL360 G7 Server.	SBCT 6.0.2.0.3 (sbc E362P4)
Avaya Aura® Integrated Management Site Administrator	6.0.07
Avaya Aura® Communication Manager Messaging (CMM)	6.0.1.8.0
Avaya one-X® Communicator (SIP & H.323)	6.1.1.02-SP1-32858
Avaya 9620 Series IP Phones (H.323)	Avaya one-X® Deskphone Edition 3.1
Avaya 96xx Series IP Telephones (SIP)	Avaya one-X® Deskphone Edition SIP 2.6.4
Avaya 2420 Series Digital Phone	--
Lucent Analog Phone	--
Fax Machines	--
SIP Softphone (For use at local PSTN in Monterrey, Mexico)	--
Alestra	
Sonus Network	6.4

Table 2 – Hardware and Software Components Tested

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

5. Configure Avaya Aura® Communication Manager

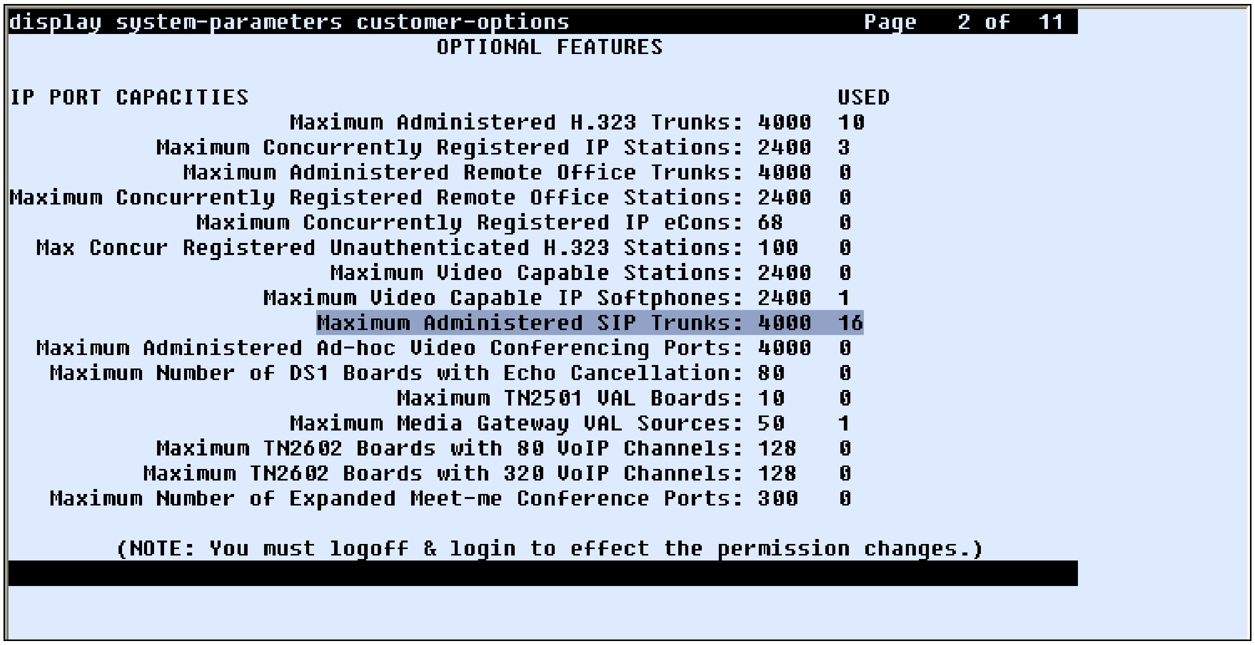
This section describes the procedure for configuring Avaya Aura® Communication Manager. A SIP trunk is established between Avaya Aura® Communication Manager and Avaya Aura® Session Manager for use by signaling traffic to and from Alestra. It is assumed the general installation of Avaya Aura® Communication Manager, Avaya G450 Media Gateway and Avaya Aura® Session Manager has been previously completed.

In configuring the Avaya Aura® Communication Manager, various components such as ip-network-regions, signaling groups, trunk groups, etc. need to be selected or created for use with the SIP connection to the service provider. Unless specifically stated otherwise, any unused ip-network-region, signaling group, trunk group, etc. can be used for this purpose.

The Avaya Aura® Communication Manager configuration was performed using Avaya Integrated Management Site Administrator. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the public 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

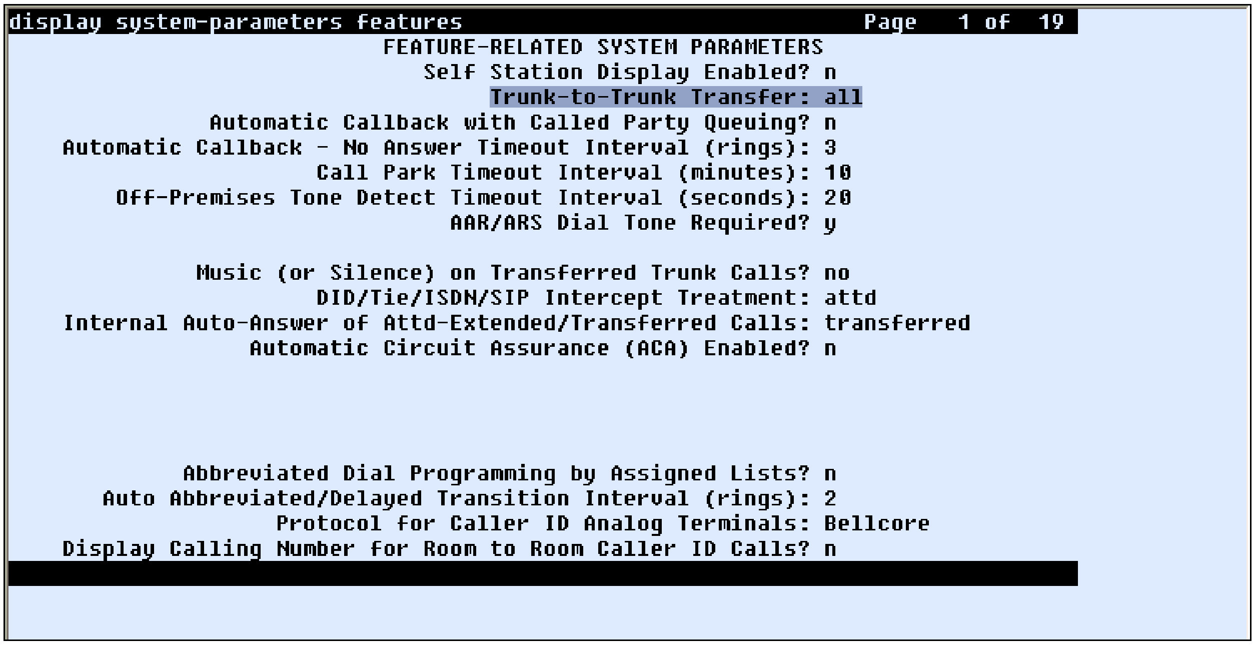
Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 licenses are available and 16 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.



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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  10
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  1
                       Maximum Administered SIP Trunks: 4000  16
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    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.)
```

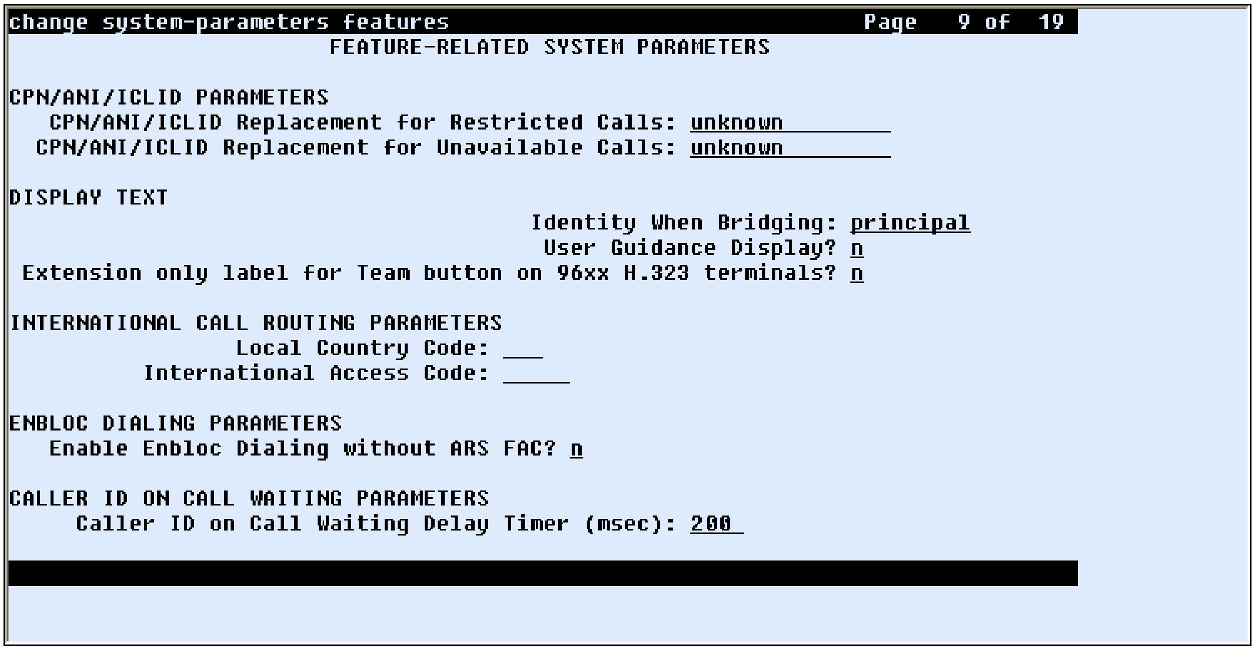
5.2. System Features

Use the **change system-parameters feature** 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**.



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

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



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

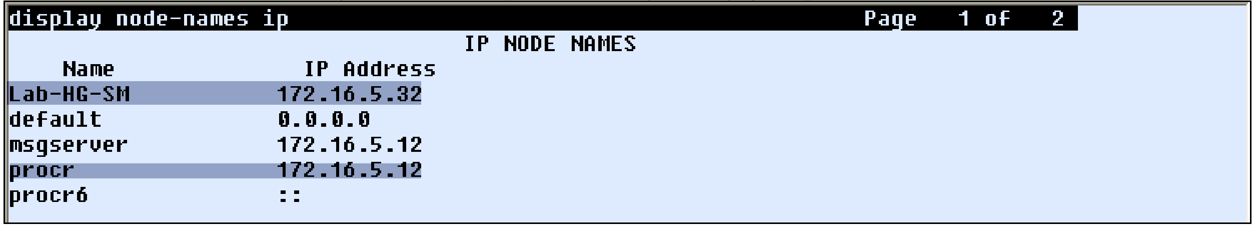
On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **Unknown** for both.



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

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

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

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code: ___
          International Access Code: _____

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

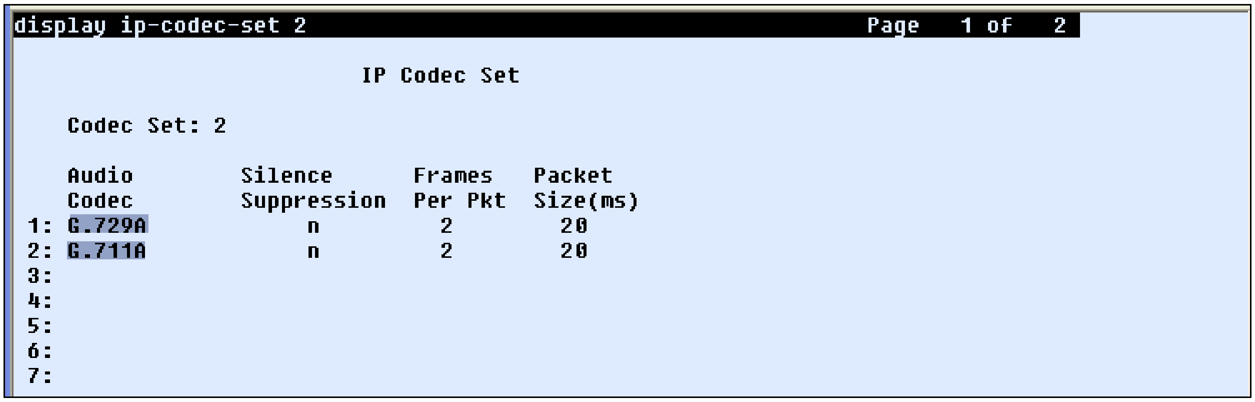
Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8300D Server running Avaya Aura® Communication Manager **(procr**) and for Avaya Aura® Session Manager (**Lab-HG-SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.



```
display node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
Lab-HG-SM            172.16.5.32
default              0.0.0.0
msgserver            172.16.5.12
procr                172.16.5.12
procr6               ::
```

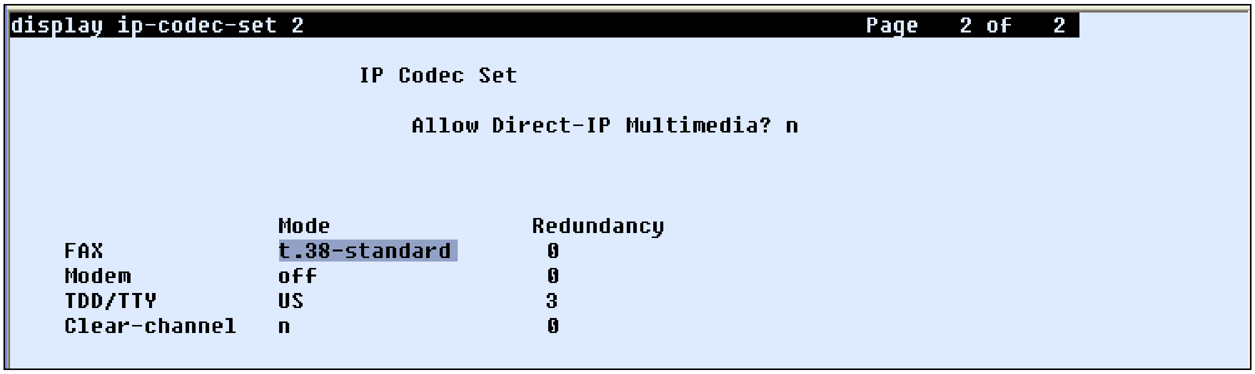
5.4. Codec's

Use the **change ip-codec-set** command to define a list of codec's to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Alestra SIP Trunking supports G.729A and G.711A. Thus, these codec's were included in this set. Enter **G.729A and G.711A** in the **Audio Codec** column of the table. Default values can be used for all other fields.



```
display 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.711A           n          2        20
 3:
 4:
 5:
 6:
 7:
```

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



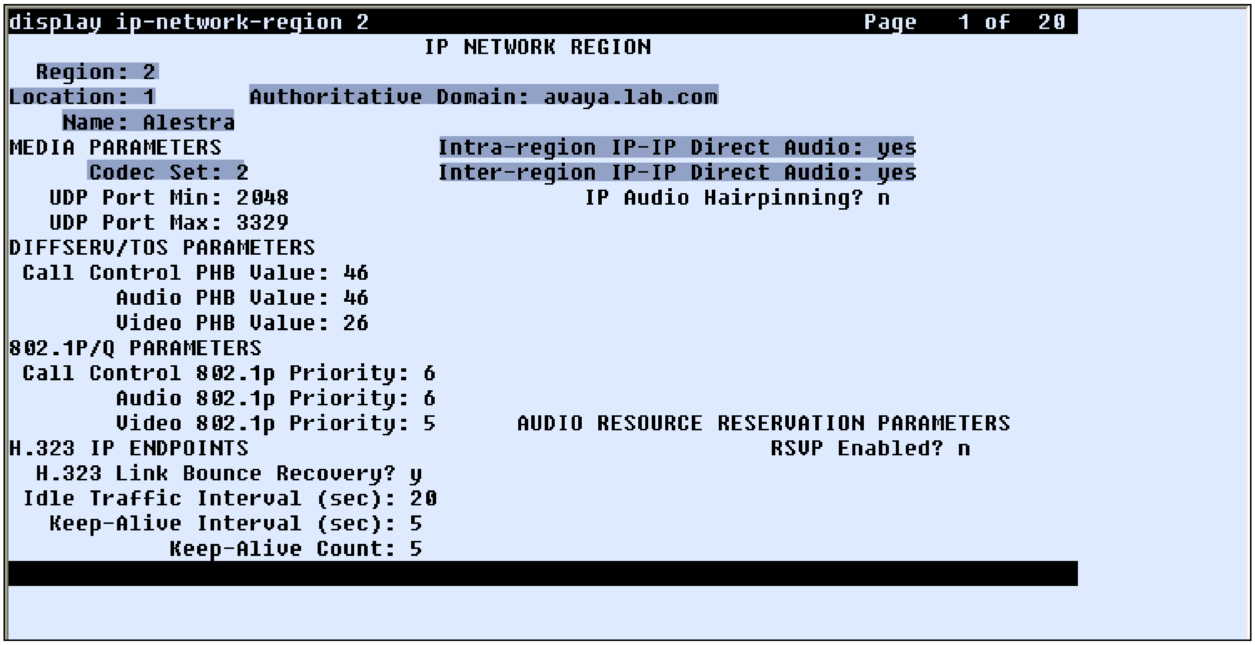
```
display ip-codec-set 2                                         Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



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

5.5. IP Network Region

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

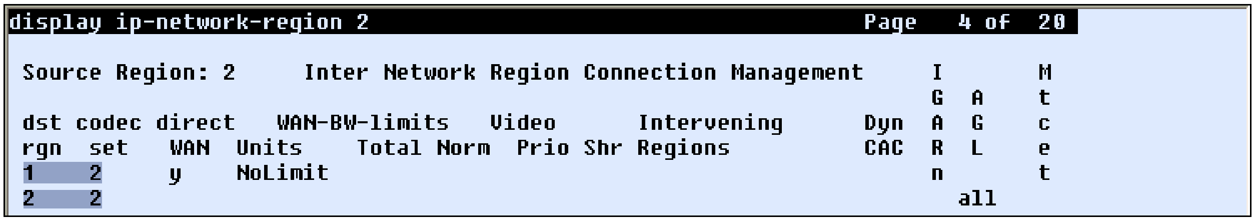
- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.lab.com**. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.

- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.



```
display ip-network-region 2                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.lab.com
    Name: Alestra
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1. 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).

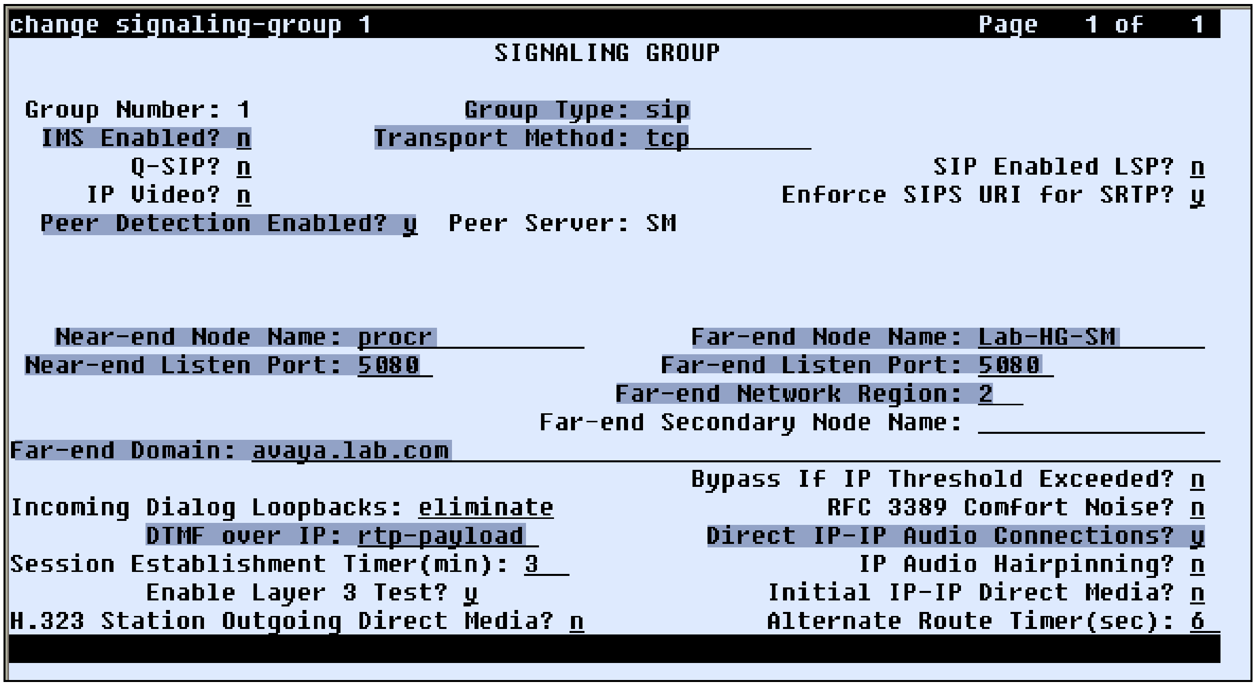


```
display ip-network-region 2                                     Page   4 of  20

 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
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Avaya Aura® Communication Manager and the Avaya Aura® 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 1 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 Avaya Aura® Communication Manager will serve as an Evolution Server for the Avaya Aura® Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp** The transport method specified here is used between the Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The transport method used between the Avaya Aura® Session Manager and the Avaya Aura® SBC is specified as TCP in **Sections 6.6** and **7.1.3**. Lastly, the transport method between the Avaya Aura® SBC and Alestra is UDP. This is defined in **Section 7.1.3** when the service provider name is selected.
- 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 Avaya Aura® Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5080**. (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 Avaya Aura® Communication Manager detects its peer as an Avaya Aura® Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Avaya S8300D Server running Avaya Aura® Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **Lab-HG-SM**. This node name maps to the IP address of Avaya Aura® 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 **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Avaya Aura® Communication Manager to redirect media traffic directly between the inside IP of the SBC 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.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Avaya Aura® Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

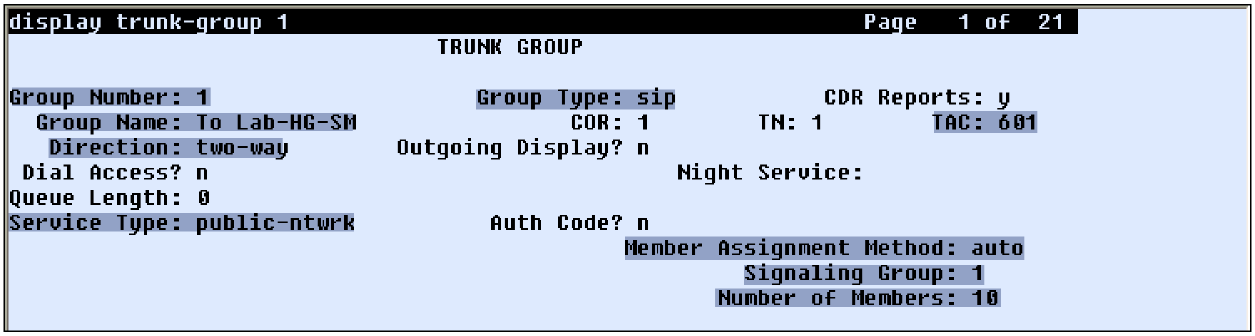


```
change signaling-group 1                                           Page   1 of   1
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                                 SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                   Far-end Node Name: Lab-HG-SM
 Near-end Listen Port: 5080                  Far-end Listen Port: 5080
                                          Far-end Network Region: 2
                                     Far-end Secondary Node Name:
Far-end Domain: avaya.lab.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

5.7. Trunk Group

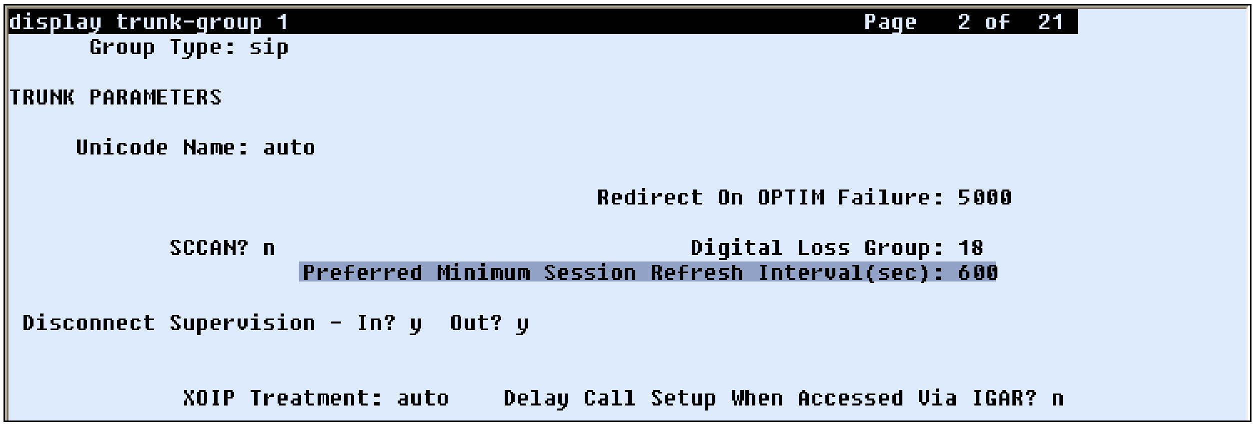
Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

- 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 **Direction** to **two-way**
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.



```
display trunk-group 1                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 1                  Group Type: sip          CDR Reports: y
  Group Name: To Lab-HG-SM              COR: 1        TN: 1        TAC: 601
   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: 1
                                                     Number of Members: 10
```

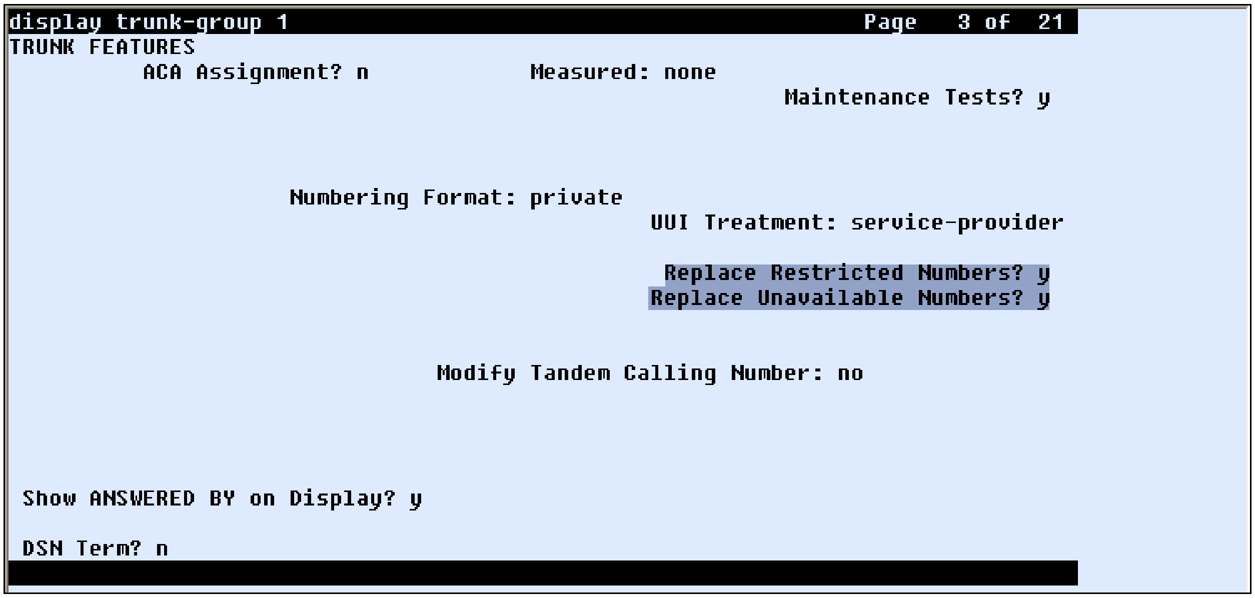
On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.



```
display trunk-group 1                                           Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Avaya Aura® 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 Alestra. Thus, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.9**).

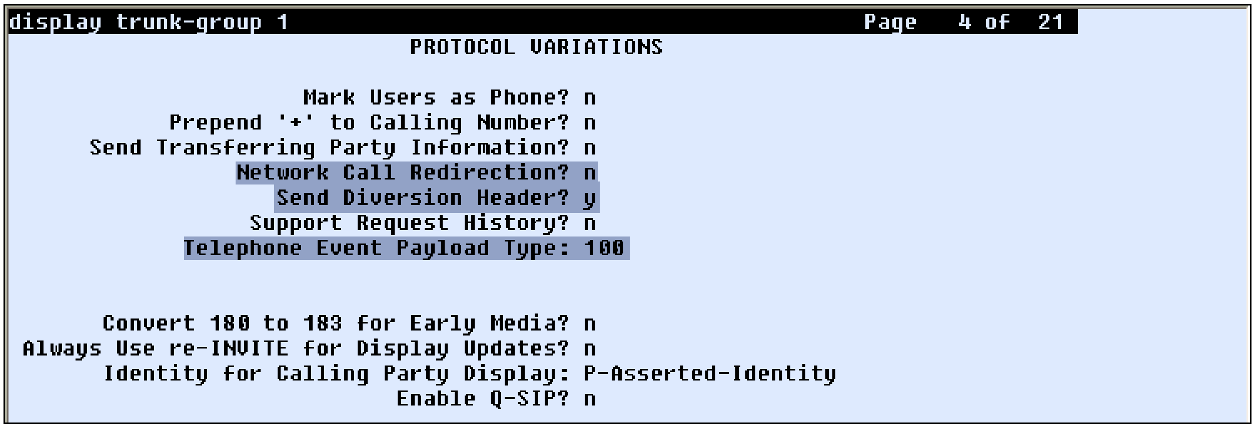
Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values were used for all other fields.



```
display trunk-group 1                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                   Maintenance Tests? y


                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y

 DSN Term? n
```

On **Page 4**, set the **Network Call Redirection** field to **n**. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **100**, the value preferred by Alestra.



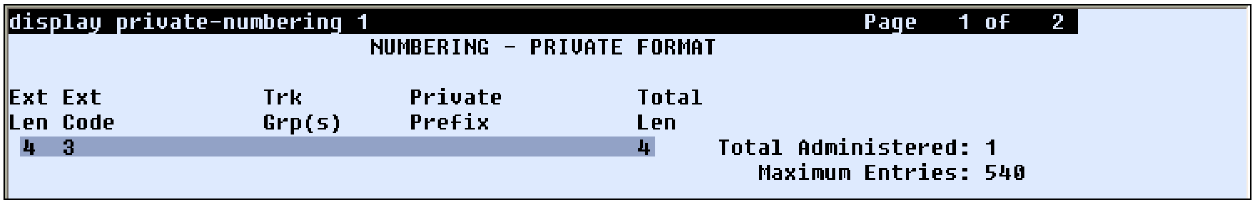
```
display trunk-group 1                                           Page   4 of  21
                              PROTOCOL VARIATIONS

                              Mark Users as Phone? n
                    Prepend '+' to Calling Number? n
              Send Transferring Party Information? n
                         Network Call Redirection? n
                            Send Diversion Header? y
                          Support Request History? n
                     Telephone Event Payload Type: 100


                Convert 180 to 183 for Early Media? n
 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 number will be assigned by the SIP service provider. It is used to authenticate the caller.

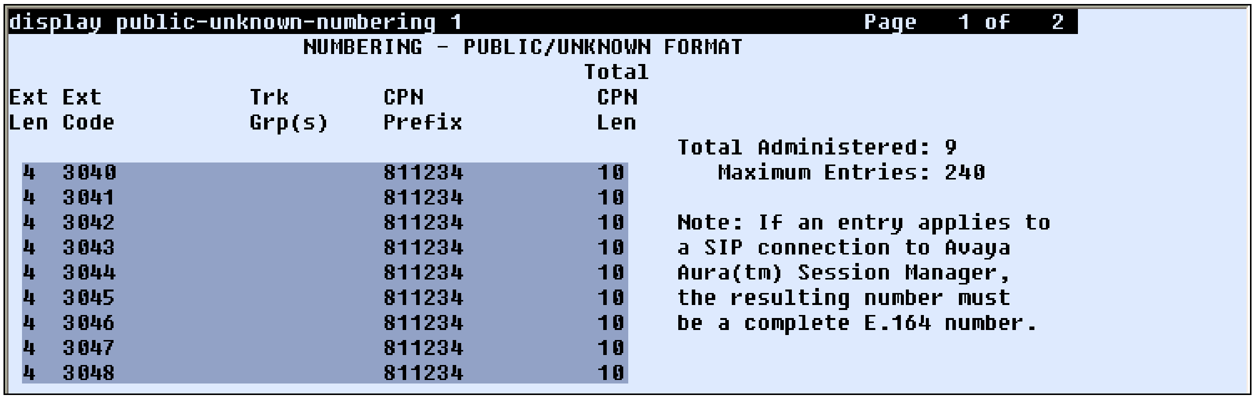
In the sample configuration, 10 DID numbers in Monterrey Mexico were assigned for testing, 81-1234-3040 thru 81-1234-3049. 9 out of the 10 DIDs numbers were assigned to extensions on

Avaya Aura® Communication Manager (extensions 3040 – 3048). Note that only the last 4 digits of the DID number were assigned; this is because in this sample configuration Alestra's network was configured to send only 4 digits to the enterprise. The highlighted row shown below configures any four digit number beginning with 3 (i.e., 3xxx) that uses any trunk group to retain the original 4 digit number (i.e., no digit manipulation is specified), and the Total Len is 4. Thus, these same 4-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 9 extensions. On outbound calls to Alestra, Avaya Aura® Session Manager was used to adapt 4 digits into 10 digits, **see section 6.4**.



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

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
 4  3                                           4     Total Administered: 1
                                                         Maximum Entries: 540
```

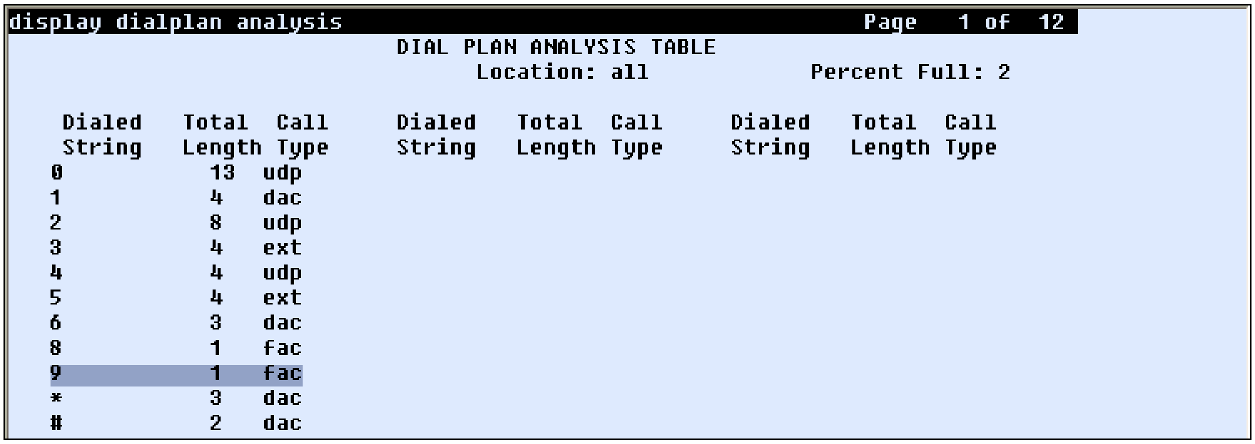
Even though private numbering was selected, currently the number used in the SIP Diversion header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table. In the example shown below the digits 811234 are being prefixed to the 4 digits extension. **81** is the area code for Monterrey, Mexico, **1234** is part of the subscriber's number (e.g., 8112343040, 8112343041, etc.).



```
display public-unknown-numbering 1                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                             Total
Ext Ext            Trk       CPN              CPN
Len Code           Grp(s)    Prefix           Len
                                                    Total Administered: 9
 4  3040                     811234           10       Maximum Entries: 240
 4  3041                     811234           10
 4  3042                     811234           10    Note: If an entry applies to
 4  3043                     811234           10    a SIP connection to Avaya
 4  3044                     811234           10    Aura(tm) Session Manager,
 4  3045                     811234           10    the resulting number must
 4  3046                     811234           10    be a complete E.164 number.
 4  3047                     811234           10
 4  3048                     811234           10
```

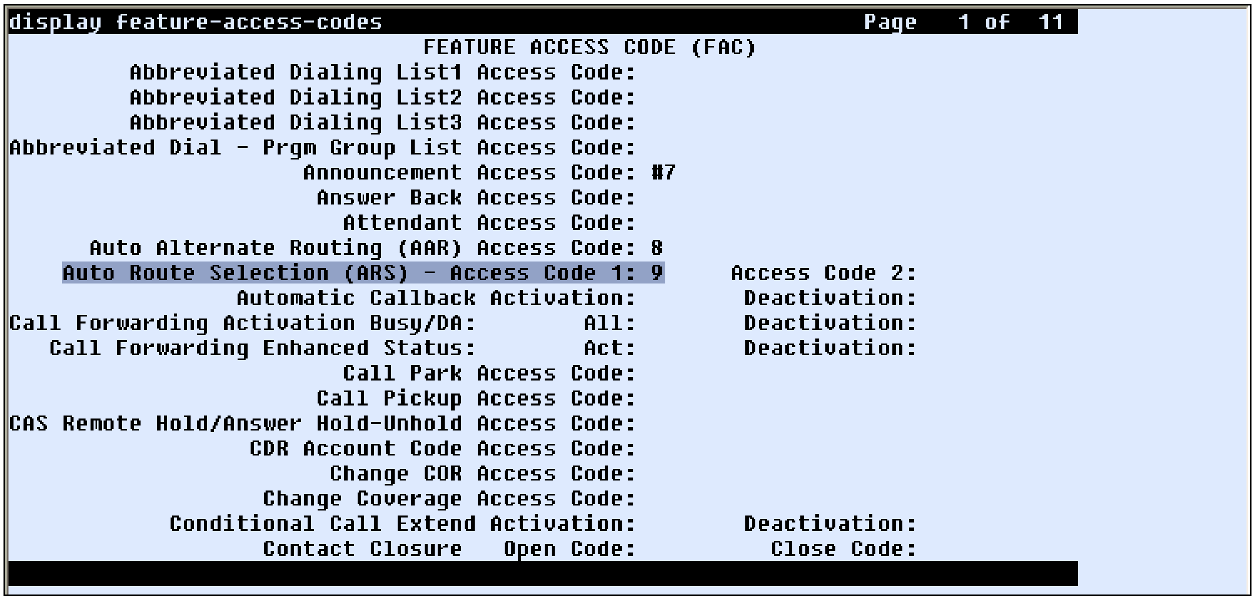
5.9. Outbound Routing

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**).



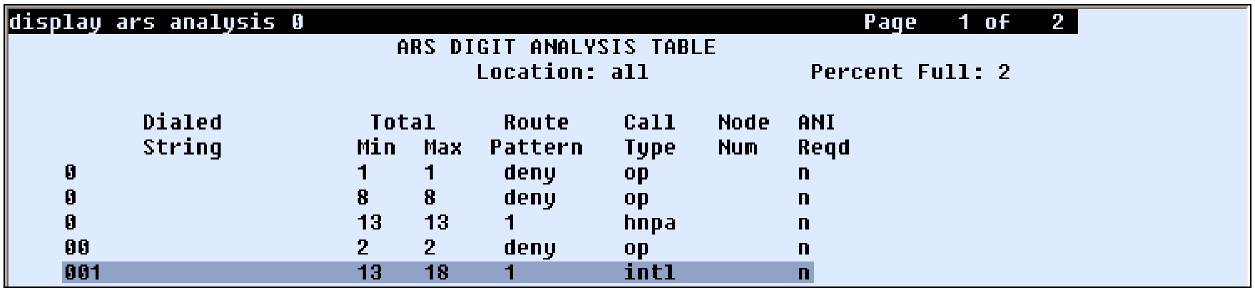
```
display dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   0           13   udp
   1           4    dac
   2           8    udp
   3           4    ext
   4           4    udp
   5           4    ext
   6           3    dac
   8           1    fac
   9           1    fac
   *           3    dac
   #           2    dac
```

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

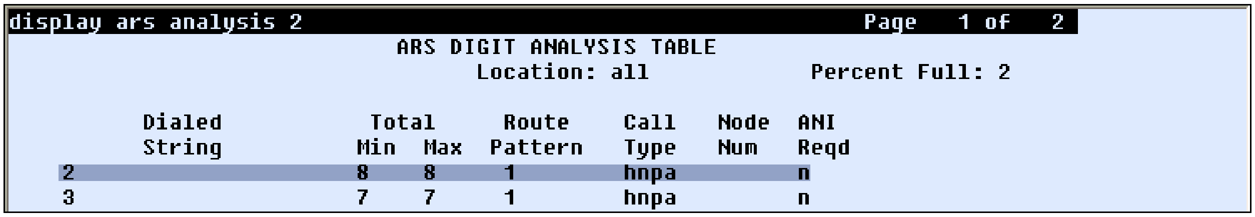


```
display feature-access-codes                                    Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: #7
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the service provider (as defined next).



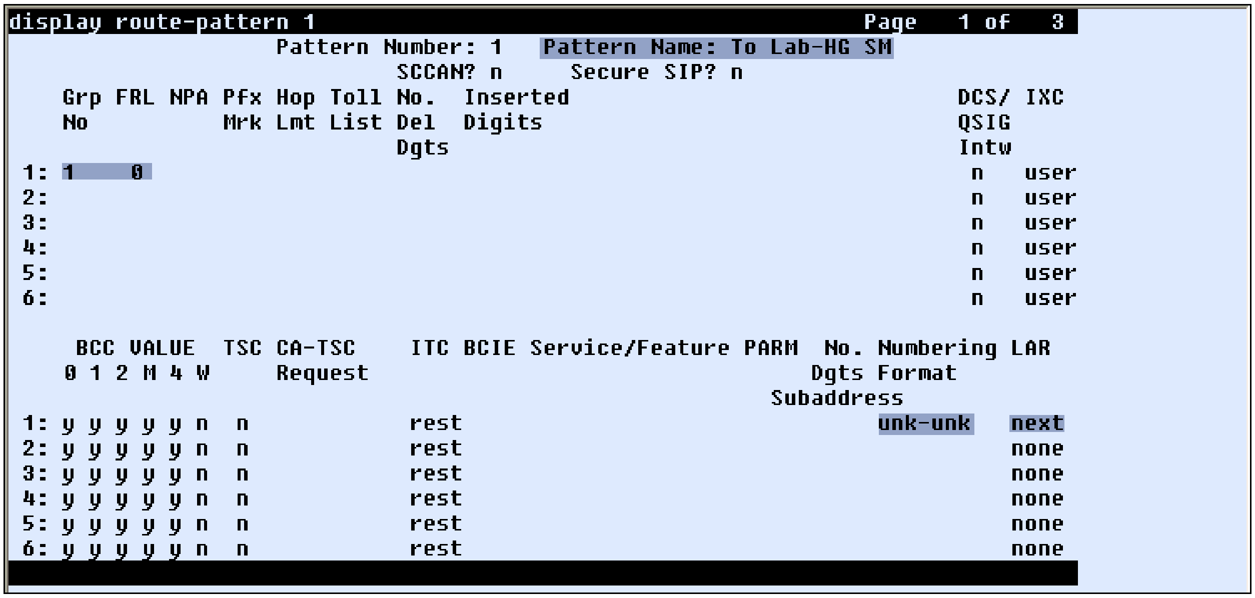
```
display ars analysis 0                                          Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                Location: all         Percent Full: 2

         Dialed            Total     Route     Call    Node   ANI
         String           Min   Max  Pattern   Type    Num    Reqd
   0                      1     1     deny     op             n
   0                      8     8     deny     op             n
   0                      13    13    1        hnpa           n
   00                     2     2     deny     op             n
   001                    13    18    1        intl           n
```



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

         Dialed            Total     Route     Call    Node   ANI
         String           Min   Max  Pattern   Type    Num    Reqd
   2                      8     8     1        hnpa           n
   3                      7     7     1        hnpa           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 1 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 1 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.
- **Numbering Format**: **unk-unk** calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**



```
display route-pattern 1                                         Page   1 of   3
                    Pattern Number: 1   Pattern Name: To Lab-HG SM
                             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: 1    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

6. Configure Avaya Aura® Session Manager

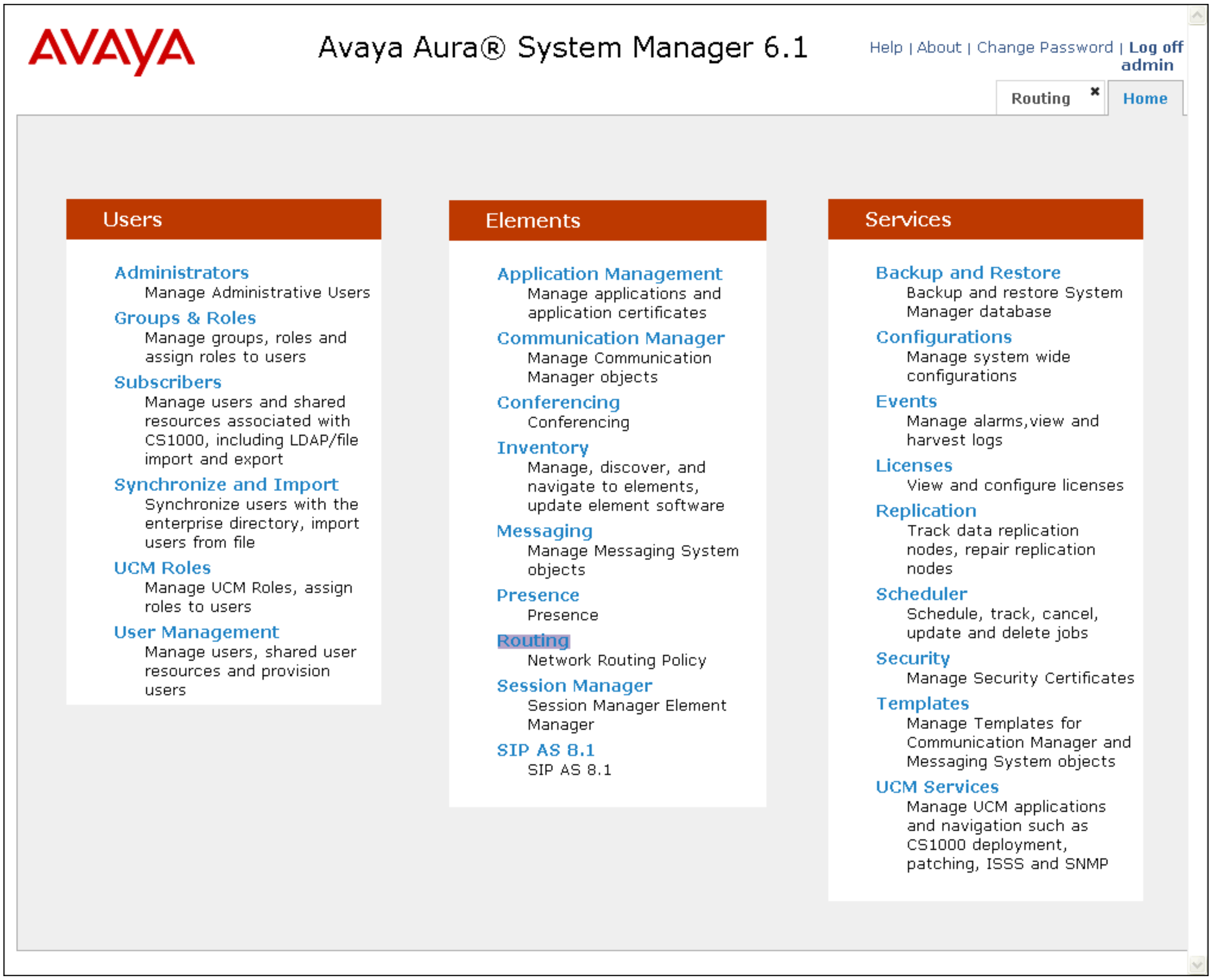
This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to Avaya Aura® Communication Manager, the Avaya Aura® SBC and Avaya Aura® Session Manager
- Entity Links, which define the SIP trunk parameters used by Avaya Aura® 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
- Regular Expressions, which also can be used to route calls
- Avaya Aura® Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager.

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

6.1. System Manager Login and Navigation

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



Avaya Aura® System Manager 6.1

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Subscribers
Manage users and shared resources associated with CS1000, including LDAP/file import and export

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

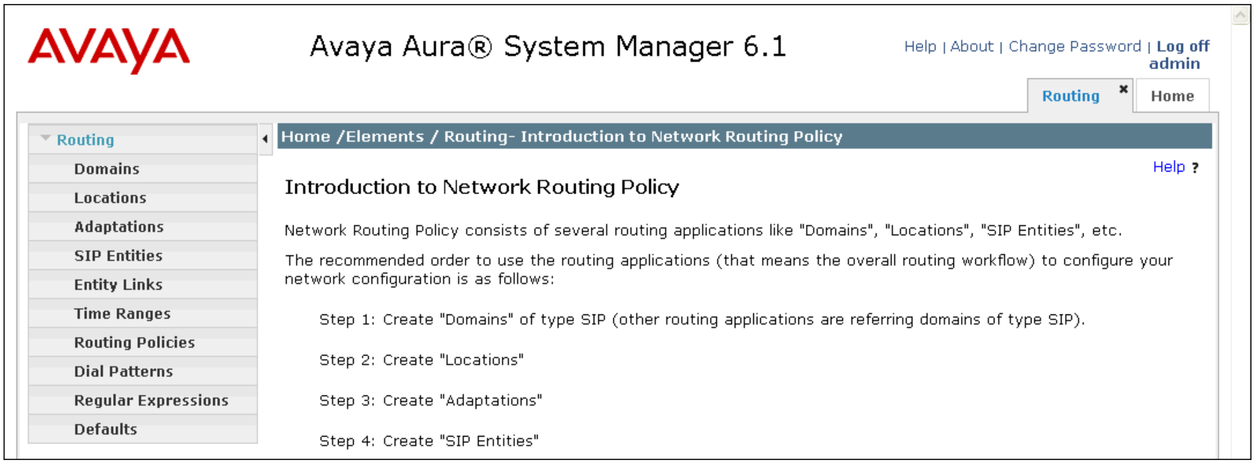
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

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



Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

6.2. Specify SIP Domain

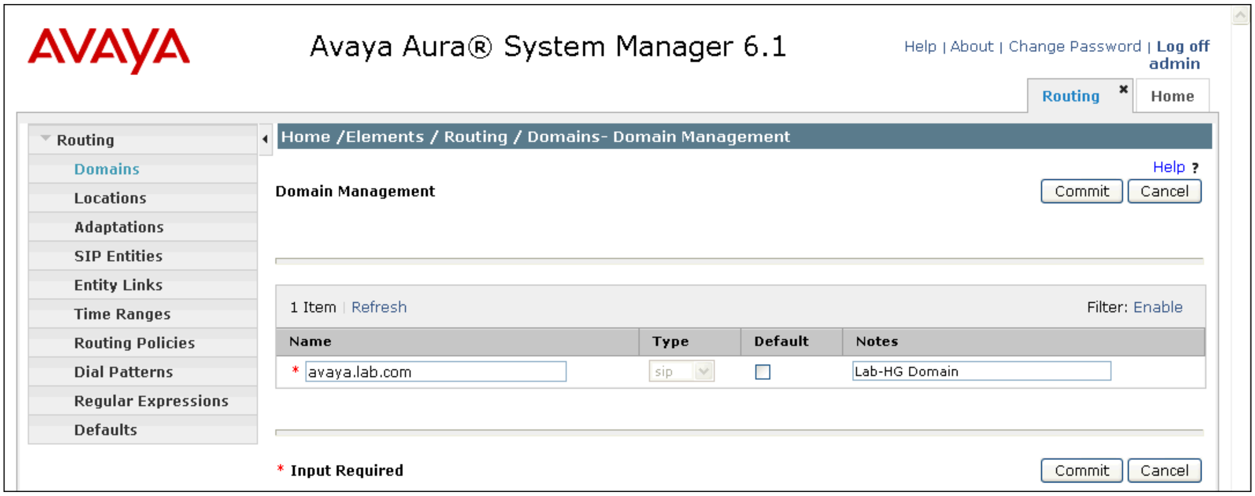
Create a SIP domain for each domain for which Avaya Aura® Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avaya.lab.com**).

Domain **asbw.alestravoip.com** shown under **Figure 1** was not used to route calls, Alestra prefers to use IP addresses instead of Domain for this purpose.

To add a domain, navigate to **Routing → Domains** in the left-hand navigation pane 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.



Domain Management

Name	Type	Default	Notes
* avaya.lab.com	sip	□	Lab-HG Domain

* Input Required

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. 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).

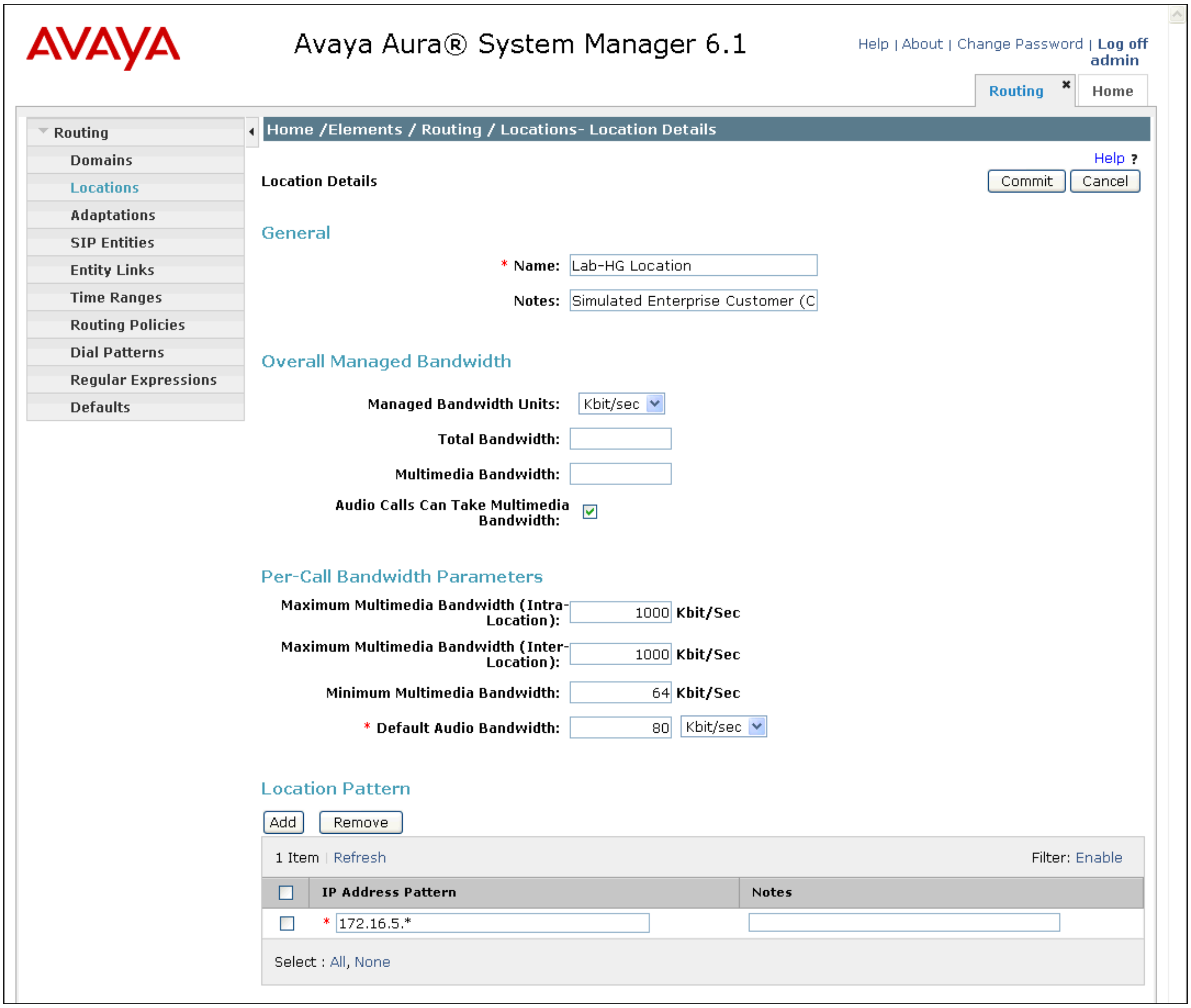
In the **General** section, enter the following values. Use default values for all remaining fields:

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

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

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

The screen below shows the addition of the **Lab-HG Location**, which includes all equipment on the **172.16.5.x** subnet including Avaya Aura® Communication Manager, and Avaya Aura® Session Manager itself. Click **Commit** to save.



Home /Elements / Routing / Locations- Location Details

Location Details

General

* Name:	Lab-HG Location
Notes:	Simulated Enterprise Customer (C

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):	1000	Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	1000	Kbit/Sec
Minimum Multimedia Bandwidth:	64	Kbit/Sec
* Default Audio Bandwidth:	80	Kbit/sec

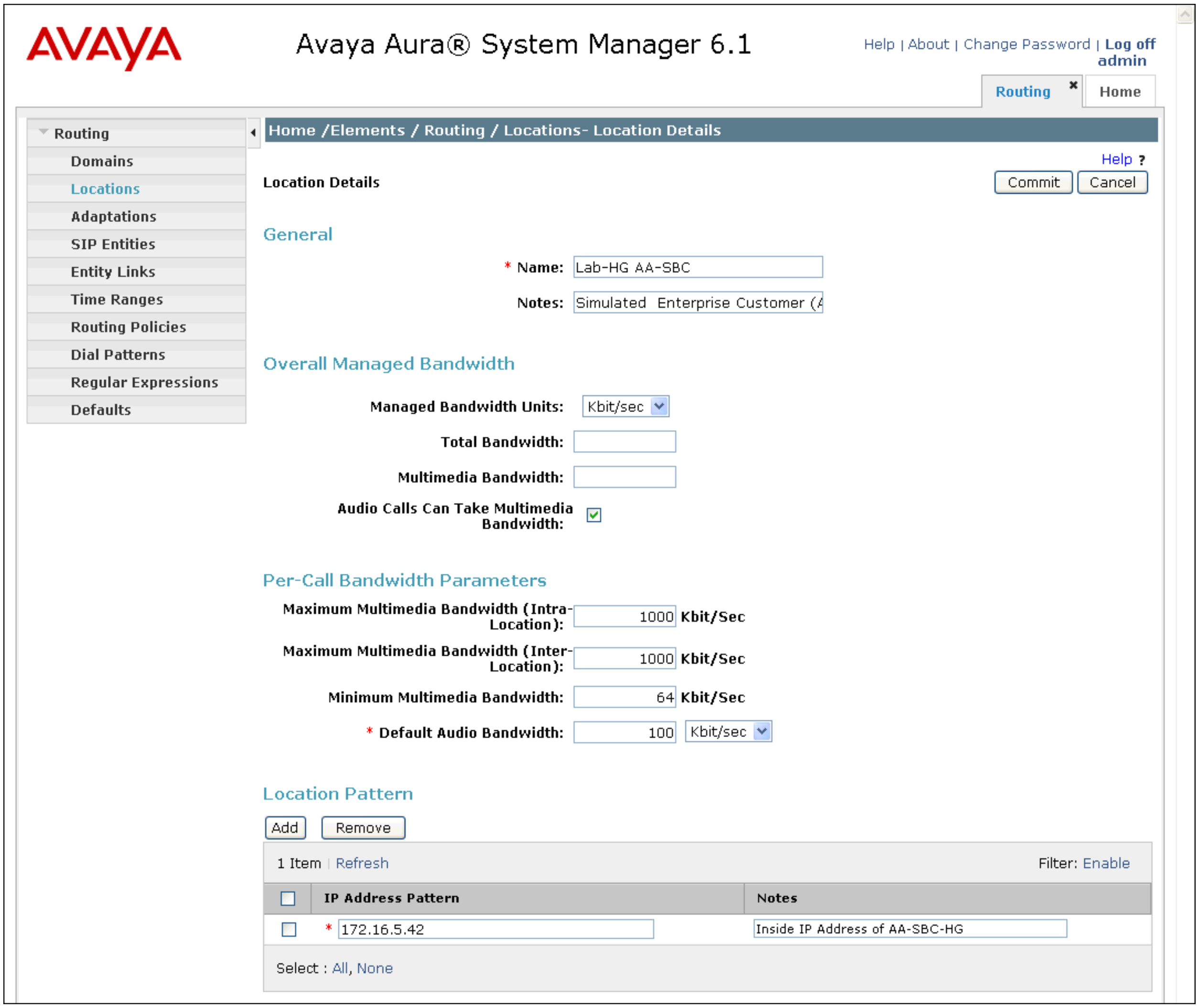
Location Pattern

1 Item | Refresh   Filter: Enable

□	IP Address Pattern	Notes
□	* 172.16.5.*	

Select : All, None

Repeat the preceding procedure to create a separate Location for Avaya Aura® SBC. The screen below shows the addition of the **Lab-HG AA-SBC** location, which specifies the specific inside IP address for the Avaya Aura® SBC. Click **Commit** to save.



Home /Elements / Routing / Locations- Location Details

Location Details

General

* Name: Lab-HG AA-SBC

Notes: Simulated Enterprise Customer (A

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 100 Kbit/sec

Location Pattern

1 Item

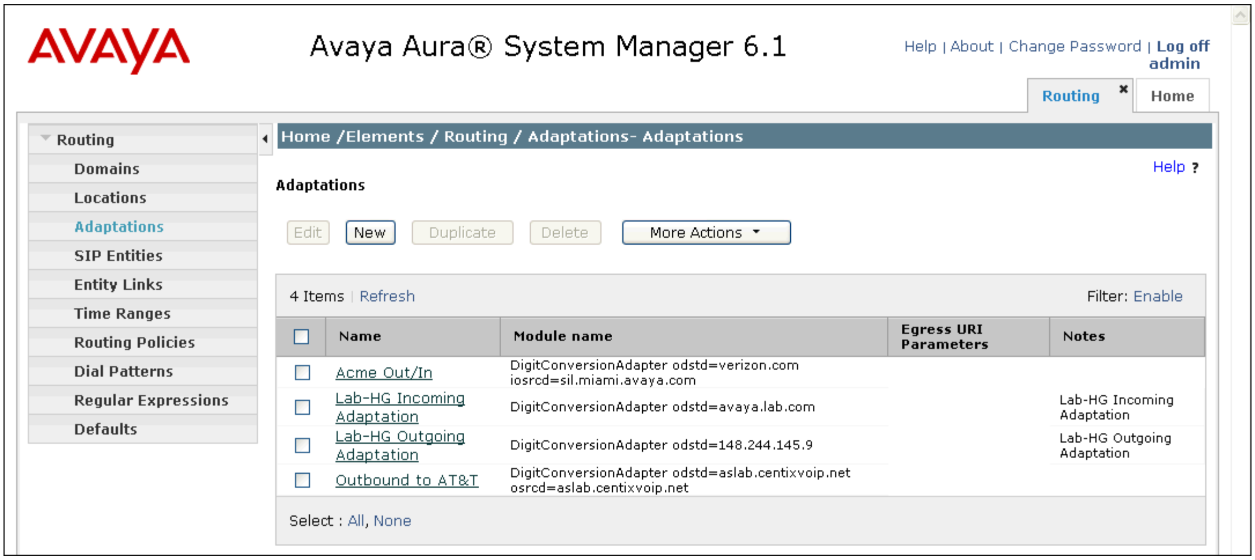
□	IP Address Pattern	Notes
□	* 172.16.5.42	Inside IP Address of AA-SBC-HG

Select : All, None

6.4. Add Adaptation Module

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

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed. The following screen shows a portion of the list of adaptations in the sample configuration.



Adaptations

☐	Name	Module name	Egress URI Parameters	Notes
☐	Acme Out/In	DigitConversionAdapter odstd=verizon.com iosrcd=sil.miami.avaya.com		
☐	Lab-HG Incoming Adaptation	DigitConversionAdapter odstd=avaya.lab.com		Lab-HG Incoming Adaptation
☐	Lab-HG Outgoing Adaptation	DigitConversionAdapter odstd=148.244.145.9		Lab-HG Outgoing Adaptation
☐	Outbound to AT&T	DigitConversionAdapter odstd=aslab.centixvoip.net osrcd=aslab.centixvoip.net		

The adaptations named **Lab-HG Incoming Adaptation** and **Lab-HG Outgoing Adaptation** were configured and used in the compliance test.

Settings for **Lab-HG Outgoing Adaptation:**

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **DigitConversionAdapter**.
- **Module parameter** Enter **odstd=222.222.222.9**

odstd=222.222.222.9 this configuration enables the outbound destination domain to be overwritten with Alestra's proxy IP address. For example, for outbound PSTN calls from the Avaya CPE to Alestra, the Request-URI will contain IP address **222.222.222.9** as expected by Alestra.

Digit Conversion for Outgoing Calls from SM this configuration can be used to append digits to the extension number received from Avaya Aura® Communication Manager for calling number display purpose on **outgoing** calls to the PSTN. In the sample configuration shown below we are matching any four digit extension number starting with **3** and prefixing **811234** to this number. **81** is the area code for Monterrey, Mexico, **1234** is part of the subscriber's number, followed by the 4 digits extension number received from Avaya Aura® Communication Manager (e.g., 8112343040, 8112343041, etc.).

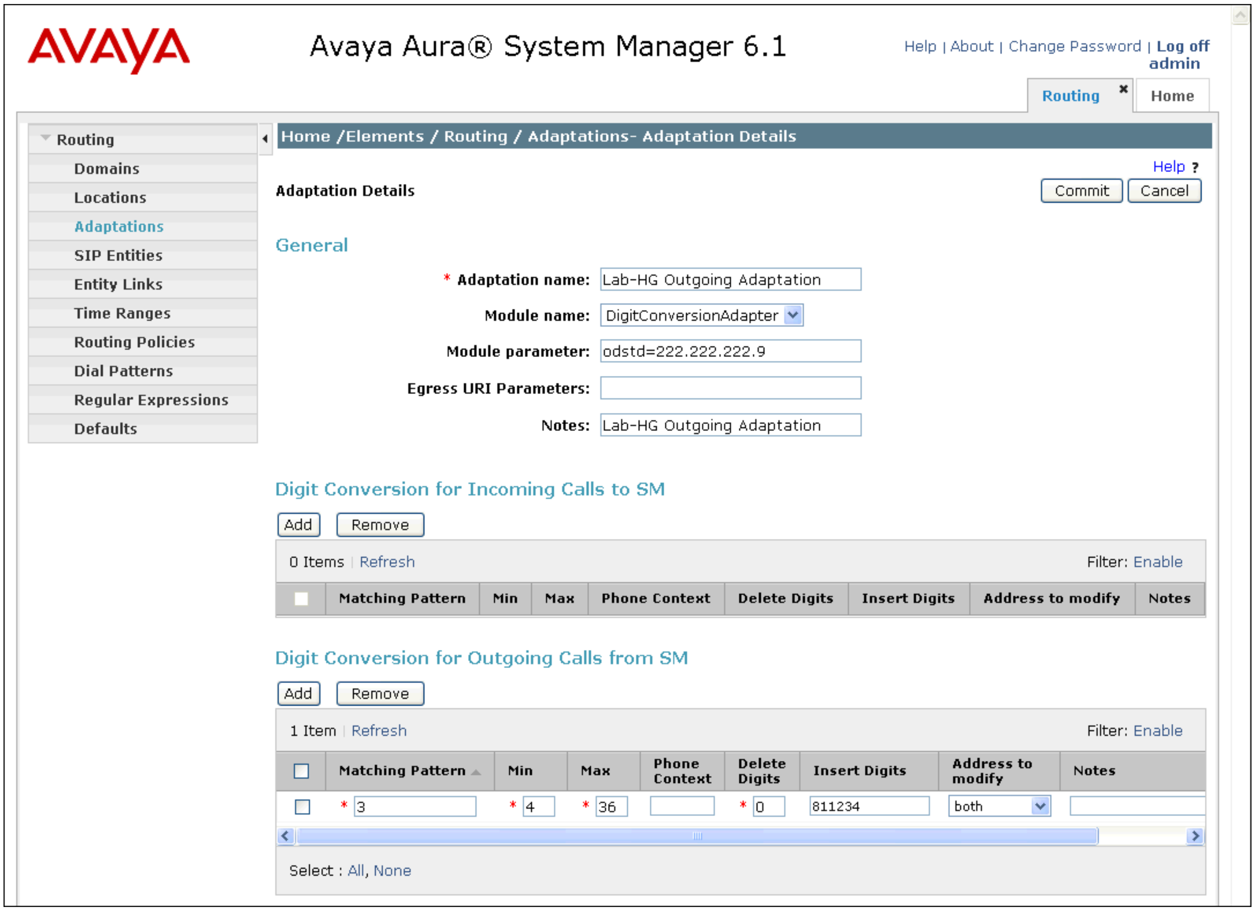
To prefix digits to Avaya Aura® Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for digits to be prefixed to the extension. Click **Add** and enter the following values. Use default values for all remaining fields:

- **Matching Pattern:** Enter a digit string used to match the extension number.
- **Min:** Enter a minimum digit length used in the match criteria.

- **Max:** Enter a maximum digit length used in the match criteria.
- **Delete Digits** Enter 0 since no digits are to be deleted.
- **Insert Digits:** Enter the number of digits to insert/append at the beginning of the received number.
- **Address to modify:** Select **both**.

Click **Commit** to save.

The **Lab-HG Outgoing adaptation** shown below will later be assigned to the **Lab-HG AA-SBC** Entity. This adaptation uses the **DigitConversionAdapter.**



Home /Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

General

* Adaptation name: Lab-HG Outgoing Adaptation

Module name: DigitConversionAdapter

Module parameter: odstd=222.222.222.9

Egress URI Parameters:

Notes: Lab-HG Outgoing Adaptation

Digit Conversion for Incoming Calls to SM

0 Items | Refresh Filter: Enable

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes

Digit Conversion for Outgoing Calls from SM

1 Item | Refresh Filter: Enable

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
□	* 3	* 4	* 36		* 0	811234	both	

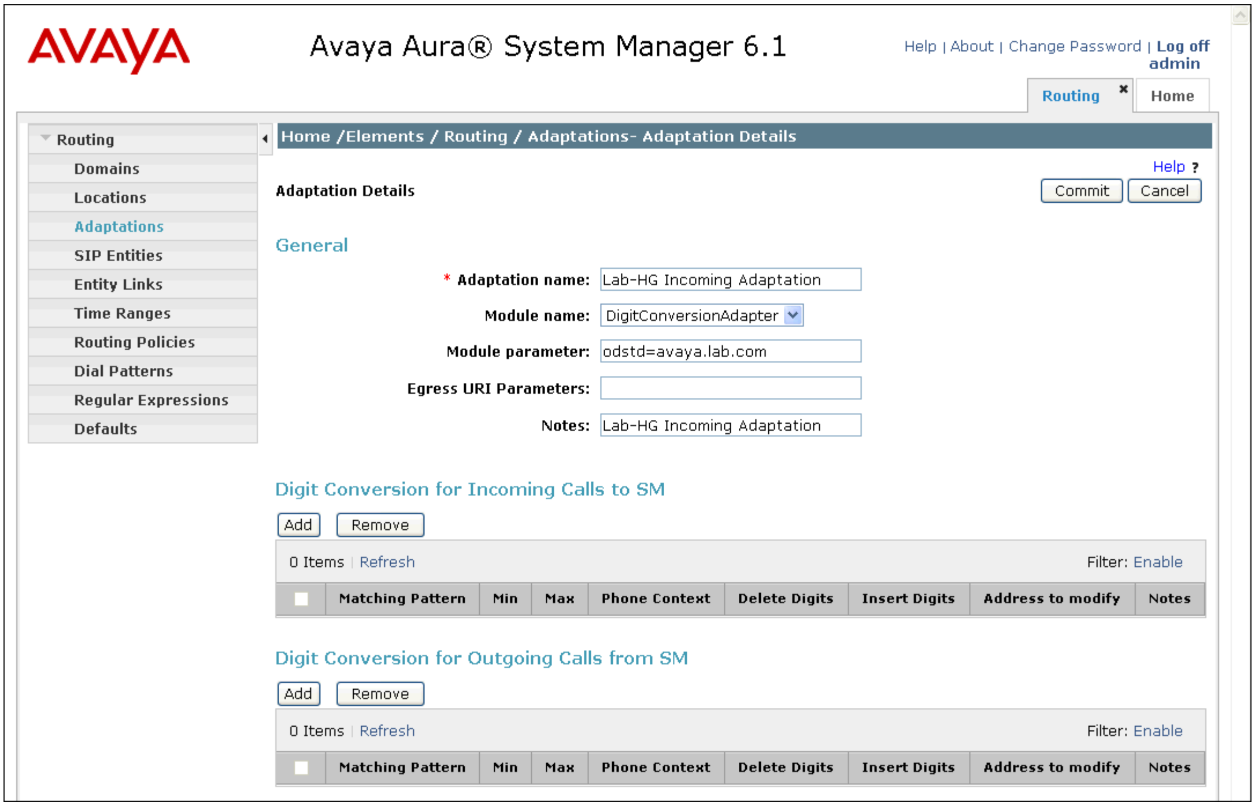
Select : All, None

The adaptation named **Lab-HG Incoming Adaptation** shown below will later be assigned to the SIP Entity for calls destined to Avaya Aura® Communication Manager. This adaptation uses the **DigitConversionAdapter** and specifies the **odstd=avaya.lab.com** parameter to adapt the domain to the domain expected by Avaya Aura® Communication Manager. More specifically, this configuration enables the destination IP to be overwritten with the domain **avaya.lab.com** for incoming calls destined to Avaya Aura® Communication Manager. For example, for inbound PSTN calls from Alestra to the Avaya CPE, the Request-URI header sent to Avaya Aura® Communication Manager will contain the domain **avaya.lab.com** as expected by Avaya Aura® Communication Manager.

Settings for **Lab-HG Incoming Adaptation:**

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **DigitConversionAdapter**.
- **Module parameter** Enter **odstd=enterprise domain name**



Adaptation Details

General

* Adaptation name:	Lab-HG Incoming Adaptation
Module name:	DigitConversionAdapter
Module parameter:	odstd=avaya.lab.com
Egress URI Parameters:	
Notes:	Lab-HG Incoming Adaptation

Digit Conversion for Incoming Calls to SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes

Digit Conversion for Outgoing Calls from SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes

6.5. Add SIP Entities

A SIP Entity must be added for Avaya Aura® Session Manager and for each SIP telephony system connected to it which includes Avaya Aura® Communication Manager and the Avaya Aura® SBC. Navigate to **Routing → SIP Entities** in the left-hand 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:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for Avaya Aura® 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.

To define the ports used by Avaya Aura® 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:

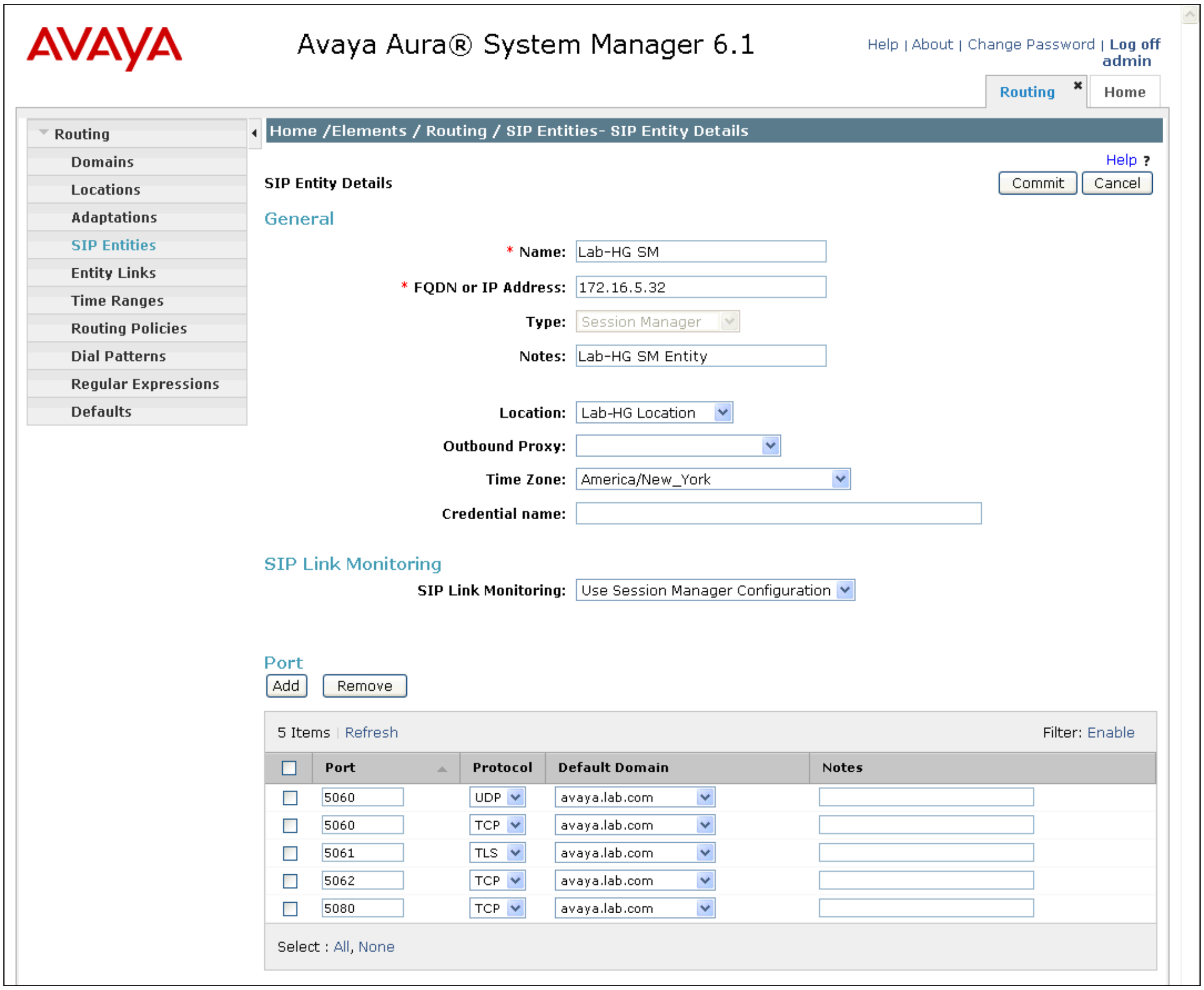
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

For the compliance test, only two Ports were used:

- **5060** with **TCP** for connecting to Avaya Aura® SBC
- **5080** with **TCP** for connecting to Avaya Aura® Communication Manager

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



Home /Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details

General

* Name:	Lab-HG SM
* FQDN or IP Address:	172.16.5.32
Type:	Session Manager
Notes:	Lab-HG SM Entity
Location:	Lab-HG Location
Outbound Proxy:	
Time Zone:	America/New_York
Credential name:	

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

Port

5 Items | Refresh   Filter: Enable

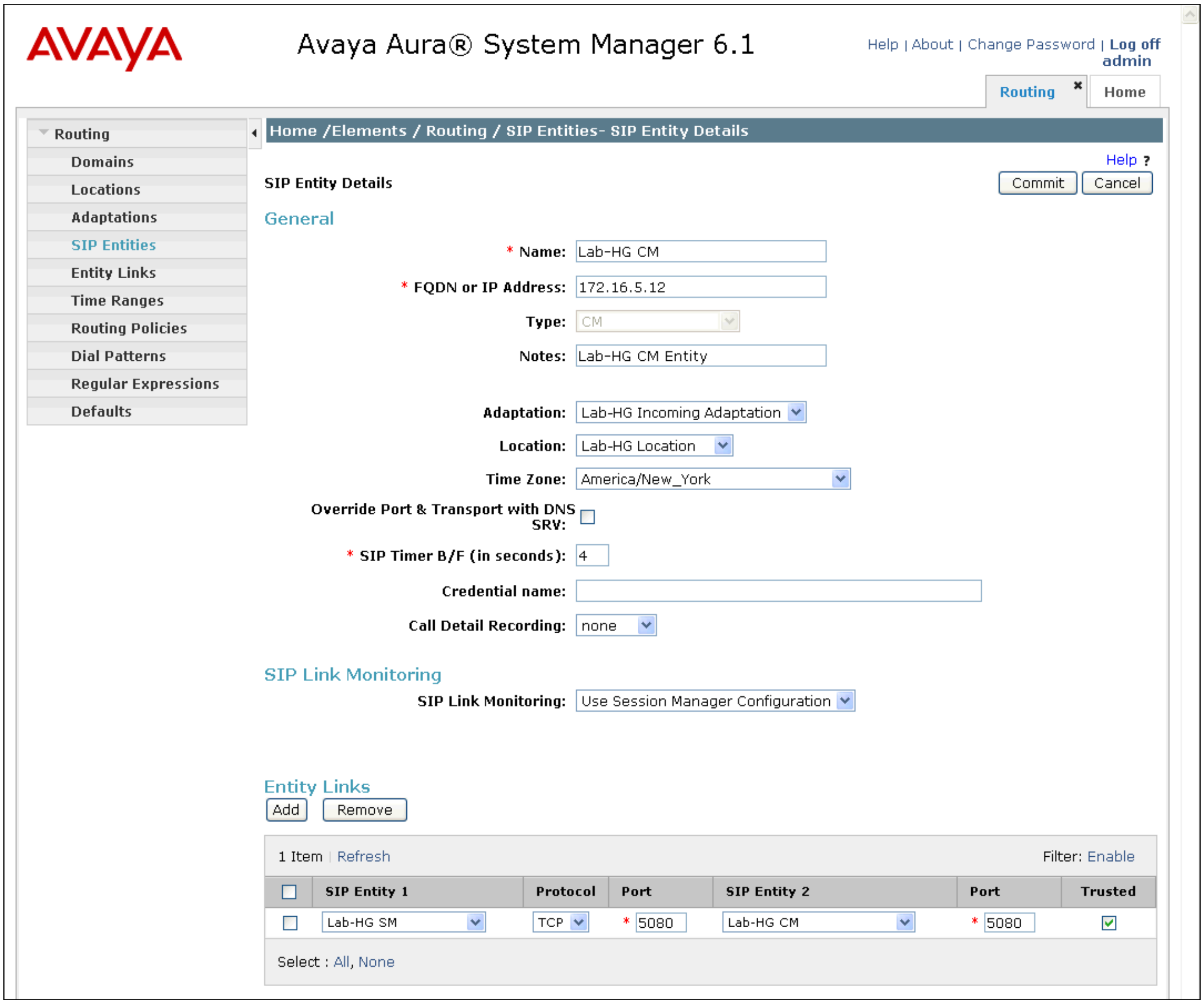
□	Port	Protocol	Default Domain	Notes
□	5060	UDP	avaya.lab.com	
□	5060	TCP	avaya.lab.com	
□	5061	TLS	avaya.lab.com	
□	5062	TCP	avaya.lab.com	
□	5080	TCP	avaya.lab.com	

Select : All, None

The following screen shows the addition of Avaya Aura® Communication Manager.

A separate SIP entity for Avaya Aura® Communication Manager, other than the one created for Avaya Aura® Session Manager connectivity during Installation, is required in order to send SIP service provider traffic.

The **FQDN or IP Address** field is set to the IP address of the Avaya S8300D Server running Avaya Aura® Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 6.4**.



SIP Entity Details

General

* Name: Lab-HG CM

* FQDN or IP Address: 172.16.5.12

Type: CM

Notes: Lab-HG CM Entity

Adaptation: Lab-HG Incoming Adaptation

Location: Lab-HG Location

Time Zone: America/New_York

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

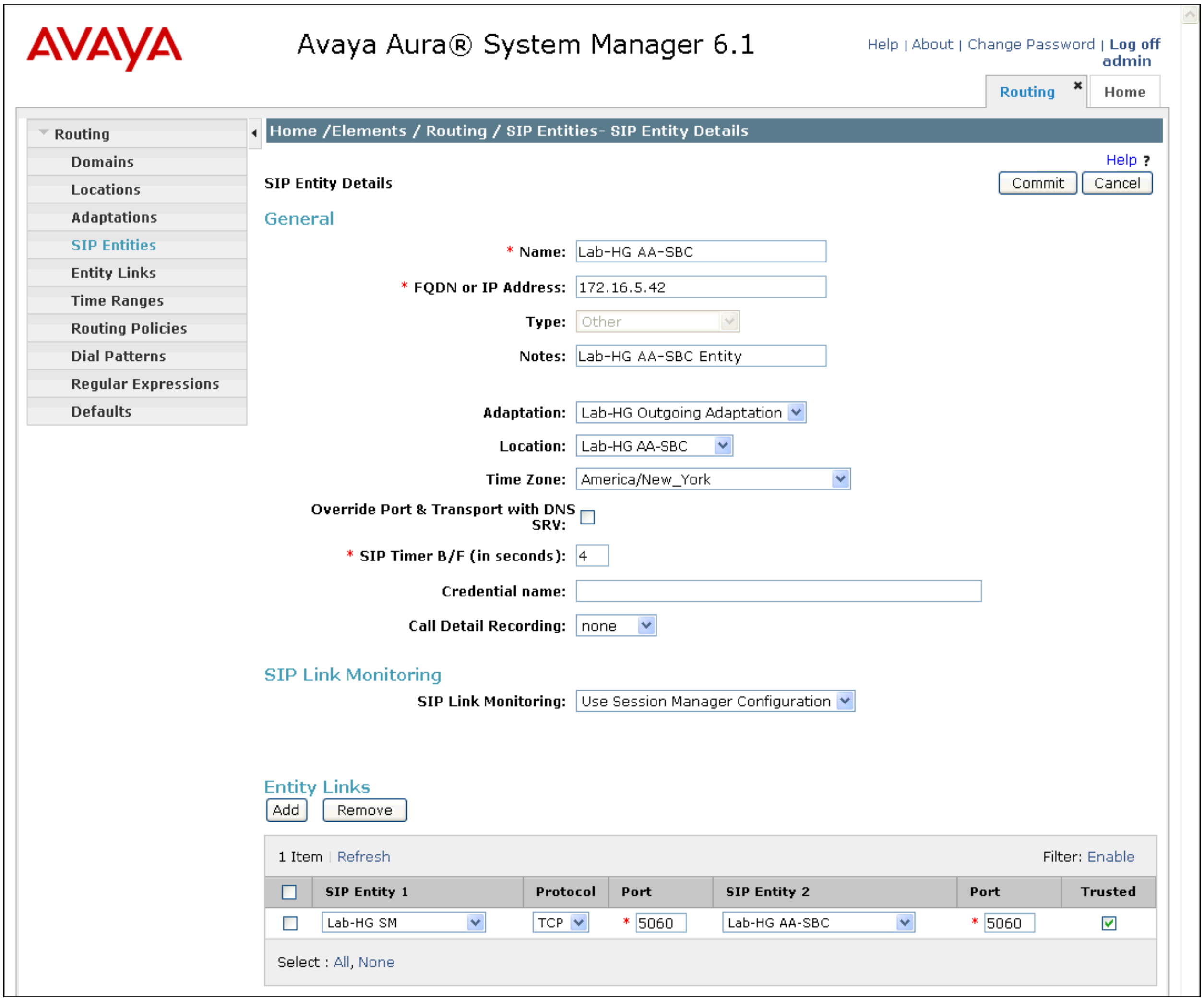
Entity Links

1 Item | Refresh Filter: Enable

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	Lab-HG SM	TCP	* 5080	Lab-HG CM	* 5080	☑

Select : All, None

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



Home /Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details

General

* Name:	Lab-HG AA-SBC
* FQDN or IP Address:	172.16.5.42
Type:	Other
Notes:	Lab-HG AA-SBC Entity
Adaptation:	Lab-HG Outgoing Adaptation
Location:	Lab-HG AA-SBC
Time Zone:	America/New_York
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

Entity Links

1 Item

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	Lab-HG SM	TCP	* 5060	Lab-HG AA-SBC	* 5060	☑

6.6. Add Entity Links

A SIP trunk between Avaya Aura® Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Avaya Aura® Communication Manager for use only by service provider traffic and one to the Avaya Aura® SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand 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:

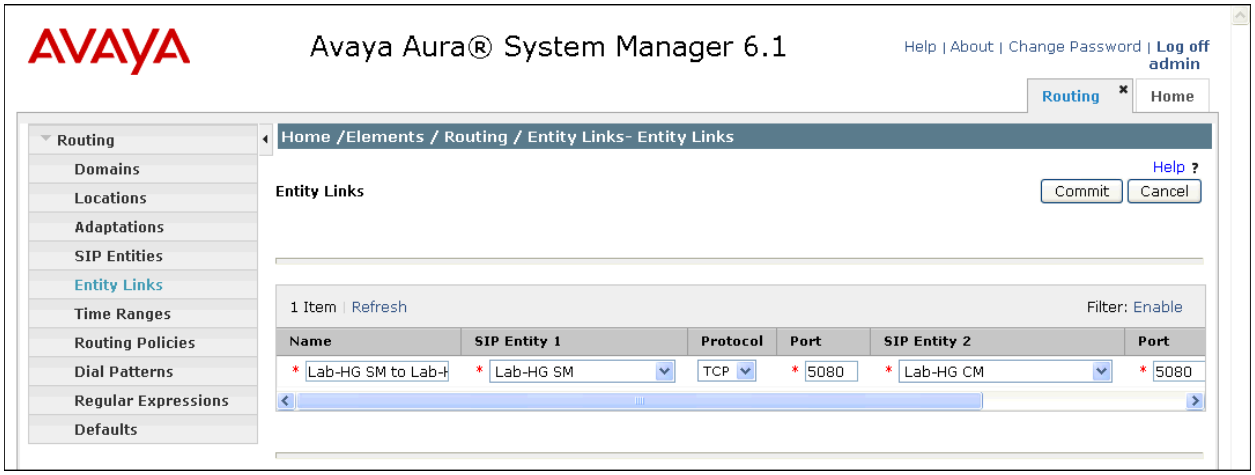
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Avaya Aura® Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager, this must match the

Far-end Listen Port defined on the Communication Manager signaling group in **Section 5.6**.

- **SIP Entity 2:** Select the name of the other system. For the Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **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 Avaya Aura® Communication Manager and the Avaya Aura® SBC. It should be noted that in a customer environment the Entity Link to Avaya Aura® Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Avaya Aura® Communication Manager signaling group form in **Section 5.6**

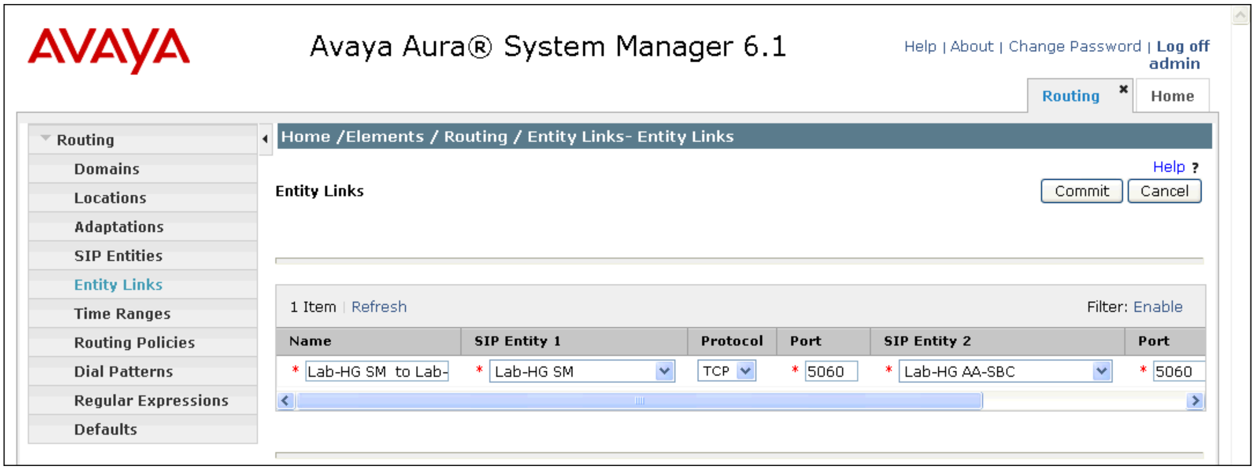
Entity Link to Avaya Aura® Communication Manager:



Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
* Lab-HG SM to Lab-H	* Lab-HG SM	TCP	* 5080	* Lab-HG CM	* 5080

Entity Link to the Avaya Aura® SBC:



Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
* Lab-HG SM to Lab-	* Lab-HG SM	TCP	* 5060	* Lab-HG AA-SBC	* 5060

6.7. Add Routing Policies

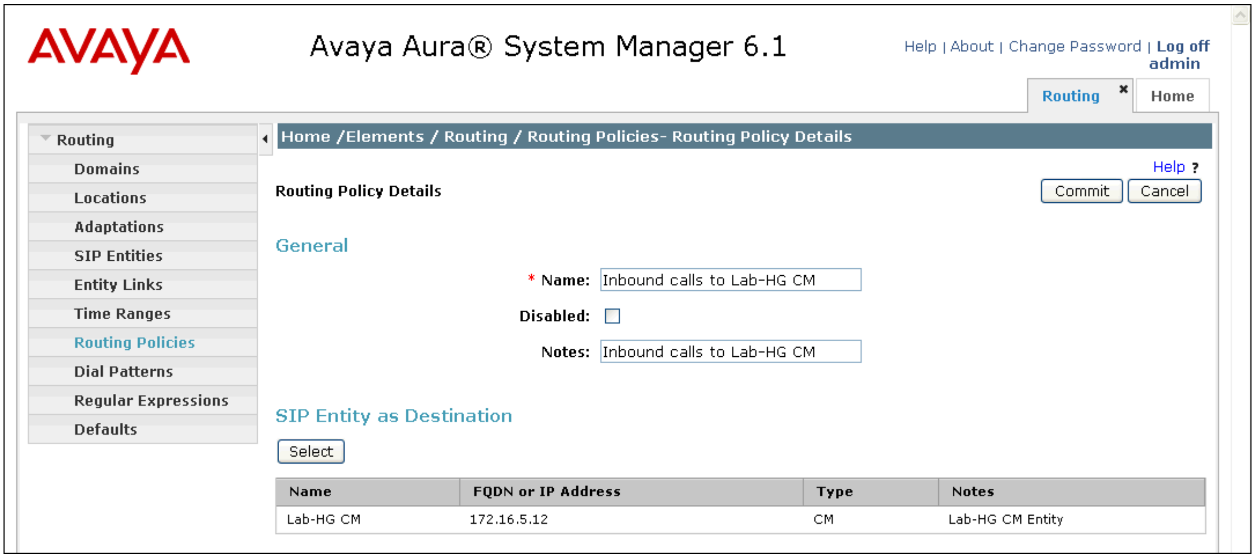
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Avaya Aura® Communication Manager and one for the Avaya Aura® SBC. To add a routing policy, navigate to **Routing → Routing Policies**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

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

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

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

The following screens show the Routing Policies for Avaya Aura® Communication Manager.



Home /Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

General

* Name: Inbound calls to Lab-HG CM

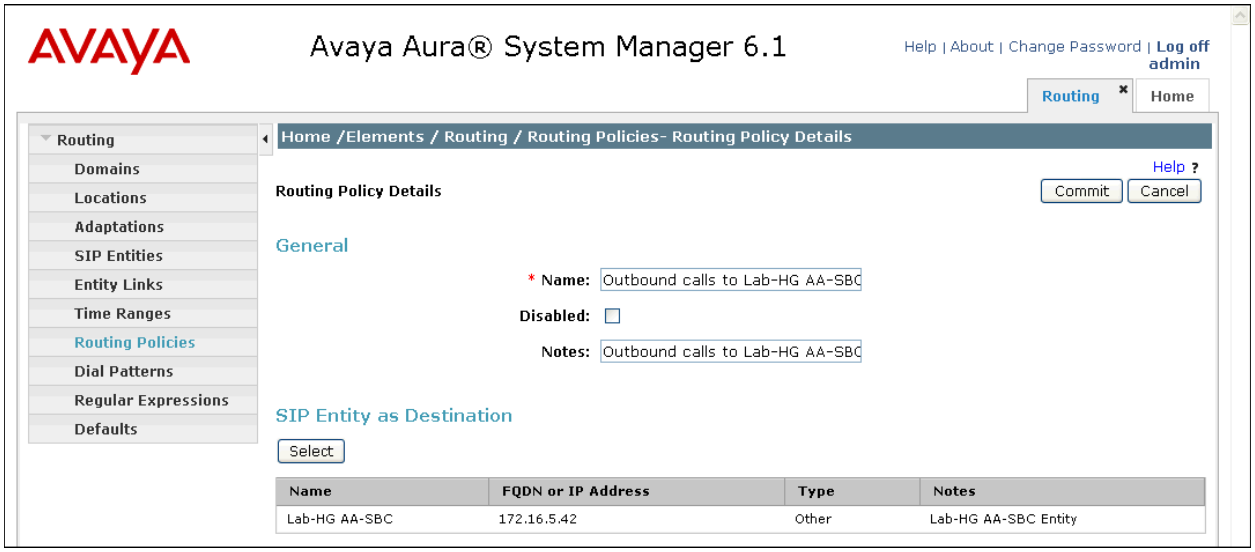
Disabled: □

Notes: Inbound calls to Lab-HG CM

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Lab-HG CM	172.16.5.12	CM	Lab-HG CM Entity

The following screens show the Routing Policies for the Avaya Aura® SBC.



Home /Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

General

* Name: Outbound calls to Lab-HG AA-SBC

Disabled: □

Notes: Outbound calls to Lab-HG AA-SBC

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Lab-HG AA-SBC	172.16.5.42	Other	Lab-HG AA-SBC Entity

6.8. Add Dial Patterns

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

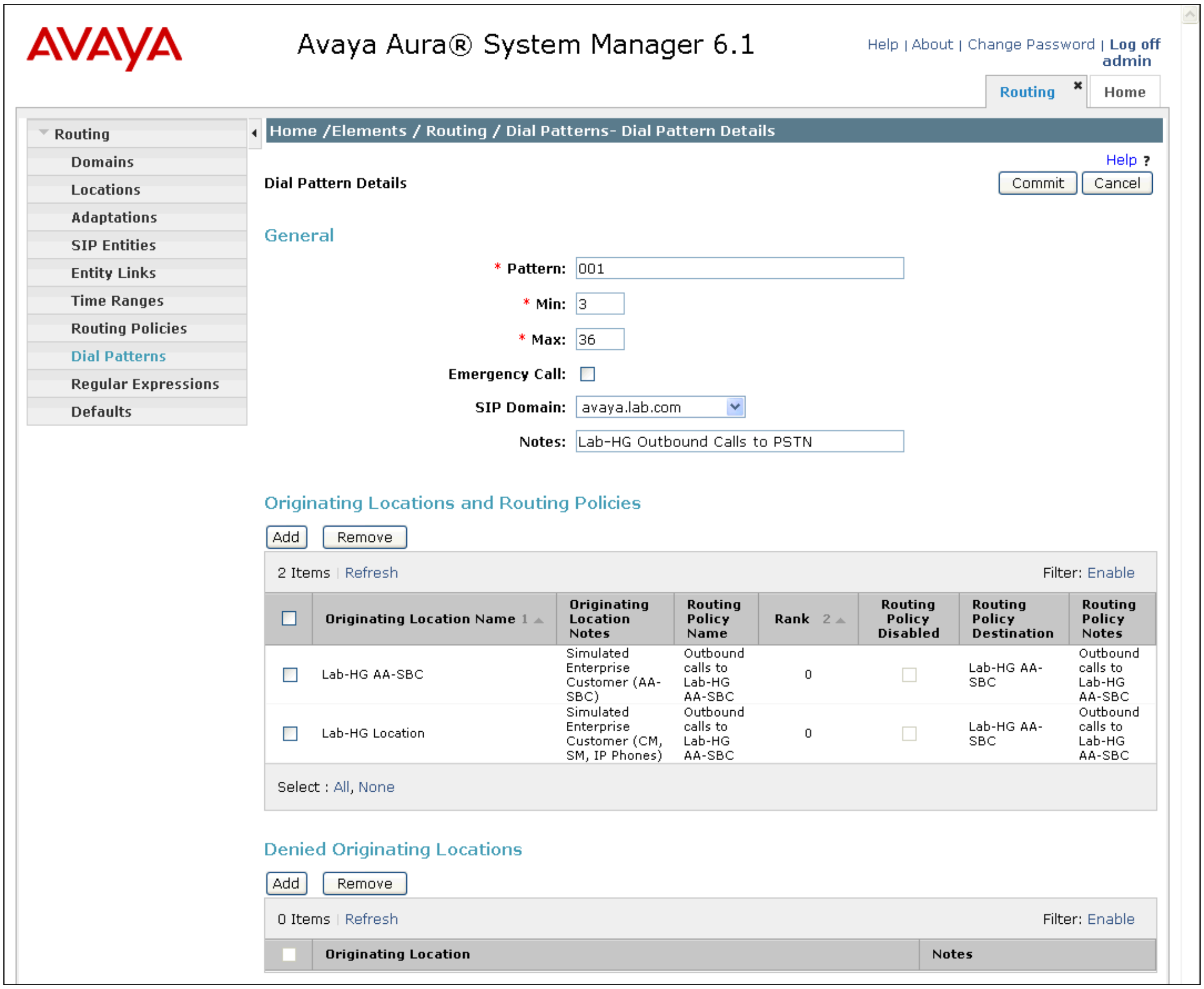
In the **General** section, enter the following values. Use default values for all remaining fields:

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

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

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

Examples of the dial patterns used for the compliance testing are shown below. The first example shows dial pattern **001** for International dialing from Mexico, have a destination domain of **avaya.lab.com** from **Locations Lab-HG AA-SBC** or **Lab-HG Location,** uses route policy **Lab-HG AA-SBC.**



Dial Pattern Details

General

* Pattern:	001
* Min:	3
* Max:	36
Emergency Call:	□
SIP Domain:	avaya.lab.com
Notes:	Lab-HG Outbound Calls to PSTN

Originating Locations and Routing Policies

Add Remove

2 Items | Refresh   Filter: Enable

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Lab-HG AA-SBC	Simulated Enterprise Customer (AA-SBC)	Outbound calls to Lab-HG AA-SBC	0	□	Lab-HG AA-SBC	Outbound calls to Lab-HG AA-SBC
□	Lab-HG Location	Simulated Enterprise Customer (CM, SM, IP Phones)	Outbound calls to Lab-HG AA-SBC	0	□	Lab-HG AA-SBC	Outbound calls to Lab-HG AA-SBC

Select : All, None

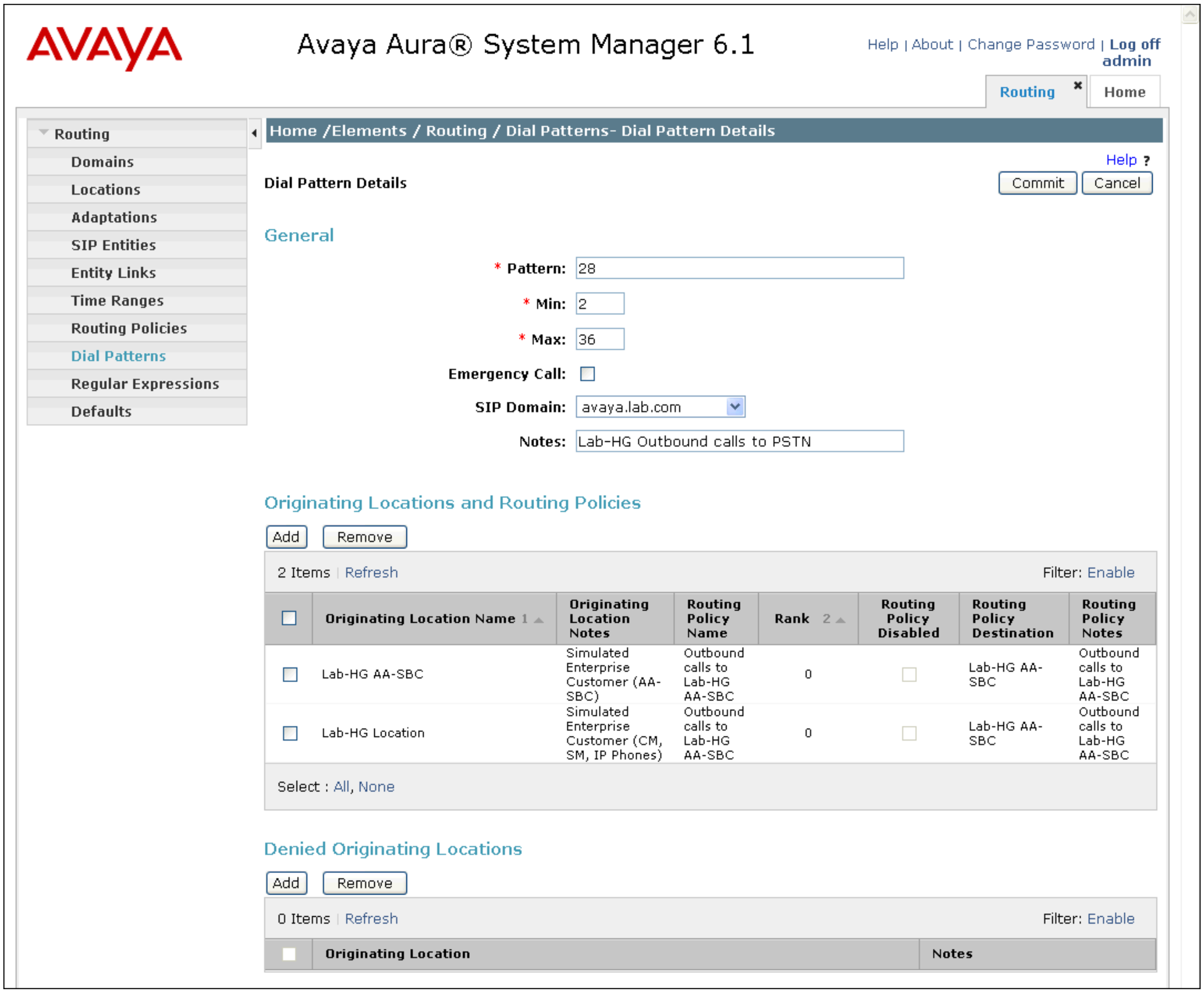
Denied Originating Locations

Add Remove

0 Items | Refresh   Filter: Enable

□	Originating Location	Notes

The following dial pattern example used for the compliance testing uses dial pattern **28** for local calling within Monterrey, Mexico, have a destination domain of **avaya.lab.com** from **Locations Lab-HG AA-SBC** or **Lab-HG Location,** uses route policy **Lab-HG AA-SBC.**



Dial Pattern Details

General

* Pattern: 28

* Min: 2

* Max: 36

Emergency Call: □

SIP Domain: avaya.lab.com

Notes: Lab-HG Outbound calls to PSTN

Originating Locations and Routing Policies

2 Items | Refresh — Filter: Enable

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Lab-HG AA-SBC	Simulated Enterprise Customer (AA-SBC)	Outbound calls to Lab-HG AA-SBC	0	□	Lab-HG AA-SBC	Outbound calls to Lab-HG AA-SBC
□	Lab-HG Location	Simulated Enterprise Customer (CM, SM, IP Phones)	Outbound calls to Lab-HG AA-SBC	0	□	Lab-HG AA-SBC	Outbound calls to Lab-HG AA-SBC

Select : All, None

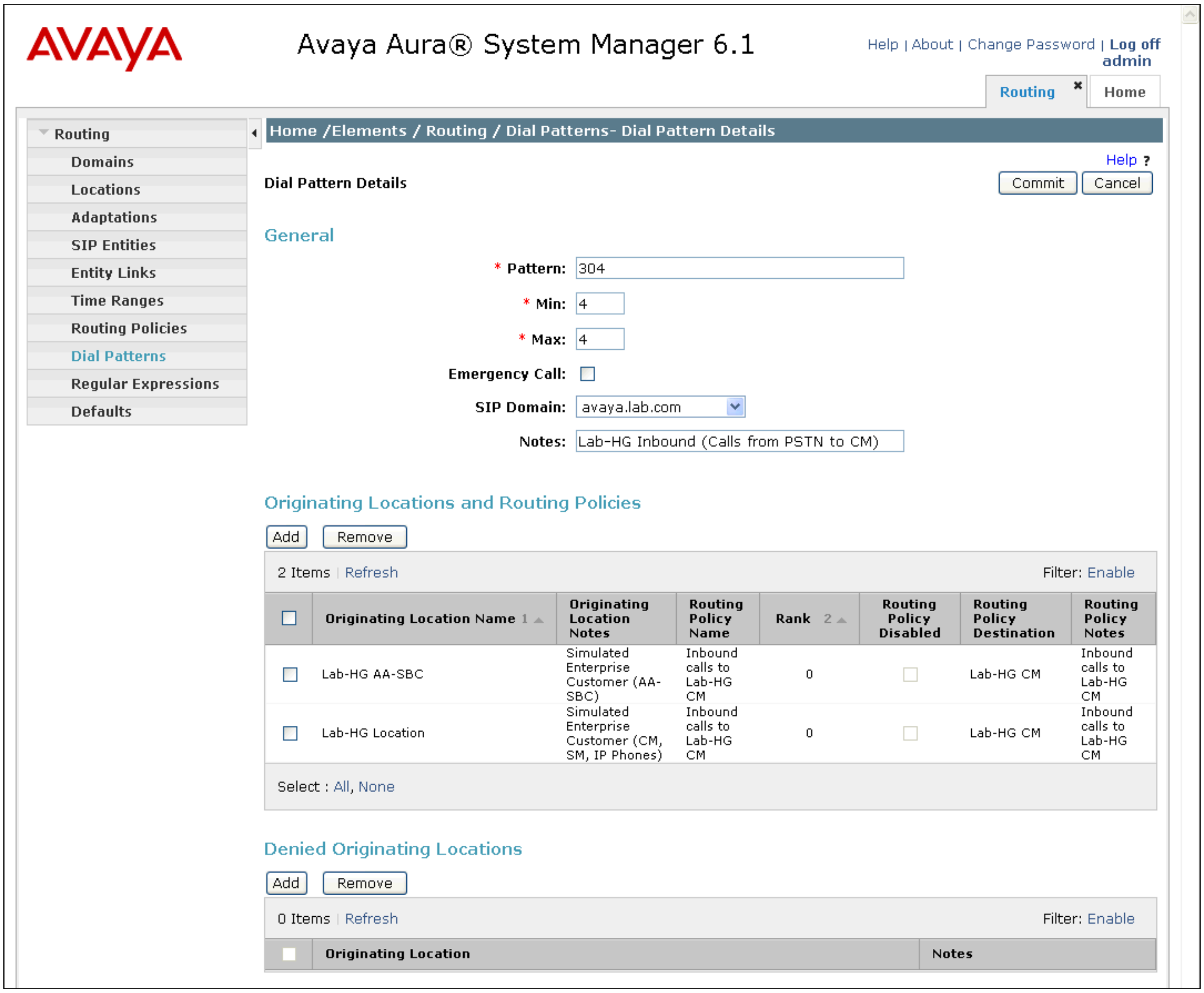
Denied Originating Locations

0 Items | Refresh — Filter: Enable

□	Originating Location	Notes

The following dial pattern example used for the compliance testing uses dial pattern **304**, these are the DID numbers assigned to the enterprise by Alestra. Have a destination domain of **avaya.lab.com** from **Locations Lab-HG AA-SBC** or **Lab-HG Location,** uses route policy **Lab-HG CM.**

Note that only the last 4 digits of the DID number were assigned; this is because in this sample configuration Alestra's network was configured to send only 4 digits to the enterprise (e.g., 3040, 3041, etc.)



Dial Pattern Details

General

* Pattern: 304

* Min: 4

* Max: 4

Emergency Call: □

SIP Domain: avaya.lab.com

Notes: Lab-HG Inbound (Calls from PSTN to CM)

Originating Locations and Routing Policies

2 Items | Refresh Filter: Enable

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Lab-HG AA-SBC	Simulated Enterprise Customer (AA-SBC)	Inbound calls to Lab-HG CM	0	□	Lab-HG CM	Inbound calls to Lab-HG CM
□	Lab-HG Location	Simulated Enterprise Customer (CM, SM, IP Phones)	Inbound calls to Lab-HG CM	0	□	Lab-HG CM	Inbound calls to Lab-HG CM

Select : All, None

Denied Originating Locations

0 Items | Refresh Filter: Enable

□	Originating Location	Notes

6.9. Add/View Avaya Aura® Session Manager

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

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

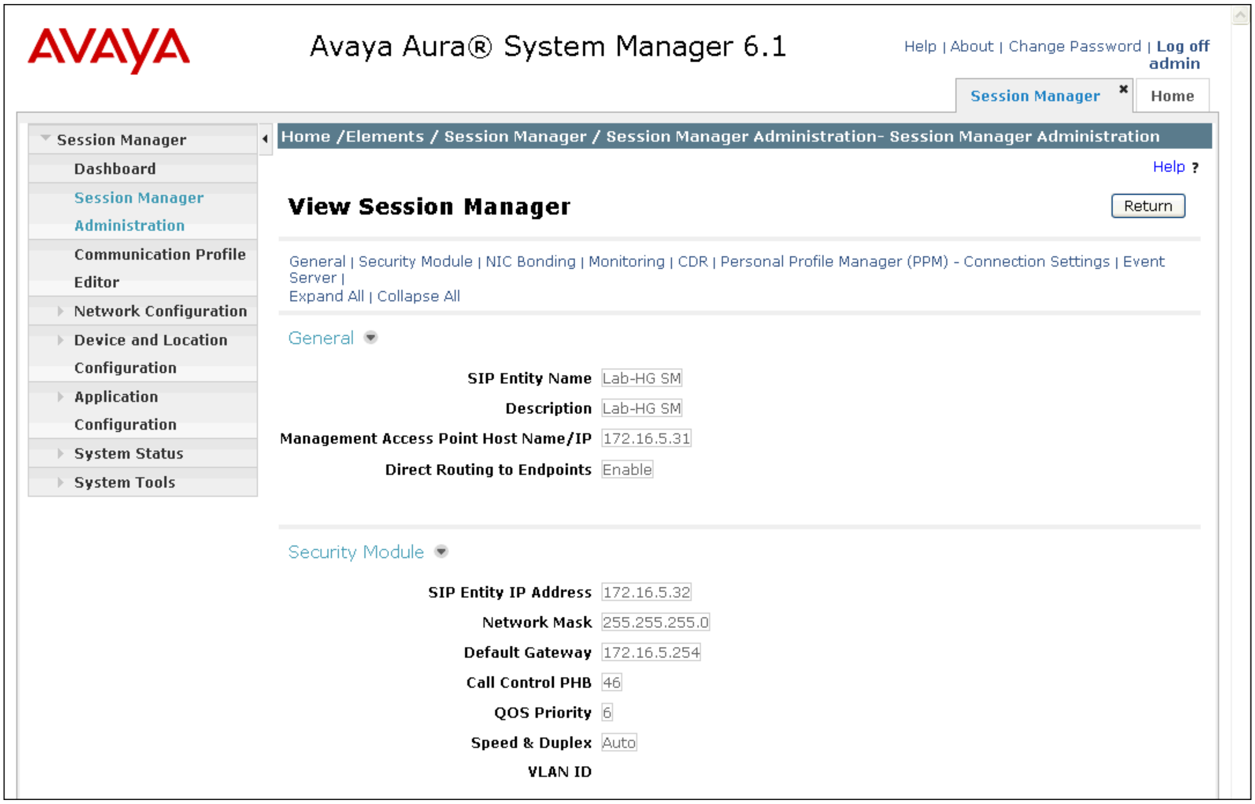
- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

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

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

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

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


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Home /Elements / Session Manager / Session Manager Administration- Session Manager Administration
Help ?
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

View Session Manager

General

SIP Entity Name	Lab-HG SM
Description	Lab-HG SM
Management Access Point Host Name/IP	172.16.5.31
Direct Routing to Endpoints	Enable

Security Module

SIP Entity IP Address	172.16.5.32
Network Mask	255.255.255.0
Default Gateway	172.16.5.254
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

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® SBC installation via the installation wizard. These Application Notes will not cover the Avaya Aura® SBC installation in its entirety but will include the use of the installation wizard. For information on installing the Avaya Aura® System Platform and the loading of the Avaya Aura® Avaya Aura® SBC template see [1].

The second part of the configuration is done after the installation is complete using the Avaya Aura® SBC web interface. The resulting Avaya Aura® SBC configuration file is shown in **Appendix A**.

7.1. Installation Wizard

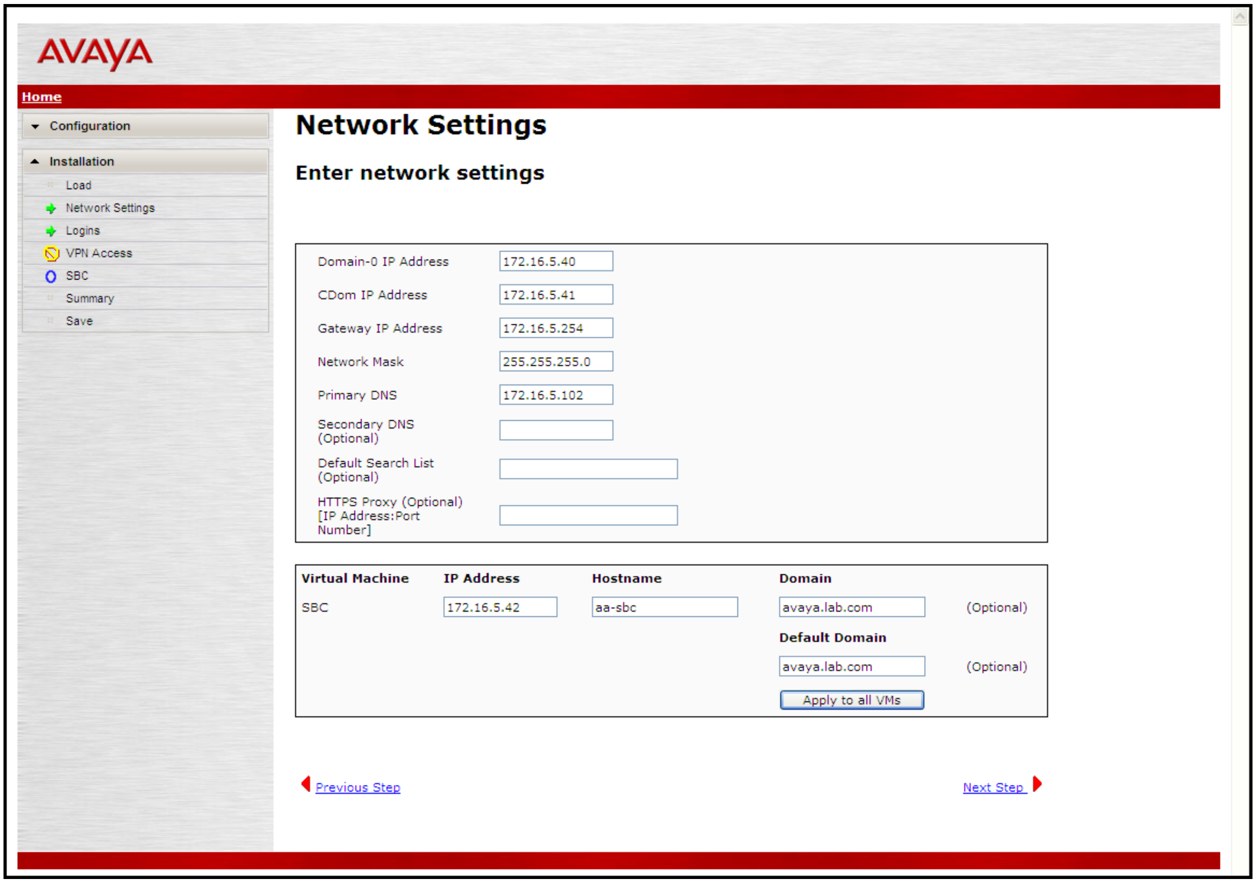
During the installation of the Avaya Aura® SBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the Avaya Aura® SBC.

7.1.1. Network Settings

The first screen of the installation wizard is the **Network Settings** screen. Fill in the fields as described below and shown in the following screen:

- **IP Address**: Enter the IP address of the private side of the Avaya Aura® SBC.
- **Hostname**: Enter a host name for the Avaya Aura® SBC.
- **Domain**: Enter the domain used for the enterprise.
- **Default Domain**: Enter the domain used for the enterprise.

Click **Next Step** (not shown) to continue.



Network Settings

Enter network settings

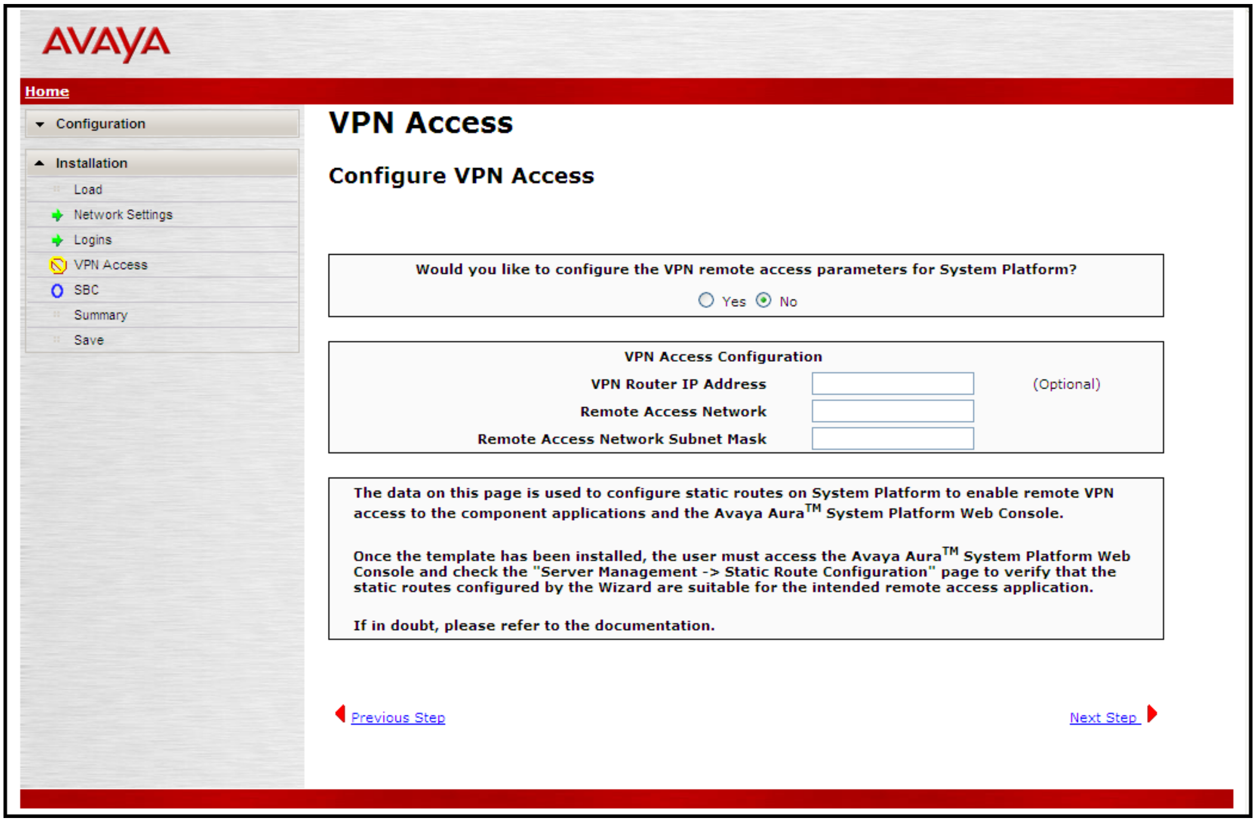
Domain-0 IP Address	172.16.5.40
CDom IP Address	172.16.5.41
Gateway IP Address	172.16.5.254
Network Mask	255.255.255.0
Primary DNS	172.16.5.102
Secondary DNS (Optional)	
Default Search List (Optional)	
HTTPS Proxy (Optional) [IP Address:Port Number]	

Virtual Machine	IP Address	Hostname	Domain	
SBC	172.16.5.42	aa-sbc	avaya.lab.com	(Optional)
			Default Domain	
			avaya.lab.com	(Optional)

7.1.2. VPN Access

VPN remote access to the Avaya Aura® SBC was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?**

Click **Next Step** to continue.



VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

○ Yes ● No

VPN Access Configuration

VPN Router IP Address		(Optional)
Remote Access Network		
Remote Access Network Subnet Mask		

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

7.1.3. SBC

On the **SBC** screen, fill in the fields as described below and shown in the following screen:

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 Alestra. Thus, **Generic** was chosen instead and further customization was done manually after the wizard was completed.
- **Port**: Enter the port number that the service provider uses to listen for SIP traffic.
- **IP Address**: Enter the SIP proxy IP address provided by Alestra. If the service provider has multiple proxies, enter the primary proxy on this screen, additional proxies can be added after installation.
- **Media Network**: Enter the subnet mask provided by Alestra where media traffic will Originate. If media can originate from multiple networks, enter one network address on this screen and additional networks can be added after installation.
- **Media Netmask**: Enter the netmask corresponding to the **Media Network**.

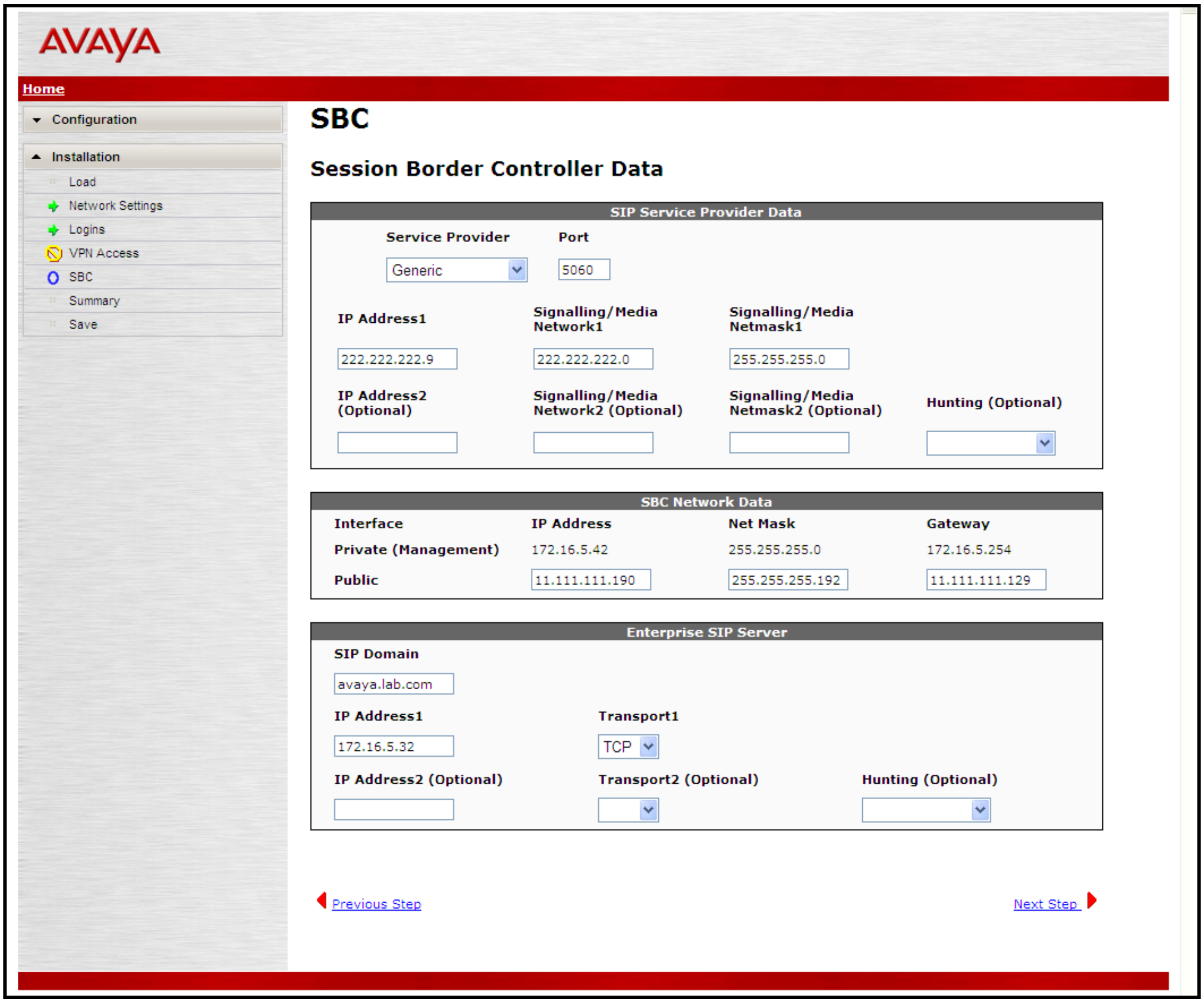
Further down on the same **SBC** screen, fill in the fields as described below:

In the **SBC Network Data** section:

- **Public IP Address**: Enter the IP address of the public side of the Avaya Aura® SBC.
- **Public Net Mask**: Enter the netmask associated with the public network to which the Avaya Aura® SBC connects.
- **Public Gateway**: Enter the default gateway of the public network.

In the **Enterprise SIP Server** section:

- **IP Address**: 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.
- **Transport**: From the pull-down menu, select the transport protocol to be used for SIP traffic between the Avaya Aura® SBC and Session Manager.
- **SIP Domain** Enter the enterprise SIP domain.



SBC

Session Border Controller Data

SIP Service Provider Data

Service Provider	Port		
Generic	5060		
IP Address1	**Signalling/Media Network1**	**Signalling/Media Netmask1**	
222.222.222.9	222.222.222.0	255.255.255.0	
IP Address2 (Optional)	**Signalling/Media Network2 (Optional)**	**Signalling/Media Netmask2 (Optional)**	**Hunting (Optional)**

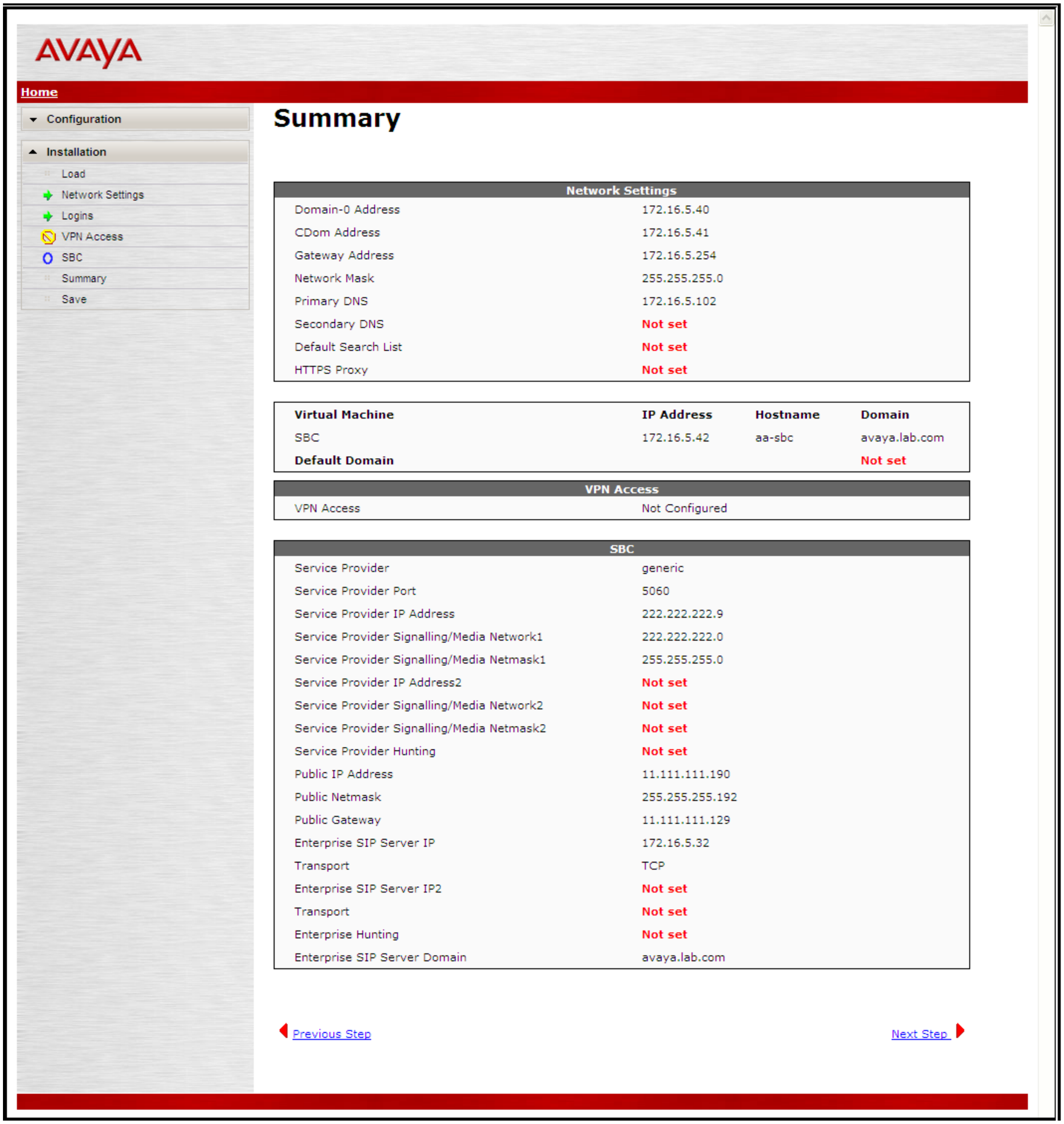
SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	172.16.5.42	255.255.255.0	172.16.5.254
Public	11.111.111.190	255.255.255.192	11.111.111.129

Enterprise SIP Server

SIP Domain		
avaya.lab.com		
IP Address1	**Transport1**	
172.16.5.32	TCP	
IP Address2 (Optional)	**Transport2 (Optional)**	**Hunting (Optional)**

Click **Next Step** to continue. The following summary screen will be displayed. Check the displayed values and click **Next Step** again to continue to the final step.



Summary

Network Settings	
Domain-0 Address	172.16.5.40
CDom Address	172.16.5.41
Gateway Address	172.16.5.254
Network Mask	255.255.255.0
Primary DNS	172.16.5.102
Secondary DNS	Not set
Default Search List	Not set
HTTPS Proxy	Not set

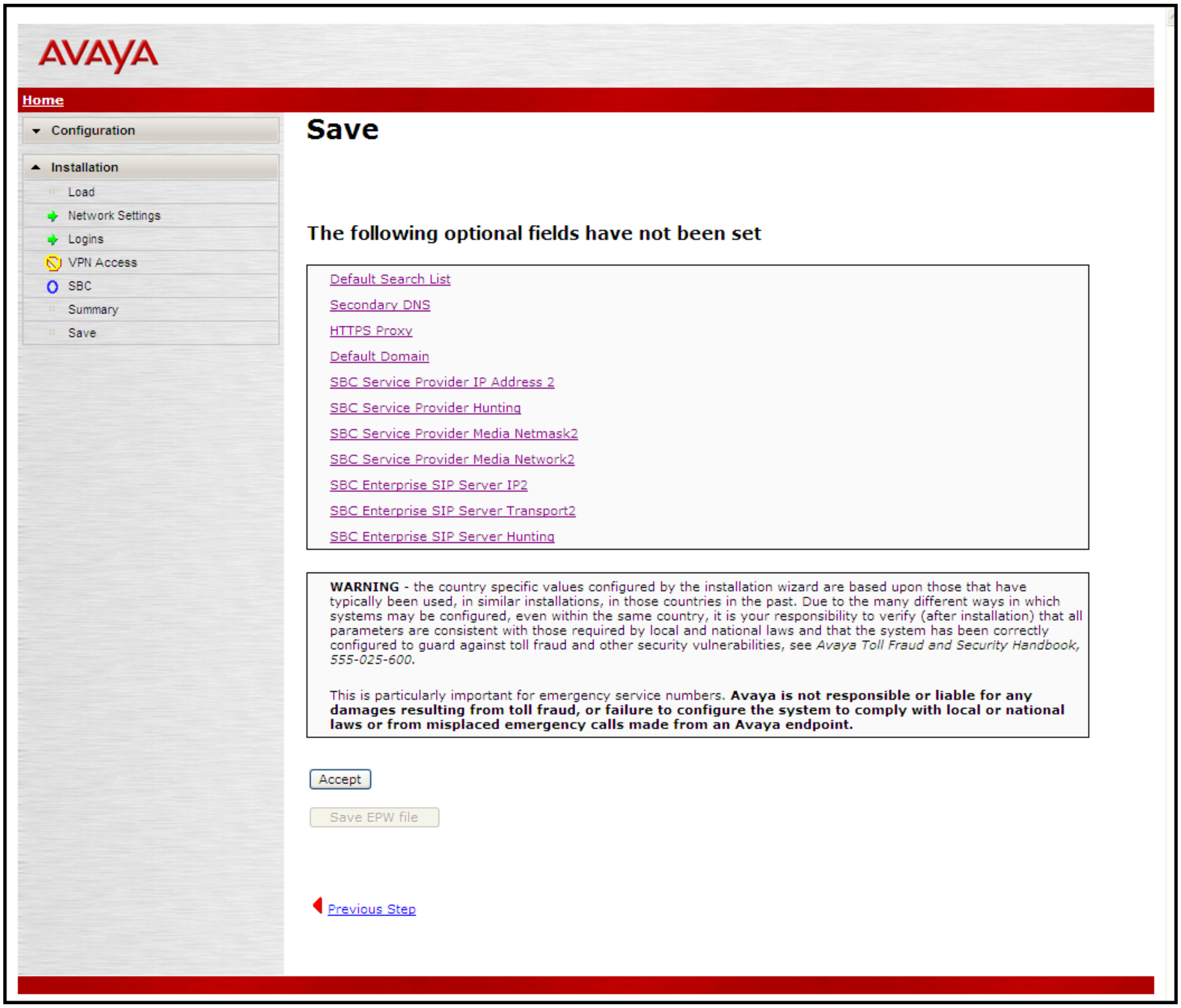
Virtual Machine	IP Address	Hostname	Domain
SBC	172.16.5.42	aa-sbc	avaya.lab.com
Default Domain			Not set

VPN Access	
VPN Access	Not Configured

SBC	
Service Provider	generic
Service Provider Port	5060
Service Provider IP Address	222.222.222.9
Service Provider Signalling/Media Network1	222.222.222.0
Service Provider Signalling/Media Netmask1	255.255.255.0
Service Provider IP Address2	Not set
Service Provider Signalling/Media Network2	Not set
Service Provider Signalling/Media Netmask2	Not set
Service Provider Hunting	Not set
Public IP Address	11.111.111.190
Public Netmask	255.255.255.192
Public Gateway	11.111.111.129
Enterprise SIP Server IP	172.16.5.32
Transport	TCP
Enterprise SIP Server IP2	Not set
Transport	Not set
Enterprise Hunting	Not set
Enterprise SIP Server Domain	avaya.lab.com

7.1.4. Confirm Installation

The **Confirm Installation** screen will indicate if any required or optional fields have not been set. The list of required fields that have not been set should be empty. If not, click **Previous Step** to navigate to the necessary screen to set the required field. Otherwise, click **Accept** to finish the wizard and to continue the overall template installation.



Save

The following optional fields have not been set

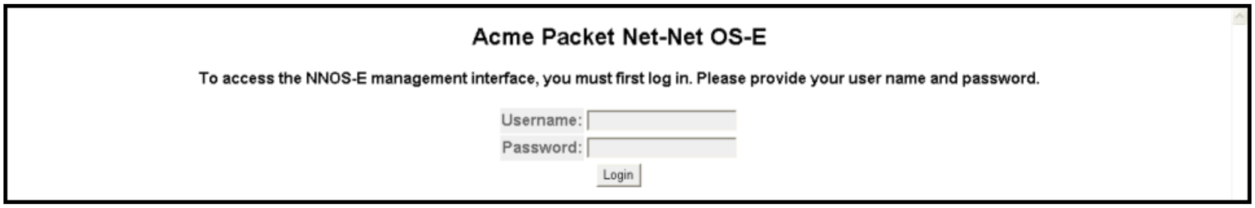
- Default Search List
- Secondary DNS
- HTTPS Proxy
- Default Domain
- SBC Service Provider IP Address 2
- SBC Service Provider Hunting
- SBC Service Provider Media Netmask2
- SBC Service Provider Media Network2
- SBC Enterprise SIP Server IP2
- SBC Enterprise SIP Server Transport2
- SBC Enterprise SIP Server Hunting

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook, 555-025-600.*

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

7.2. Post Installation Configuration

The installation wizard configures the Avaya Aura® Session Border Controller for use with the service provider chosen in **Section 7.1**. Since a different service provider other than Alestra had to be selected in the installation wizard then additional manual changes must also be performed. These changes are performed by accessing the browser-based GUI of the Avaya Aura® Session Border Controller, using the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 7.1**. Log in with proper credentials.



Acme Packet Net-Net OS-E

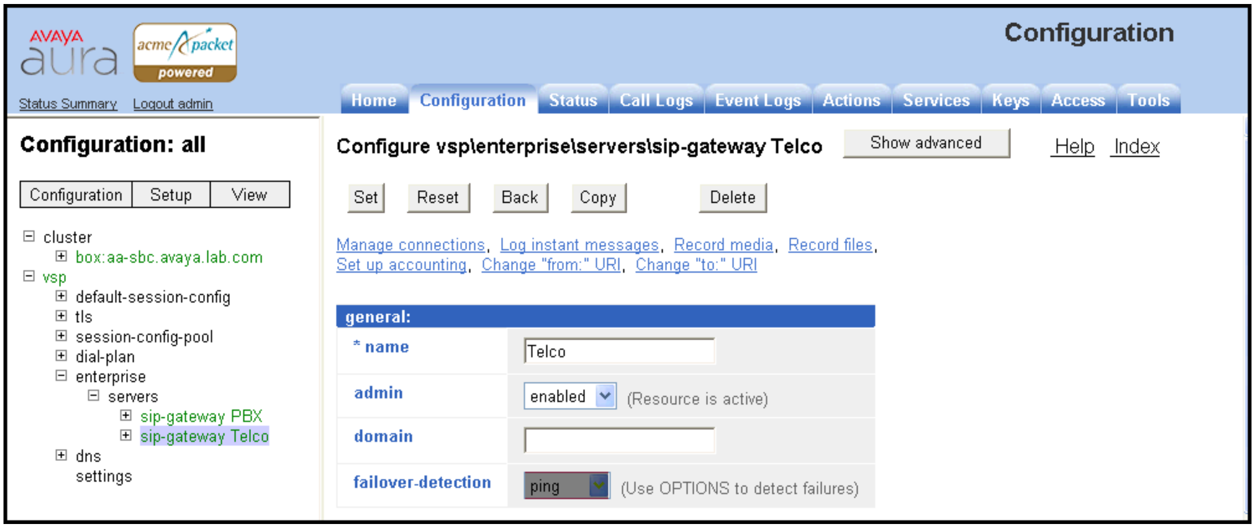
To access the NNOS-E management interface, you must first log in. Please provide your user name and password.

Username:

Password:

7.2.1. Options Frequency

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



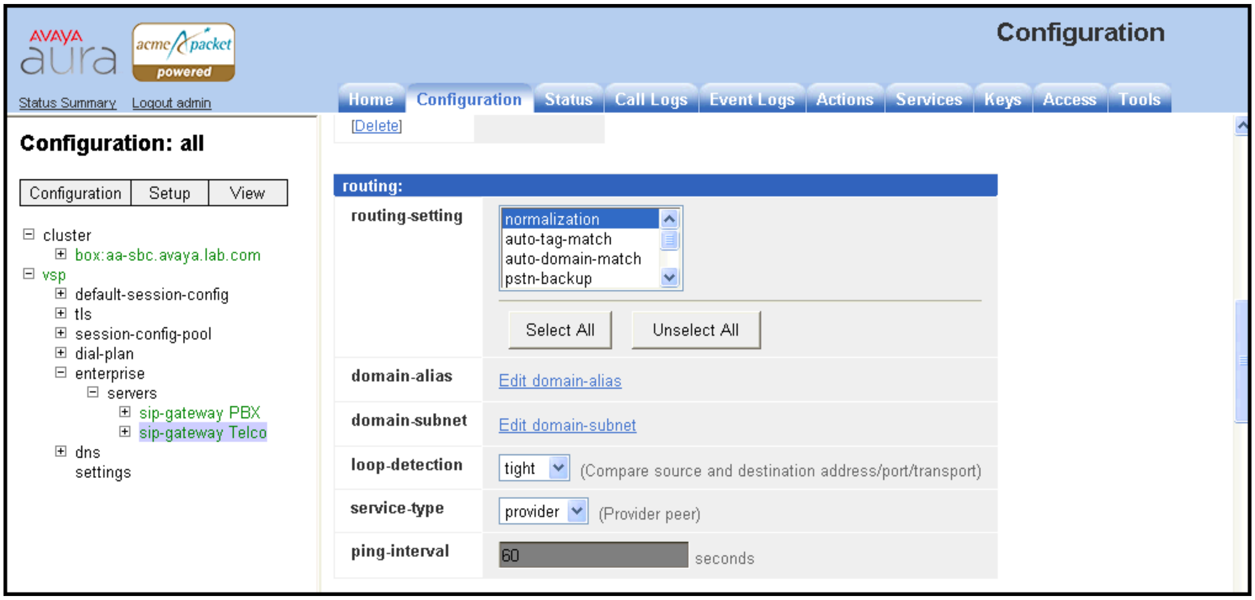
Configuration: all

- cluster
  - box:aa-sbc.avaya.lab.com
- vsp
  - default-session-config
  - tls
  - session-config-pool
  - dial-plan
  - enterprise
    - servers
      - sip-gateway PBX
      - sip-gateway Telco
  - dns
  - settings

Configure vsp\enterprise\servers\sip-gateway Telco

general:	
* name	Telco
admin	enabled (Resource is active)
domain	
failover-detection	ping (Use OPTIONS to detect failures)

Scroll down to the **routing** section of the form. Enter the desired interval in the **ping-interval** field. Click **Set** at the top of the form (shown in previous figure).



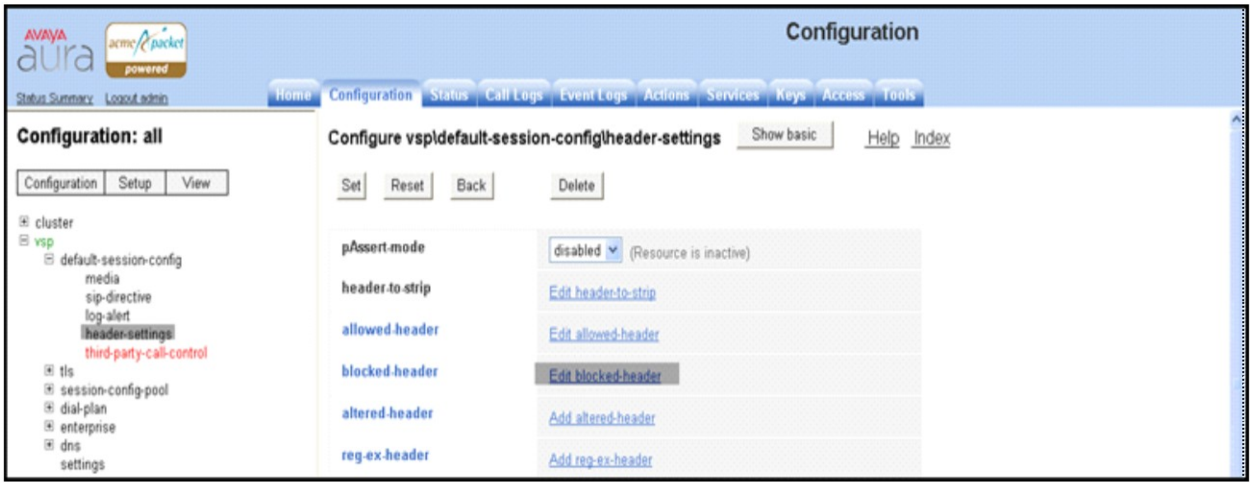
routing:

routing-setting	normalization auto-tag-match auto-domain-match pstn-backup
domain-alias	Edit domain-alias
domain-subnet	Edit domain-subnet
loop-detection	tight (Compare source and destination address/port/transport)
service-type	provider (Provider peer)
ping-interval	60 seconds

Similar procedures can be used to set the Options Frequency from Avaya Aura® SBC to Avaya Aura® Session Manager in **vsp →enterprise →servers →sig-gateway PBX**.

7.2.2. Blocked Headers

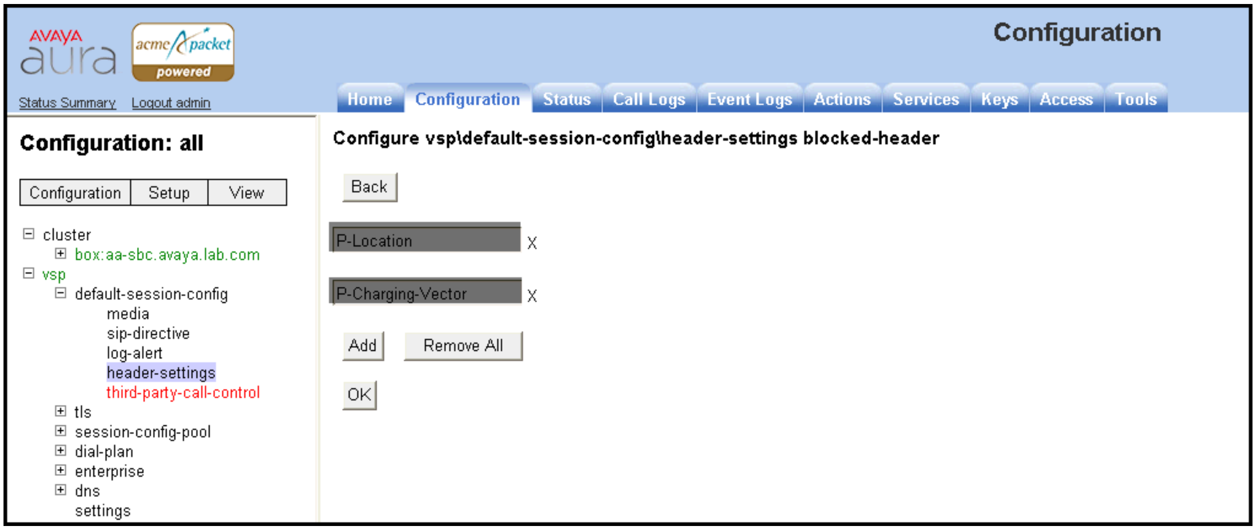
The P-Location and P-Charging-Vector headers are sent in SIP messages from the Avaya Aura® Session Manager. These headers should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both requests and responses for both inbound and outbound calls. To create a rule for blocking a header on an outbound call, first navigate to **vsp →default-session-config → header-settings**. Click **Edit blocked-header**.



Configure vsp\default-session-config\header-settings

pAssert-mode	disabled (Resource is inactive)
header-to-strip	Edit header-to-strip
allowed-header	Edit allowed-header
blocked-header	Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header

In the right pane, click **Add.** In the blank field that appears, 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** header and the **P-Charging-Vector** header were configured to be blocked for the compliance test. Click **OK** to continue.

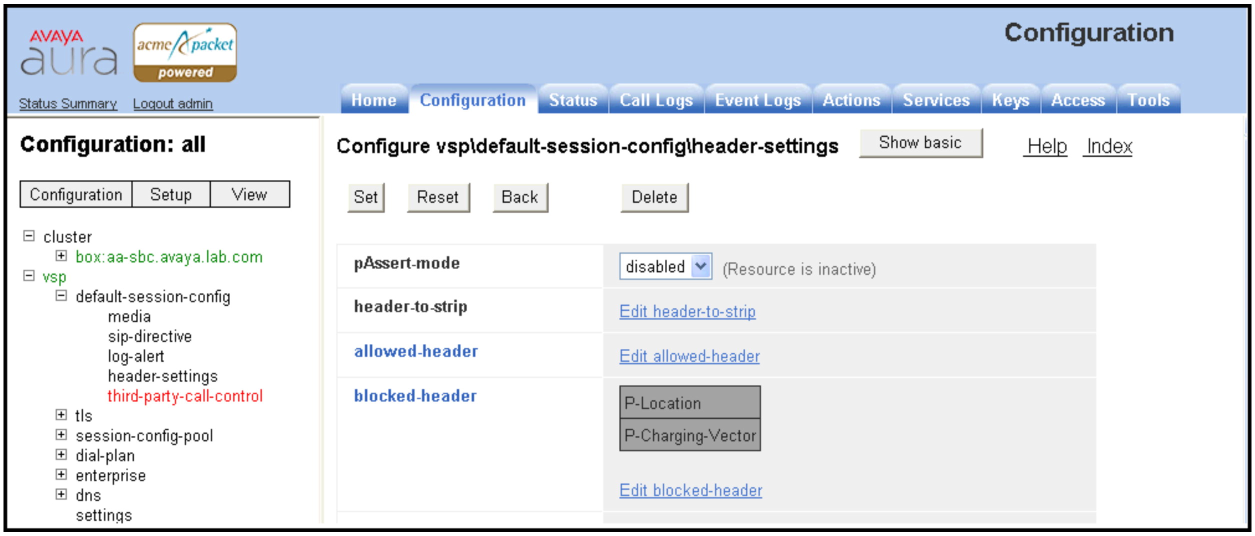


Configure vsp\default-session-config\header-settings blocked-header

P-Location X

P-Charging-Vector X

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

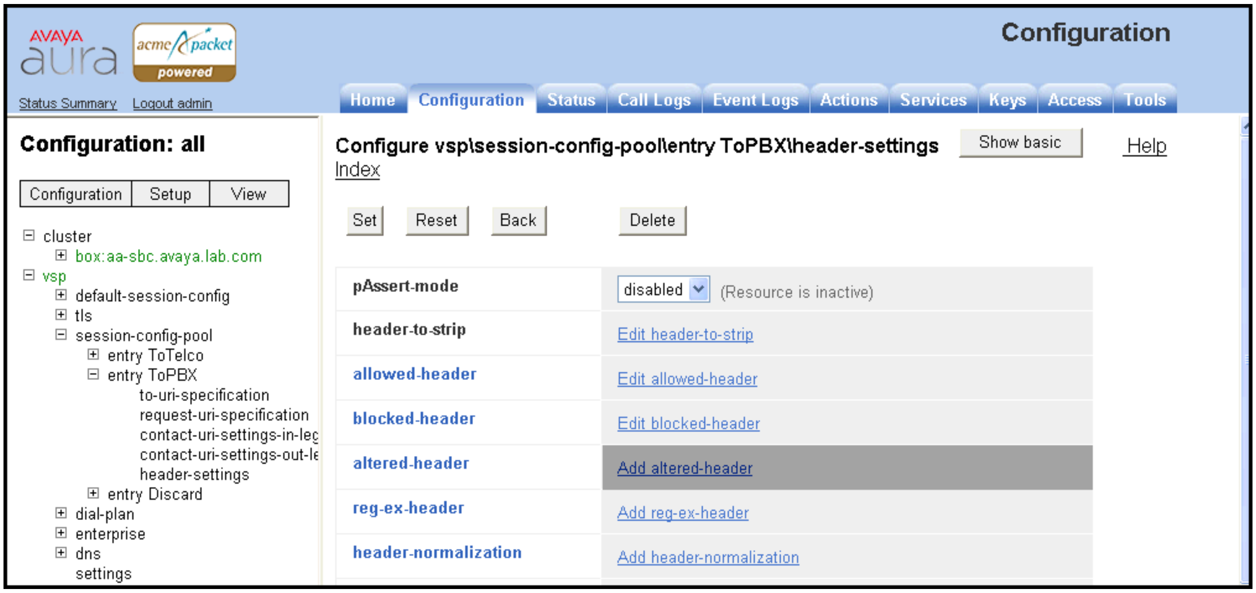


Configure vsp\default-session-config\header-settings

pAssert-mode	disabled (Resource is inactive)
header-to-strip	Edit header-to-strip
allowed-header	Edit allowed-header
blocked-header	P-Location P-Charging-Vector Edit blocked-header

7.2.3. Max-Forwards Value

On incoming PSTN calls to an enterprise SIP phone, the Max-Forwards value in the incoming SIP INVITE is too small to allow the message to traverse all the SIP hops internal to the enterprise to reach the SIP phone. Thus, the Avaya Aura® SBC was used to increase this value when the INVITE arrived at the Avaya Aura® SBC from the network. To do this, navigate to **vsp → session-config-pool → entry ToPBX → header-settings** and click **Add altered-header**.



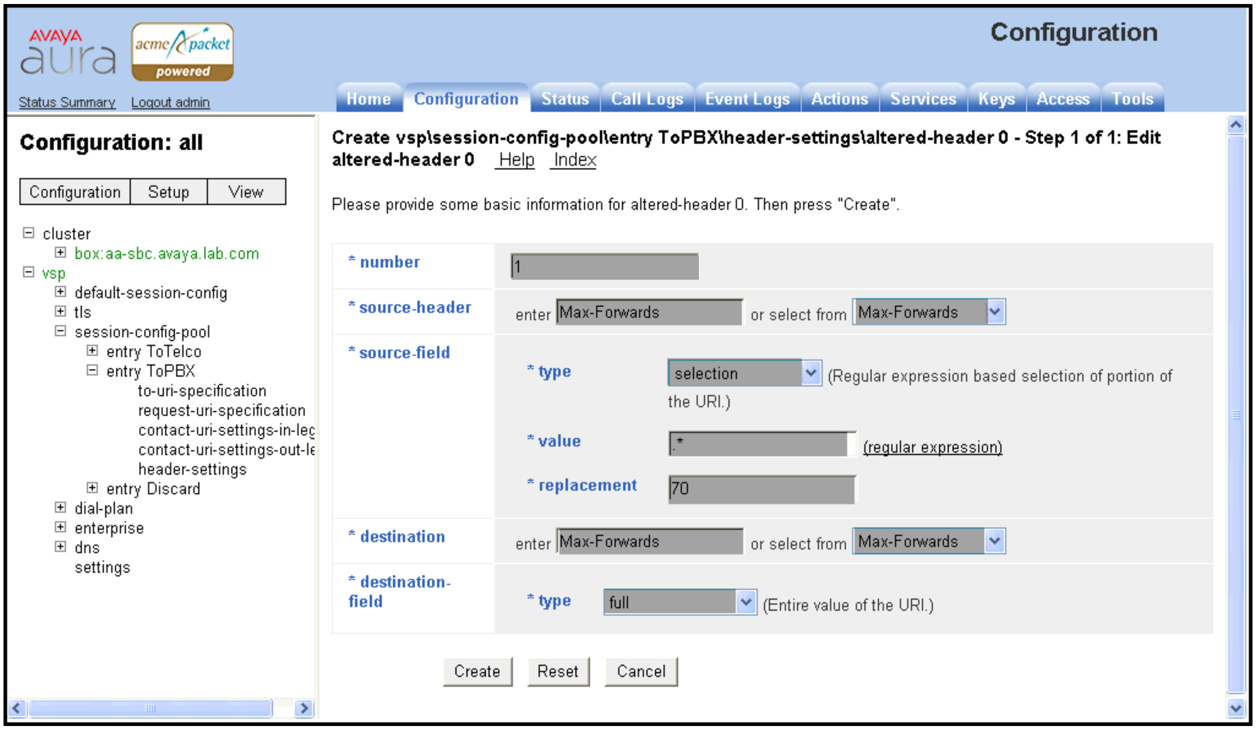
Configure vsp\session-config-pool\entry ToPBX\header-settings

pAssert-mode	disabled (Resource is inactive)
header-to-strip	Edit header-to-strip
allowed-header	Edit allowed-header
blocked-header	Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header
header-normalization	Add header-normalization

In the right pane that appears, enter the following in the fields specified below.

- **number**: Enter a unique number for this altered header.
- **source-header**: Specify the header from which the system initially derives the data that is to be written to the destination header. In this case, enter **Max-Forwards**.
- **source-field type**: Enter **selection**. If **selection** is chosen, then the user may enter a value to match on and a replacement value.
- **source-field value**: Enter **.*** as the value. This is a regular expression that allows the system to match on any value.
- **source-field replacement**: Enter the replacement value. In this case, the value of **70** was used.
- **destination**: Specify the destination header. In this case, enter **Max-Forwards**.
- **destination-field**: Enter **full**. This specifies that the full destination header will be over-written with the new one that was derived from the source header.

Click the **Create** button.

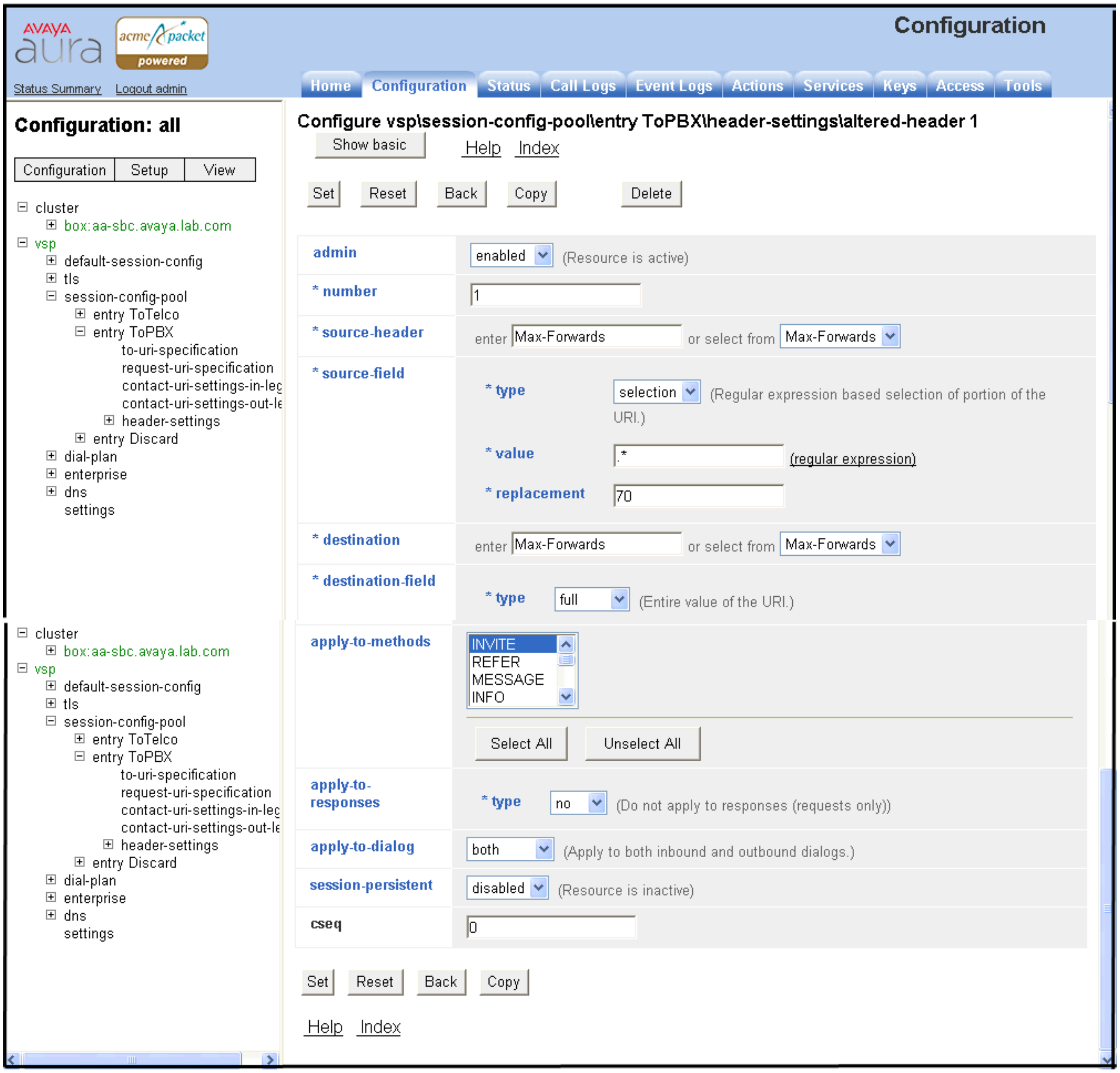


Create vsp\session-config-pool\entry ToPBX\header-settings\altered-header 0 - Step 1 of 1: Edit altered-header 0 Help Index

Please provide some basic information for altered-header 0. Then press "Create".

* number	1
* source-header	enter Max-Forwards or select from Max-Forwards
* source-field	* type: selection (Regular expression based selection of portion of the URI.) * value: .* (regular expression) * replacement: 70
* destination	enter Max-Forwards or select from Max-Forwards
* destination-field	* type: full (Entire value of the URI.)

The right pane then displays the newly created altered header with default values for all other fields. Click the **Set** button on this page to complete the configuration.

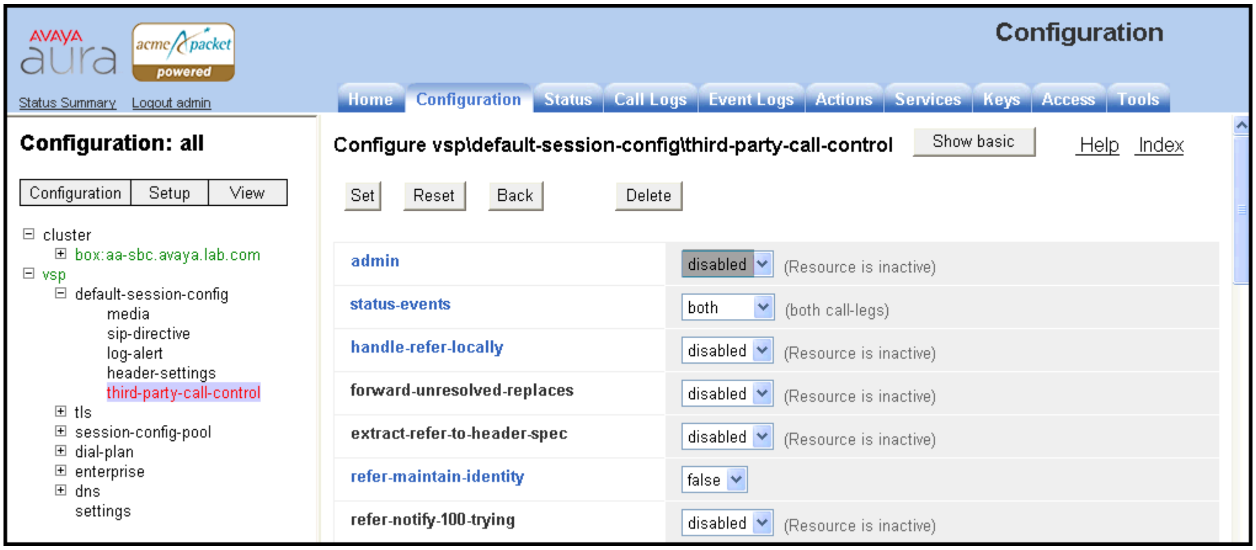


Configure vsp\session-config-pool\entry ToPBX\header-settings\altered-header 1

admin	enabled (Resource is active)
* number	1
* source-header	enter Max-Forwards or select from Max-Forwards
* source-field	* type: selection (Regular expression based selection of portion of the URI.) * value: .* (regular expression) * replacement: 70
* destination	enter Max-Forwards or select from Max-Forwards
* destination-field	* type: full (Entire value of the URI.)
apply-to-methods	INVITE REFER MESSAGE INFO
apply-to-responses	* type: no (Do not apply to responses (requests only))
apply-to-dialog	both (Apply to both inbound and outbound dialogs.)
session-persistent	disabled (Resource is inactive)
cseq	0

7.2.4. Third Party Call Control

Disable third party call control. Navigate to **vsp → default-session-config → third-party-call-control**. Set the **admin** field to **disabled**.

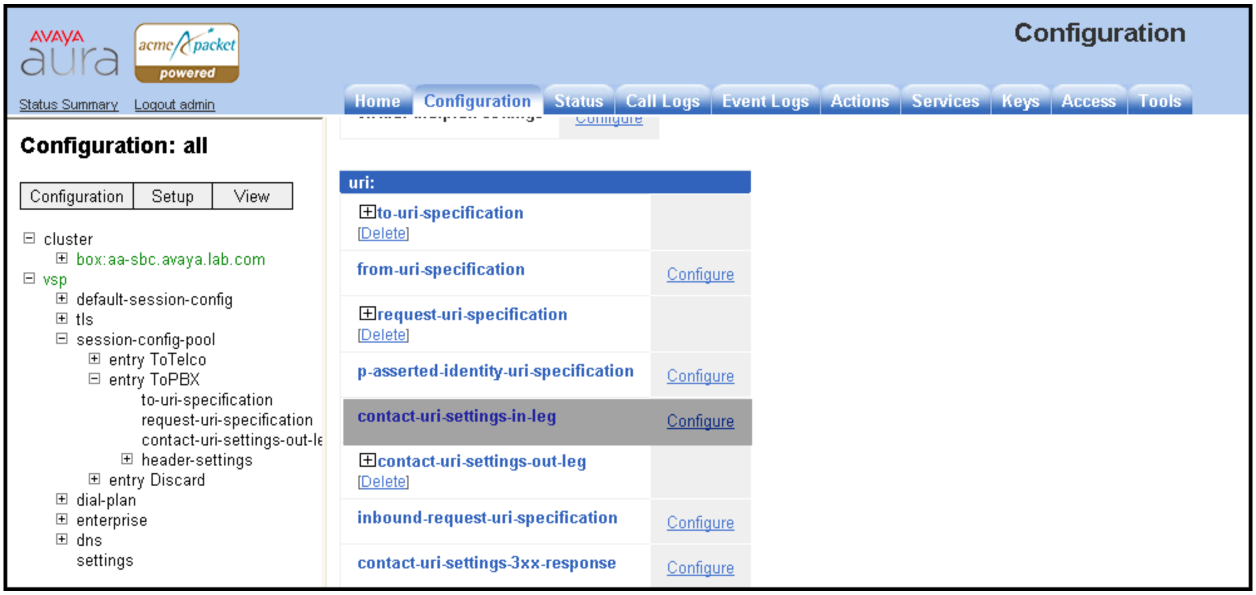


Configure vsp\default-session-config\third-party-call-control

admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	disabled	(Resource is inactive)
forward-unresolved-replaces	disabled	(Resource is inactive)
extract-refer-to-header-spec	disabled	(Resource is inactive)
refer-maintain-identity	false	
refer-notify-100-trying	disabled	(Resource is inactive)

7.2.5. Contact Header

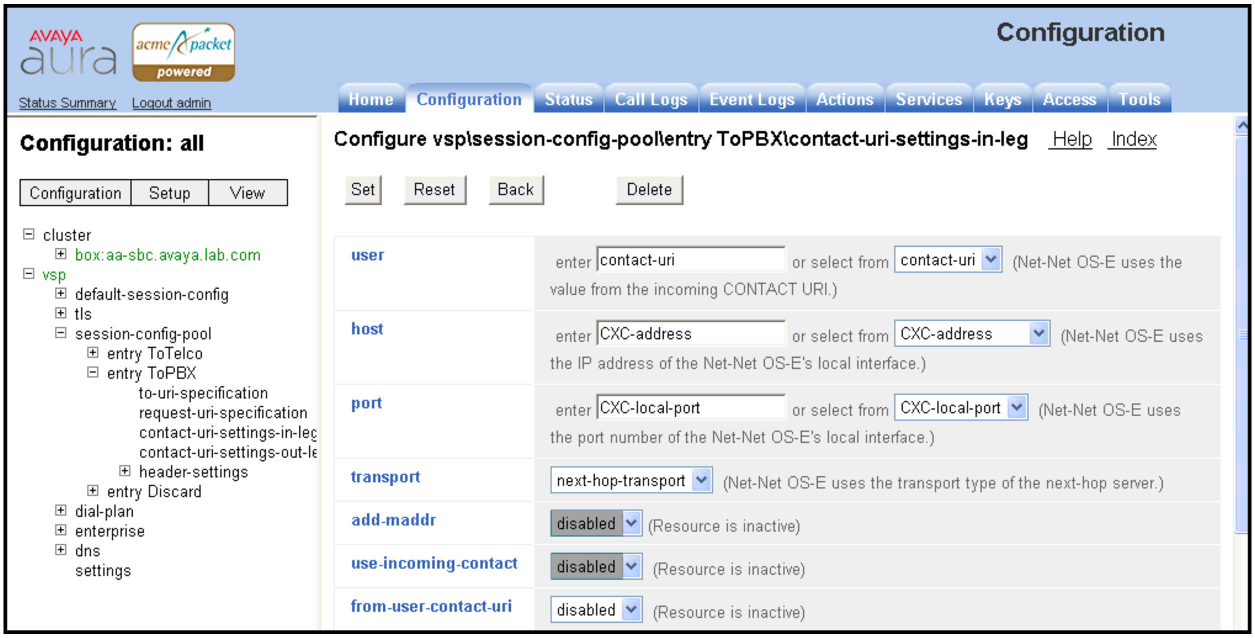
Using the settings chosen in the installation wizard, the Avaya Aura® SBC does not automatically pass to the service provider the updated Contact header that results from a redirected call. In order to have the updated Contact header passed to the service provider, first navigate to **vsp → session-config-pool → entry ToPBX**. Scroll down to the **uri** section and click **Configure** next to **contact-uri-settings-in-leg**.



uri:

⊞to-uri-specification [Delete]	
from-uri-specification	Configure
⊞request-uri-specification [Delete]	
p-asserted-identity-uri-specification	Configure
contact-uri-settings-in-leg	Configure
⊞contact-uri-settings-out-leg [Delete]	
inbound-request-uri-specification	Configure
contact-uri-settings-3xx-response	Configure

In the right pane that appears, set the **add-maddr** field to **disabled** and the **use-incoming-contact** field to **disabled**.



Configure vsp\session-config-pool\entry ToPBX\contact-uri-settings-in-leg

user	enter contact-uri or select from contact-uri (Net-Net OS-E uses the value from the incoming CONTACT URI.)
host	enter CXC-address or select from CXC-address (Net-Net OS-E uses the IP address of the Net-Net OS-E's local interface.)
port	enter CXC-local-port or select from CXC-local-port (Net-Net OS-E uses the port number of the Net-Net OS-E's local interface.)
transport	next-hop-transport (Net-Net OS-E uses the transport type of the next-hop server.)
add-maddr	disabled (Resource is inactive)
use-incoming-contact	disabled (Resource is inactive)
from-user-contact-uri	disabled (Resource is inactive)

Use the same procedure described in this section to set these same values for the **contact-uri-settings-out-leg**. Repeat again for the **contact-uri-settings-in-leg** and **contact-uri-settings-out-leg** of the ToTelco session-config-pool by navigating to **vsp → session-config-pool → entry ToTelco**.

7.2.6. Normalizing Calling Number in From Header

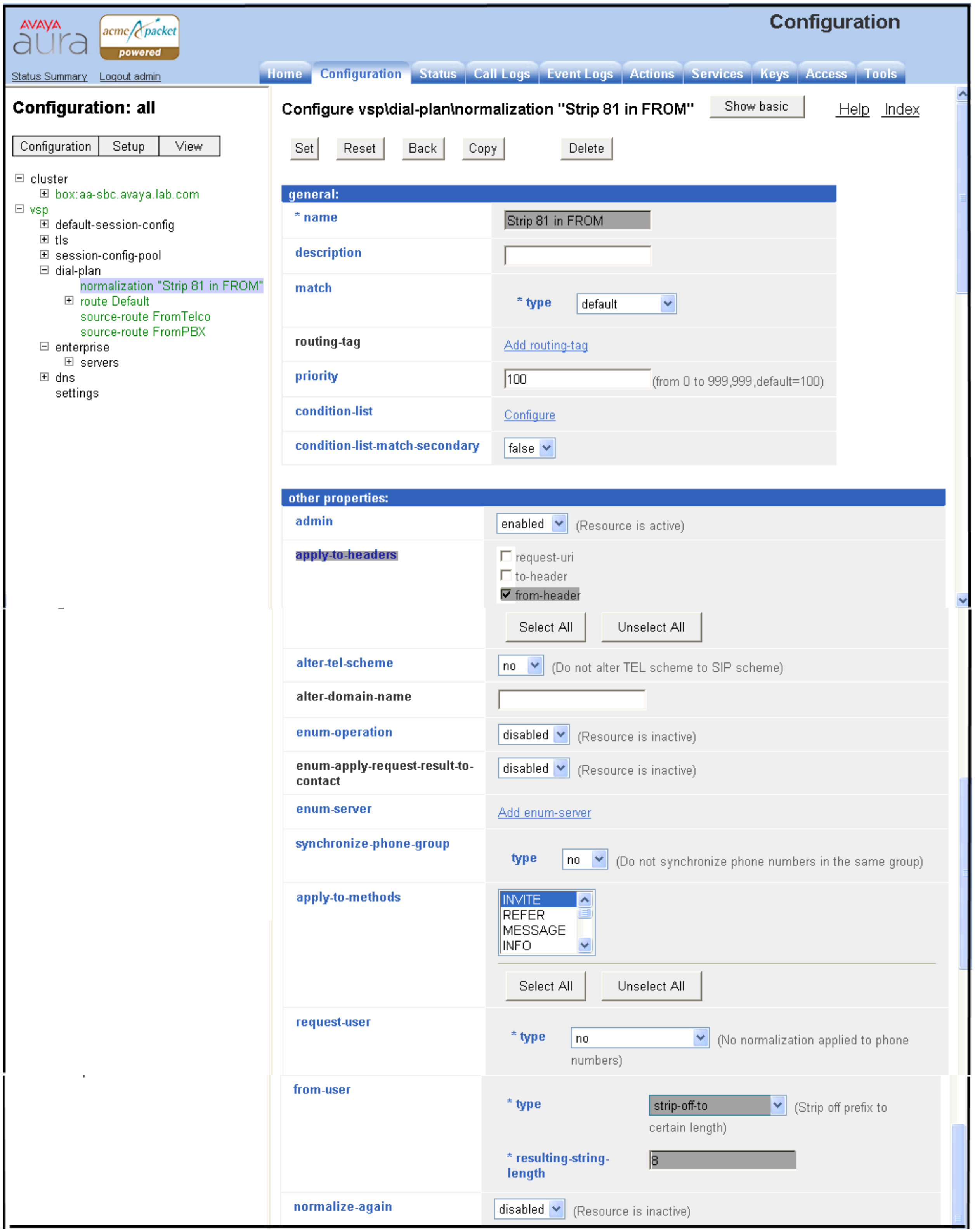
The inbound call INVITE from Alestra to the enterprise contains an **81** followed by **8** digits in the **From** header for the calling number. This prevents some of the EC500 mobility call features from working properly since the EC500 mobile number configured on Avaya Aura® Communication Manager (in **off-pbx-telephone station-mapping** form) has to match the number in the inbound INVITE **From** header. With Alestra Enlace IP SIP Trunk service, Sonus was not programmed to route calls with leading digits **81**. To have the EC500 number configured on Avaya Aura® Communication Manager (in **off-pbx-telephone station-mapping** form) without the **81**, the calling number in the **From** header needs to be normalized to be 8-digits, without the **81** (e.g.,12343093). To do this, navigate to **vsp → dial-plan** and click the **Add normalization** link on the right (not shown). The screen below shows the edit screen for a previously added dial-plan normalization for stripping the **81** from the calling number in the **From** header.

Under the **general:** heading, enter a descriptive text string for **name**.

Scroll down to the **other properties:** heading, check the **from-header** option box for **apply-to-headers**.

Scroll down further to **from user**. Select **strip-off-to** for type, then enter **8** for resulting-string-length. Verify that **INVITE** is selected (default) for **apply-to-methods**.

Click the **Set** button (not shown) after making / verifying all the configuration changes.



Configuration: all

- cluster
  - box:aa-sbc.avaya.lab.com
- vsp
  - default-session-config
  - tls
  - session-config-pool
  - dial-plan
    - normalization "Strip 81 in FROM"
    - route Default
    - source-route FromTelco
    - source-route FromPBX
  - enterprise
    - servers
  - dns
  - settings

Configure vsp\dial-plan\normalization "Strip 81 in FROM"

general:

* name	Strip 81 in FROM
description	
match	* type: default
routing-tag	Add routing-tag
priority	100 (from 0 to 999,999,default=100)
condition-list	Configure
condition-list-match-secondary	false

other properties:

admin	enabled (Resource is active)
apply-to-headers	□ request-uri □ to-header ☑ from-header
alter-tel-scheme	no (Do not alter TEL scheme to SIP scheme)
alter-domain-name	
enum-operation	disabled (Resource is inactive)
enum-apply-request-result-to-contact	disabled (Resource is inactive)
enum-server	Add enum-server
synchronize-phone-group	type: no (Do not synchronize phone numbers in the same group)
apply-to-methods	INVITE REFER MESSAGE INFO
request-user	* type: no (No normalization applied to phone numbers)
from-user	* type: strip-off-to (Strip off prefix to certain length) * resulting-string-length: 8
normalize-again	disabled (Resource is inactive)

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. Alestra SIP Trunking Configuration

To use Alestra SIP Trunking, a customer must request the service from Alestra using their sales processes. The process can be started by contacting Alestra via the corporate web site at http://www.alestra.com.mx/negocios.asp?id=206 and requesting information via the online sales links or telephone numbers.

During the signup process, Alestra will require that the customer provide the public IP address used to reach the Avaya Aura® SBC at the edge of the enterprise. Alestra will provide the IP address of the SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and the Avaya Aura® SBC configuration discussed in the previous sections.

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

9. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Aura® SBC to connect to Alestra SIP Trunking. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

10. 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. Avaya Aura® 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 station** <extension number> - Displays signaling and media information for an active call on a specific station.
   - **status trunk** <trunk access code number> - Displays trunk group information.
   - **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.
2. Avaya Aura® Session Manager:
   - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.
   - **traceSM -x** – Avaya Aura® Session Manager command line tool for traffic analysis. Login to the Avaya Aura® Session Manager management interface to run this command.
3. Avaya Aura® Session Border Controller:
   - **Call Logs** - On the element manager user interface of the Avaya Aura® SBC, the **Call Logs** tab can provide useful diagnostic or troubleshooting information.

11. Conclusion

Alestra Enlace IP SIP Trunk Service passed compliance testing. These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to Alestra SIP Trunking. Alestra SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Alestra SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

12. References

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

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

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

[3] *Installing and Configuring Avaya Aura® Communication Manager, Release 6.0.1, December 2010.*

[4] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.

[5] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.0* June 2010, *D*ocument Number 555-245-205.

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

[7] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011. Number 03-603473.

[8] *Administering Avaya Aura® Session Manager,* Release 6.1, November 2010, Document Number 03-603324.

[9] *Avaya Aura® Session Border Controller System Administration Guide*, V.6.0, September 2010

[10] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* Release 3.1, November 2009, Document Number 16-300698.

[11] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide,* Release 2.6, June 2010, Document Number 16-601944.

[12] *Using Avaya one-X® Communicator,* April 2011.

[13] *Administering Avaya one-X® Communicator, Release 6.1, April 2011*

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

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

13. Appendix A: Avaya Aura® SBC Configuration File

```
#
#  Copyright (c) 2004-2011  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 18:28:16 Fri 2011-09-09
#
config cluster
 config box 1
  set hostname aa-sbc.avaya.lab.com
  set name aa-sbc.avaya.lab.com
  set identifier 00:ca:fe:57:98:68
  config interface eth0
   config ip inside
    set ip-address static 172.16.5.42/24
    config ssh
    return
    config snmp
     set trap-target 192.168.10.41 162
     set trap-filter generic
     set trap-filter dos
     set trap-filter sip
     set trap-filter system
    return
    config web
    return
    config web-service
     set protocol https 8443
     set authentication certificate "vsp\tls\certificate ws-cert"
    return
    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 Static0
      set admin disabled
      set destination network 192.11.13.4/30
      set gateway 172.16.5.40
     return
     config route Static1
      set destination network 192.168.10.0/24
      set gateway 172.16.5.254
     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
    return
   return
  return
  config interface eth2
   config ip outside
    set ip-address static 11.111.111.190/26
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
    return
    config icmp
    return
    config media-ports
     set base-port 5000
     set count 60000
    return
    config routing
     config route Default
      set gateway 11.111.111.129
     return
     config route external-sip-media-1
      set destination network 123.45.67.0/24
      set gateway 123.45.67.1
     return
    return
    config kernel-filter
     config allow-rule allow-sip-udp-from-peer-1
      set destination-port 5060
      set source-address/mask 222.222.222.9/24
      set protocol udp
     return
     config allow-rule allow-sip-tcp-from-peer-1
      set destination-port 5060
      set source-address/mask 222.222.222.9/24
      set protocol tcp
     return
     config deny-rule deny-all-sip
      set destination-port 5060
     return
    return
   return
  return
  config cli
   set prompt aa-sbc.sil.miami.avaya.com
  return
 return
return

config services
 config event-log
  config file access
   set filter access info
   set count 3
  return
  config file system
   set filter system info
   set count 3
  return
  config file errorlog
   set filter all error
   set count 3
  return
  config file db
   set filter db debug
   set filter dosDatabase info
   set count 3
  return
  config file management
   set filter management info
   set count 3
  return
  config file peer
   set filter sipSvr info
   set count 3
  return
  config file dos
   set filter dos alert
   set filter dosSip alert
   set filter dosTransport alert
   set filter dosUrl alert
   set count 3
  return
  config file krnlsys
   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 header-settings
   set blocked-header P-Location
   set blocked-header P-Charging-Vector
  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
    set host local-ip
   return
   config contact-uri-settings-in-leg
```

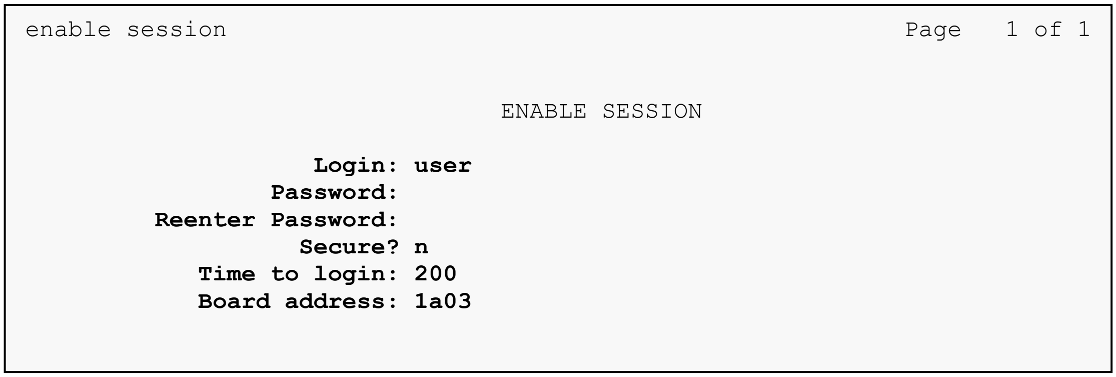
```
    set add-maddr disabled
   return
   config contact-uri-settings-out-leg
    set add-maddr disabled
   return
  return
  config entry ToPBX
   config to-uri-specification
    set host next-hop-domain
   return
   config request-uri-specification
    set host next-hop-domain
   return
   config contact-uri-settings-in-leg
    set add-maddr disabled
   return
   config contact-uri-settings-out-leg
    set add-maddr disabled
   return
   config header-settings
    config altered-header 1
     set source-header Max-Forwards
     set source-field selection .* 70
     set destination Max-Forwards
     set destination-field full
    return
   return
  return
  config entry Discard
   config sip-directive
   return
  return
 return
 config dial-plan
  config normalization "Strip 81 in FROM"
   set apply-to-headers from-header
   set apply-to-methods INVITE
   set from-user strip-off-to 8
  return
  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 avaya.lab.com
    set failover-detection ping
    set ping-interval 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
     config server PBX1
      set host 172.16.5.32
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set failover-detection ping
    set ping-interval 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
     config server Telco1
      set host 222.222.222.9
      config error-response-codes
      return
     return
    return
   return
  return
 return
 config dns
  config resolver
   config server 192.168.10.254
   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 Max-Forwards
  set enum-strings SIPSourceHeader Diversion
 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
0x0014d07f72183a9d417919ba8b88534c69edc277fa62db53c537eaa171
   set permissions access\permissions superuser
  return
  config user cust
   set password
0x003f399c1599a5b724d456aa2f1a5533c42f5cb44dd90bb2735fa9c31c
   set permissions access\permissions read-only
  return
  config user init
   set password
0x00aca232f01ac9dffd3fbd7512ed9cee89c2d2664a014bcede192e92ec
   set permissions access\permissions superuser
  return
  config user craft
   set password
0x0061d457b58ba03af19d47b7b1b811e10c3fd18ba4355a82907d0b5d7a
   set permissions access\permissions superuser
  return
  config user dadmin
   set password
0x00b55638536bf8eb548f114ea9f69b8b5295457d8a4e64f6a60d354429
   set permissions access\permissions read-only
  return
 return
return

config features
return
```

14. Appendix B: Workaround for Double DTMF Digit Detection

DTMF digits detection: In the sample configuration Alestra was sending DTMF digits, both in-band as audible tones and out-of-band as RTP events (RFC2833) and the two were not precisely aligned. The Avaya G450 Gateway was detecting the in-band and out-of-band digits as two separate digits instead of the same digit sent two ways, and this was causing problems with voice mail retrieval during the login process to the voice mail system. For interoperability, Alestra must disable the sending of in-band digits and only send DTMF digits as out-of-band RTP events. Alestra technician must disable this at the time of service activation. Otherwise, the detection of incoming DTMF digits from the network is unreliable. In-band tones must be disabled when using either the G.711A or G.729A codec. In rare cases if problems persist, the workaround described in this Appendix can also be applied. However, this is not recommended unless **absolutely** necessary since it burdens the media resources of the Communication Manager with additional processing.

This Appendix describes the steps to enable a firmware workaround to address the condition when DTMF tones are received both in-band and out-of-band but are not properly aligned with each other. **Steps 1** and **2** describe the procedure if a TN2602 MedPro circuit pack is used. **Step 3** describes the procedure for the G450 and G430 gateways. This firmware workaround will only be applied for trunks that have enabled use of RFC2833 for DTMF transmission (i.e., the **DTMF over IP** field is set to **rtp-payload** on the Avaya Aura® Communication Manager signaling form). This procedure requires logging into the circuit pack directly via SSH or Telnet. The ability to access the circuit pack directly must first be enabled through the Avaya Aura® Communication Manager SAT interface.

Step	Description
1.	**Enable Session for TN2602** In order to log into the TN2602 Circuit Pack, first enable this capability by using the **enable session** command on the Avaya Aura® Communication Manager SAT interface. Set the parameters as described below. ▪ **Login**: Create a login name for use when logging into the circuit pack. ▪ **Password**: Create a password for this login name. ▪ **Reenter Password**: Enter the password again. ▪ **Secure?**: Select ***n*** for Telnet or ***y*** for SSH. ▪ **Time to login**: Enter the number of minutes this login will be valid. The maximum value is 255. ▪ **Board address**: Enter the cabinet/carrier/slot location for the circuit pack that will be accessed. This value can be found from the **list configuration all** command. 

```
enable session                                                    Page   1 of 1

                                 ENABLE SESSION

                     Login: user
                  Password:
          Reenter Password:
                   Secure? n
             Time to login: 200
             Board address: 1a03
```

Step	Description

2.	**Login and Set Parameters**
	Log in to the TN2602 IP address using either Telnet or SSH as defined in the previous step. The IP address can be found using the **list ip-interface all** command. When prompted, enter the **Login** and **Password** as defined in the previous step. At the command prompt, enter the following three commands.
	▪ **setVoipParam 60,1** - Sets up a temporary buffer with VOIP parameter 60 set to value 1. This parameter enables the firmware workaround.
	▪ **sendVoipParams** - Sends any VOIP parameters to the DSPs.
	▪ **saveVoipParams** - Save parameters to flash memory so the configuration will survive a reset.
	`Enter Login ID: user`
	`Password:`
	`SIMPLEX-> setVoipParam 60,1`
	`value = 0 = 0x0`
	`SIMPLEX-> sendVoipParams`
	`value = 0 = 0x0`
	`SIMPLEX-> saveVoipParams`
	`value = 0 = 0x0`
	`SIMPLEX->`

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

G450/G430 Gateway
If a G450/G430 is used in the configuration, then log in to the gateway using proper credentials and issue the following command shown in bold below.

- **voip-parameters** – Enter the VoIP parameters configuration mode.
- **set id 60 value 1** - Sets up a temporary buffer with VOIP parameter 60 set to value 1. This parameter enables the firmware workaround.
- **dsp-downlink** - Sends any VOIP parameters to the DSPs.
- **Exit** – Exit the VoIP parameter mode.
- **copy run start** - Save parameters to flash memory so the configuration will survive a reset.

```
sp3-g450-001(super)# voip-parameters
Warning:
The values chosen for non-default voip parameters can significantly affect
the quality of service that users experience.  Avaya recommends seeking
technical assistance from Avaya before making any modifications to the voip
parameter defaults.
sp3-g450-001(super-voip-parameters)# set id 60 value 1
Done!
sp3-g450-001(super-voip-parameters)# dsp-downlink
Done!
sp3-g450-001(super-voip-parameters)# exit
sp3-g450-001(super)# copy run start
Warning! It is a recommended policy to override default configuration
master key with user defined secret - for details see user reference.
Otherwise device saves configuration secrets using Avaya default secret.
Beginning copy operation .................. Done!
sp3-g450-001(super)#
```

</td></tr>
</table>

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.