Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller 6.0 with Level 3 Communications SIP Trunking – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Level 3 Communications SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya Aura® Session Border Controller or Avaya Aura® Session Manager.

Level 3 Communications is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the steps required to configure Session Initiation Protocol (SIP) Trunking between Level 3 Communications SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Boarder Controller, Avaya Aura® Session Manager and Avaya Aura® Communication Manager, along with various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Level 3 Communications SIP Trunking service are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Aura® Session Border Controller to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to Level 3 Communications SIP Trunking service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

Level 3 Communications SIP Trunking service passed compliance testing.

2.1. Interoperability Compliance Testing

To verify SIP Trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client).
- Avaya one-X Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. H.323 was the only protocol tested.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls and local directory assistance (411).
- Codecs G.729A, G.711MU and G.711A.
- T.38 Fax
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Network Call Redirection using the SIP REFER method

- Off-net call forwarding and mobility (extension to cellular).

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- Network Call Redirection using the 302 response is not supported by Level 3.

2.2. Test Results

Interoperability testing of Level 3 Communication's SIP Trunking service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. 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/Level3 SIP Trunk solution. It is listed here simply as an observation.

- **Max-Forwards:** On incoming PSTN calls to an enterprise phone that is forwarded off-net to another PSTN phone, the Max-Forwards value in the incoming SIP INVITE was too small to allow the message to traverse all the SIP hops internal to the enterprise to reach the PSTN phone. Thus, the SBC was used to increase this value when the INVITE arrived at the SBC from the network. (See **Section 7.2.7**)

- **Outbound Calling Number Restriction**: Communication Manager sends the calling party number (CPN) in the P-Asserted Identity header when a station is programmed to block the CPN. Level 3 requires a number associated with the SIP trunk to be in either the From, Diversion, or Remote-Party-ID headers. The SBC was used to create a Remote-Party-ID header using information sent in the P-Asserted Identity header. (See **Section 7.2.6**)

- **No Support for G.729B:** Level 3 SIP Trunk service does not support G.729B codec.

- **SIP 302 Redirect Method is not supported**: When a Communication Manager vector is programmed to redirect an inbound call to a PSTN number before answering the call, Level 3 SIP Trunk service will send an ACK to the "302 Moved Temporarily" SIP message from the enterprise but will not redirect the call to the new party in the Contact header of the 302 message. The originator of the inbound call hears a busy signal in this failure scenario. A workaround is to use the REFER method to redirect the call by having Communication Manager answer the call first with an announcement in the vector.

2.3. Support

For technical support on Level 3 Communications SIP Trunking service, contact Level 3 using the Customer Care links at www.Level3.com.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Level 3 Communications Managed IP Telephony Service. This is the configuration used for compliance testing.

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

- Avaya S8300C Server running Avaya Aura® Communication Manager
- Avaya G430 Media Gateway
- HP DL360 Server running Avaya Aura® Session Manager
- HP DL360 Server running Avaya Aura® System Manager
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 4600-Series IP telephones (H.323)
- Avaya 1600-Series IP telephones (H.323)
- Avaya one-X Communicator (H.323)
- Avaya digital and analog telephones

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 SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

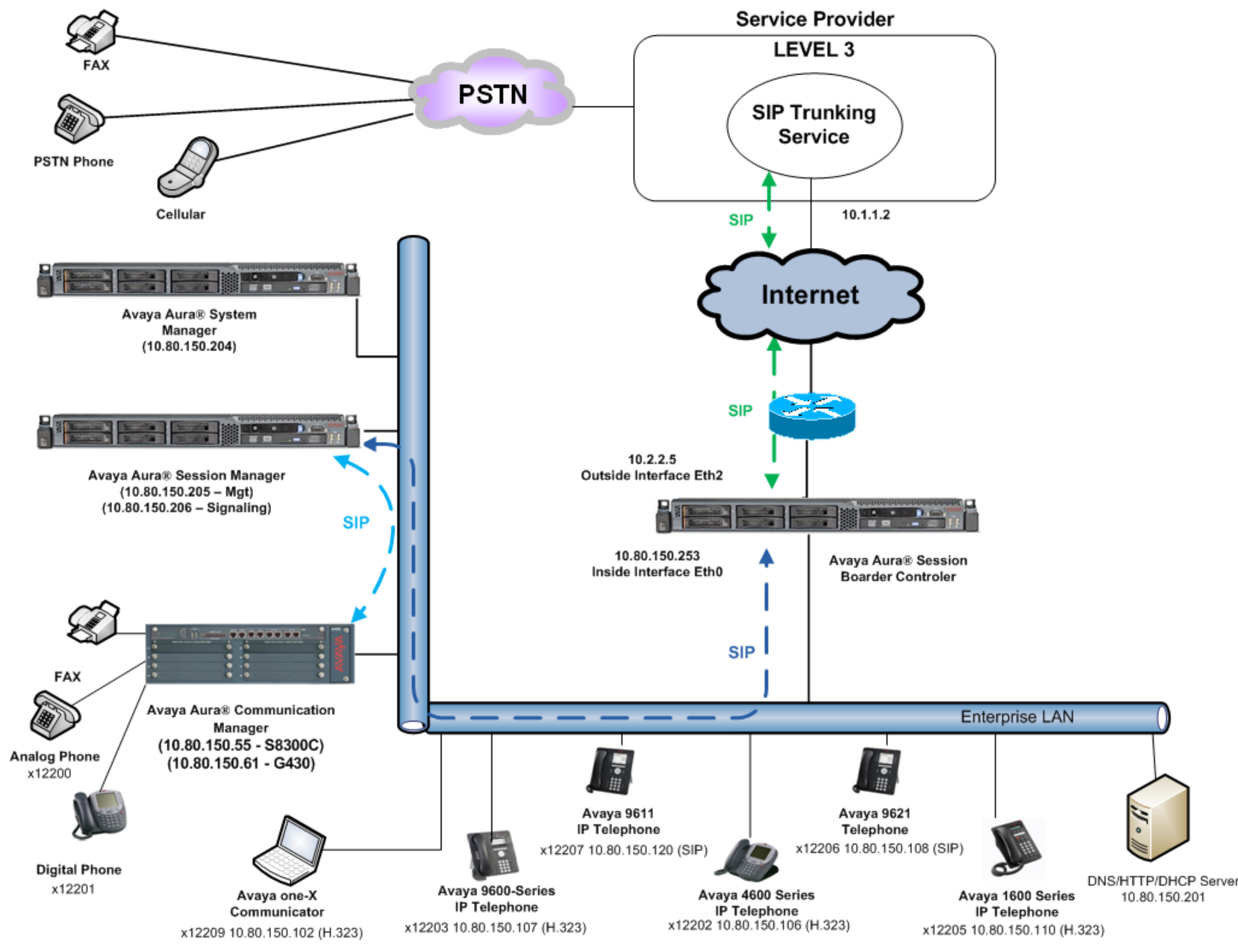


Figure 1: Avaya IP Telephony Network using Level 3 Communications SIP Trunk Service

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

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

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager uses configured dial patterns (or regular expressions) to determine the route to the SBC. From the SBC, the call is sent to Level 3 Communications SIP Trunk service.

Level 3 Communications requires outbound toll-free calls to be dialed with 1 + 10 digits while all other North American Numbering Plan (NANP) numbers can be dialed with either 10 digits or 11 digits (1 + 10).

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manger running on Avaya S8300c Server	R015x.02.1.016.4
Avaya Aura® Messaging	R016x.00.1.510.1
Avaya Aura® System Manager	6.1.0.0.7345-6.1.5.115
Avaya Aura® Session Manager	6.1.4.0.614005
Avaya Aura® Session Border Controller	E362
Avaya G430	31.18.1
Avaya 4625SW IP Telephone (H.323)	2.9010
Avaya 1608 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.2
Avaya 9641 IP Telephone (H.323)	Avaya one-X Deskphone Edition 6.0
Avaya 9621 IP Telephone (SIP)	Avaya one-X Deskphone SIP Edition 6.0
Avaya one-X Communicator (H.323 and SIP)	6.1.0.12
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Level 3 Communication Components	
Component	Release
Broadworks	R14 SP9

The specific configuration above was used for the compatibility 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 Communication Manager

This section describes the procedure for configuring Avaya Aura® Communication Manager for Level 3 Communication's SIP Trunk service. A SIP trunk is established between Communication Manager and Avaya Aura® Session Manager for use by signaling traffic to and from Level 3. It is assumed the general installation of Communication Manager, Avaya G430 Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these

Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN phone 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 **450** licenses are available and **265** 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: 450   18
           Maximum Concurrently Registered IP Stations: 450   4
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 450   0
                        Maximum Video Capable Stations: 450   0
                   Maximum Video Capable IP Softphones: 450   0
                       Maximum Administered SIP Trunks: 450   265
  Maximum Administered Ad-hoc Video Conferencing Ports: 450   0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 0     0
                     Maximum Media Gateway VAL Sources: 50    1
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

5.2. System Features

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

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

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

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

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

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

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

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 Communication Manager **(procr**) and Session Manager (**ASM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM                  10.80.150.206
CMM                  10.80.150.56
default              0.0.0.0
procr                10.80.150.55
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, **ip-codec-set 2** was used for this purpose. Level 3 Communications SIP Trunking service supports G.729A, G.711A and G.711MU. During compliance testing each of the supported codecs were tested independently by changing the order of preference to list the codec being tested as the first chose. The true order of preference is defined by the end customer. In the example below, **G.729A** and **G.711MU** was entered in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 2

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

Set the **Fax Mode** to **t.38-standard**.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

5.5. IP Network Region

Create a separate IP network region for the service provider SIP 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 10 was chosen for the service provider SIP trunk. IP network region 1 is the default IP network region and was used for the Processor Ethernet and the G430 gateway. IP network region 2 was used for the IP phones. Use the **change ip-network-region 10** command to configure region 10 with the following parameters:

- Set the **Location** field to match the enterprise location for this SIP trunk.
- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avayalab.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.

```
change ip-network-region 10                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 10
Location: 1       Authoritative Domain: avayalab.com
    Name: SIP Trunks
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                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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 10 and any other regions used in the enterprise. Enter the desired IP codec set in the **codec set** column of the row with destination regions (**dst rgn**) used in the enterprise. 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 10 (the service provider region) and regions 1 (Processor Ethernet and G430) and 2 (IP Phones).

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

 Source Region: 10    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     y    NoLimit                                             n       t
...
 10   2                                                                all
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security).
- 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 that Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. For ease of troubleshooting, the compliance test was conducted with the **Transport Method** set to **tcp** and the **Near-end Listen Port** and **Far-end Listen Port** set to **5070**. (For TCP, the well-known port value is 5060).
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **ASM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.

- Default values may be used for all other fields.

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

 Group Number: 1             Group Type: sip
                       Transport Method: tcp
  IMS Enabled? n
     IP Video? n




   Near-end Node Name: procr                 Far-end Node Name: ASM
 Near-end Listen Port: 5070                Far-end Listen Port: 5070
                                        Far-end Network Region: 10
Far-end Domain: avayalab.com

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                     Direct IP-IP Early 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**.
- Set the **COR** to the class of restriction number used in the enterprise for PSTN trunks.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

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

Group Number: 1                   Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SP            COR: 1        TN: 1        TAC: *101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                      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.

```
add 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
```

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end.

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. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

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


                     Numbering Format: public
                                                 UUI Treatment: service-provider

                                                  Replace Restricted Numbers? y
                                                 Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no



 Show ANSWERED BY on Display? y
```

On **Page 4**, set the **Network Call Redirection** field to **y**. This allows inbound calls transferred back to the PSTN to use the SIP REFER method, see [17]. Set the **Send Diversion Header** field to **y**. This field will add a Diversion header and 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 **Support Request History** field to **n**.

Set the **Telephone Event Payload Type** to **101**, the value preferred by Level 3 Communications.

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

5.8. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Level 3 Communications is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID. As an example, the following screen illustrates a conversion of DID number **7205550700** to extension **12200**.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of  30
                      INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 7205550700       10  12200
 public-ntwrk    10 7205550705       10  12201
 public-ntwrk    10 7205550720       10  12202
 public-ntwrk    10 7205550721       10  12203
 public-ntwrk    10 7205550722       10  12204
 public-ntwrk    10 7205550723       10  12205
 public-ntwrk    10 7205551182       10  12206
 public-ntwrk    10 7205551814       10  12207
 public-ntwrk    10 7205550748       10  12208
 public-ntwrk    10 7205554149       10  12209
 public-ntwrk
```

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, ten DID numbers were assigned for testing. These ten numbers were assigned to the ten extensions **12200** to **12209**. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these ten extensions.

```
change 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: 11
 5  1               1         7205550700     10         Maximum Entries: 240
 5  12200           1         7205550700     10
 5  12201           1         7205550705     10
 5  12202           1         7205550720     10
 5  12203           1         7205550721     10
 5  12204           1         7205550722     10
 5  12205           1         7205550723     10
 5  12206           1         7205551182     10
 5  12207           1         7205551814     10
 5  12208           1         7205550748     10
 5  12209           1         7205554149     10
```

5.10. Outbound Routing

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

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all          Percent Full:    0

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

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

```
change feature-access-codes                                     Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: #110
         Abbreviated Dialing List2 Access Code: #111
         Abbreviated Dialing List3 Access Code: #112
Abbreviated Dial - Prgm Group List Access Code: #113
                      Announcement Access Code: #114
                       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: *40
                       Call Pickup Access Code: *41
CAS Remote Hold/Answer Hold-Unhold Access Code: *42
```

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).

```
                              ARS DIGIT ANALYSIS TABLE
                                    Location:  all           Percent Full:    0

           Dialed           Total     Route     Call   Node  ANI
           String          Min  Max  Pattern    Type   Num   Reqd
     12                    11   11    1         fnpa         n
     12007                 5    5     1         locl         n
     13                    11   11    1         fnpa         n
     14                    11   11    1         fnpa         n
     15                    11   11    1         fnpa         n
     16                    11   11    1         fnpa         n
     17                    11   11    1         fnpa         n
     18                    11   11    1         fnpa         n
     19                    11   11    1         fnpa         n
     1xxx555               11   11    deny      fnpa         n
     1xxx976               11   11    deny      fnpa         n
     303                   10   10    1         hnpa         n
     411                   3    3     1         svcl         n
     720                   10   10    1         hnpa         n
     911                   3    3     1         svcl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider 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.
- **Pfx Mrk**: **1** The prefix mark (**Pfx Mrk**) of **1** will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: To SIP SP
                             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       1                                                       n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

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

Use the **change ars digit-conversion** command to manipulate the routing of dialed digits that match the DIDs to prevent these calls from going out the PSTN and using unnecessary SIP trunk resources. The example below shows the DID numbers assigned by Level 3 being converted to 5 digit extensions.

```
change ars digit-conversion 0                                  Page   1 of   2
                       ARS DIGIT CONVERSION TABLE
                                 Location: all               Percent Full: 0

  Matching Pattern      Min   Max   Del   Replacement String   Net  Conv ANI Req

  7205550700            10    10    10    12200                ext   y       n
  7205550705            10    10    10    12201                ext   y       n
  7205550720            10    10    10    12202                ext   y       n
  7205550721            10    10    10    12203                ext   y       n
  7205550722            10    10    10    12204                ext   y       n
  7205550723            10    10    10    12205                ext   y       n
  7205551182            10    10    10    12206                ext   y       n
  7205551814            10    10    10    12207                ext   y       n
  7205550748            10    10    10    12208                ext   y       n
  7205554149            10    10    10    12209                ext   y       n
  720991                10    10    5                          ext   y       n
                                                                             n
                                                                             n
```

6. Configure Avaya Aura® Session Manager

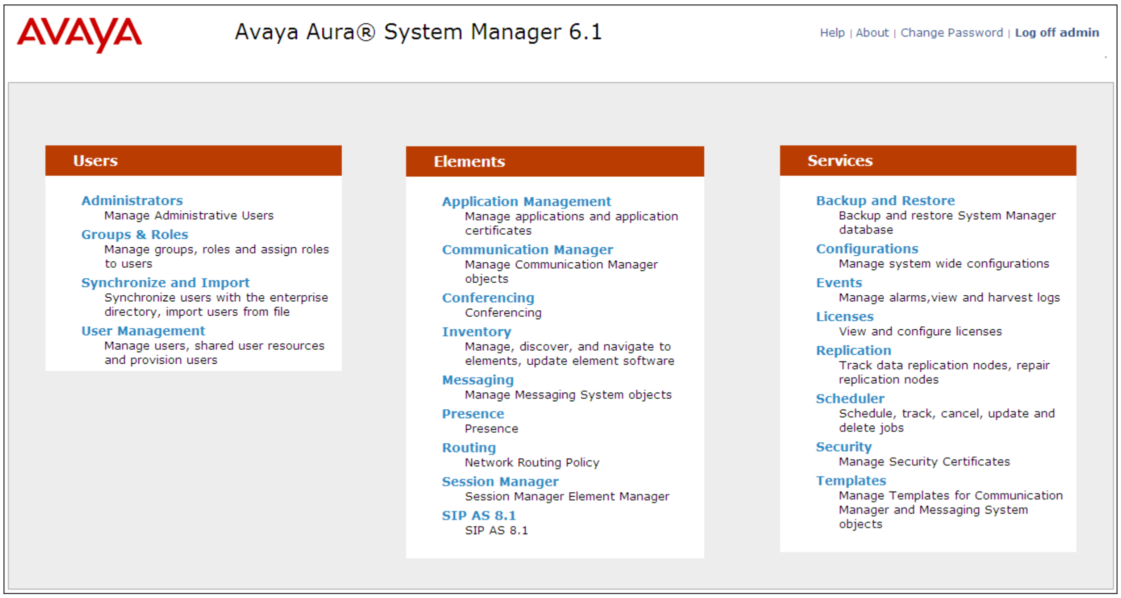
This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include adding the following items:

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

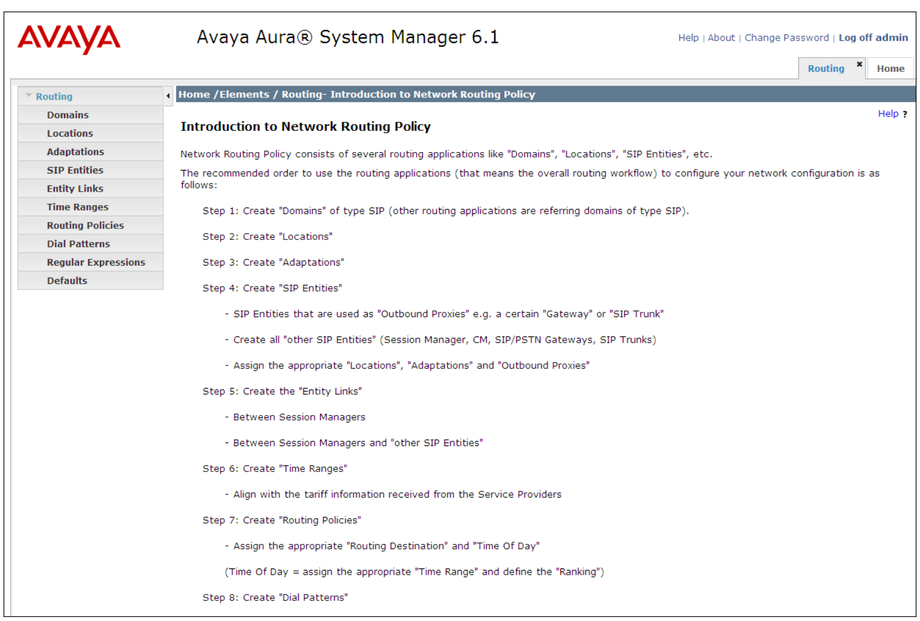
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. System Manager Login and Navigation

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



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

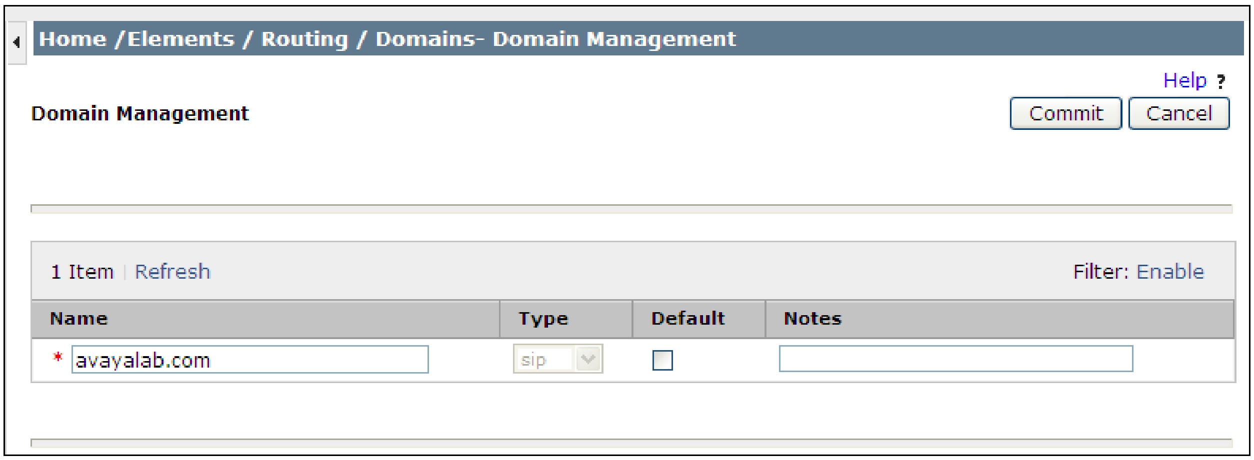


6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, 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 **avayalab.com** domain.



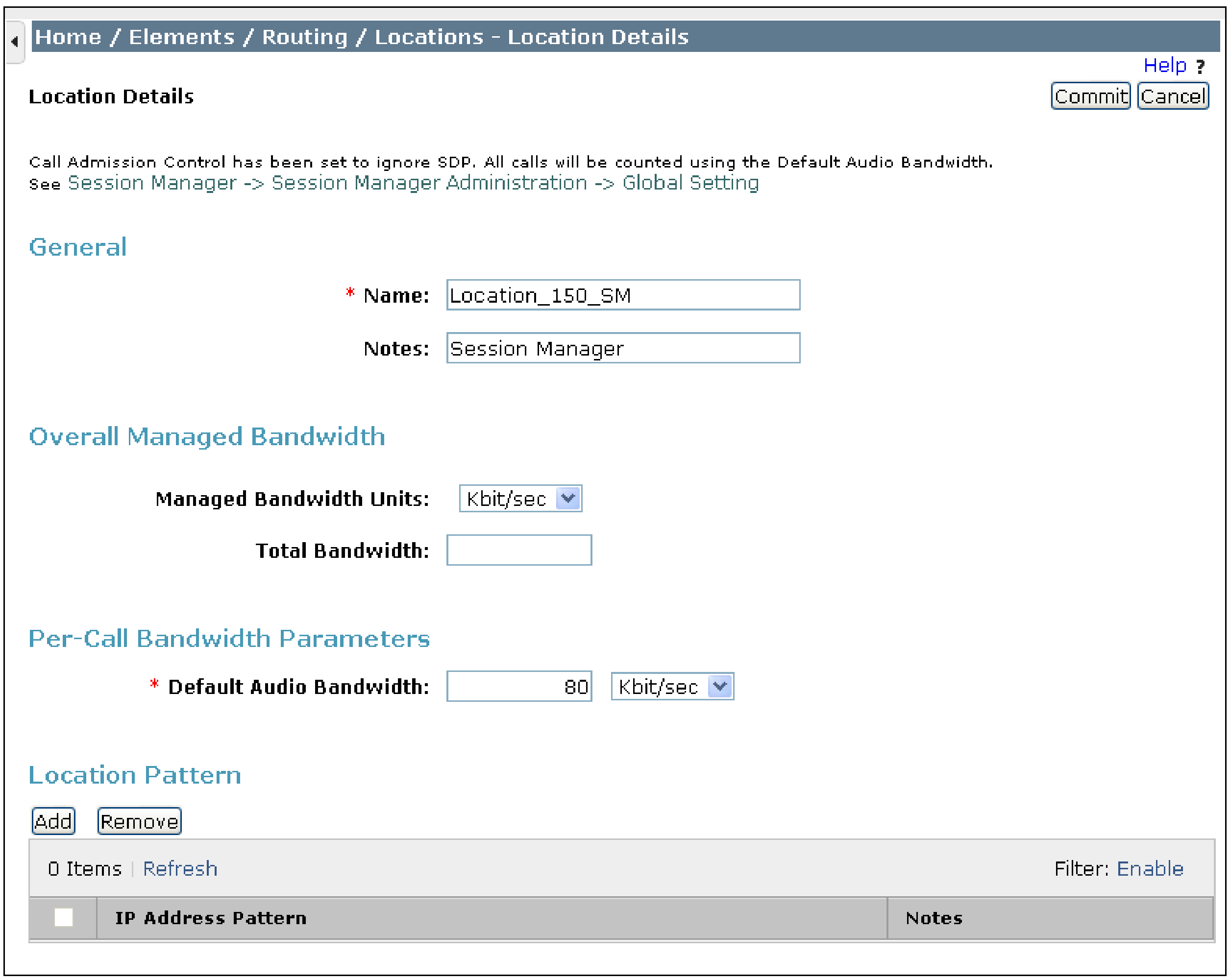
6.3. Add Location

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

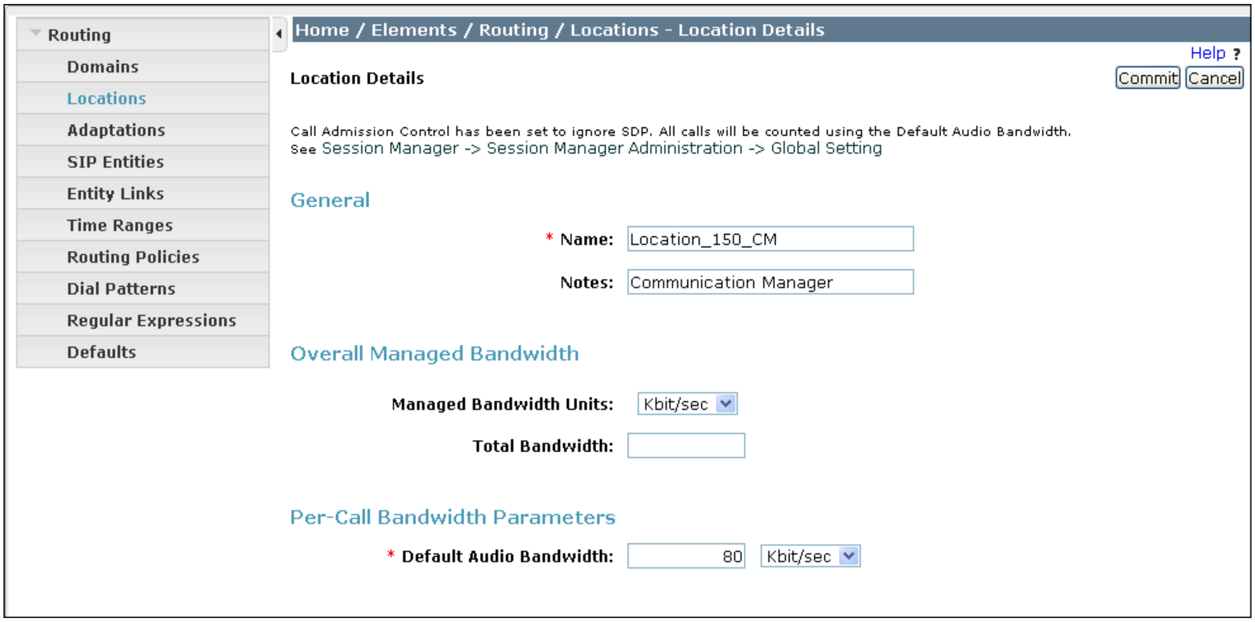
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The screen below shows the addition of **Location_150_SM**. This location will be used for the Session Manager. Click **Commit** to save.

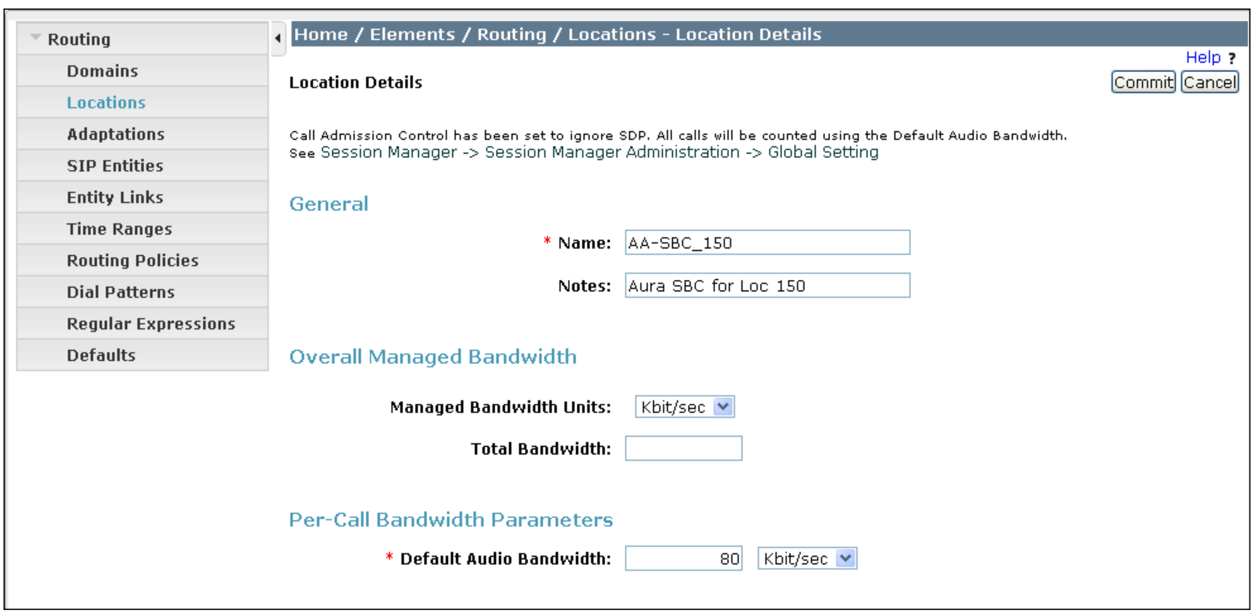


Note: that call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for the Communication Manager and SBC. Displayed below is the screen for **Location_150_CM** used for Communication Manager.



Below is the screen for **AA-SBC_150** used for SBC.



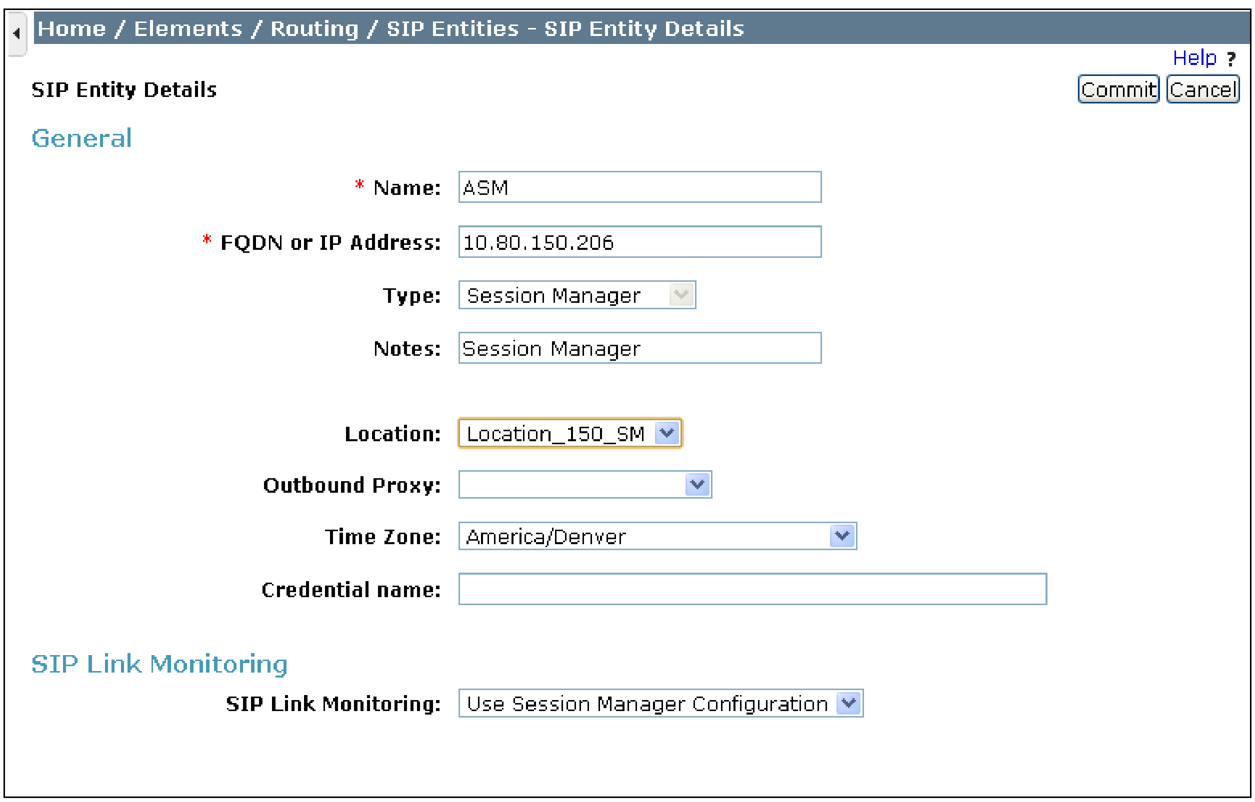
6.4. Add SIP Entities

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

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.



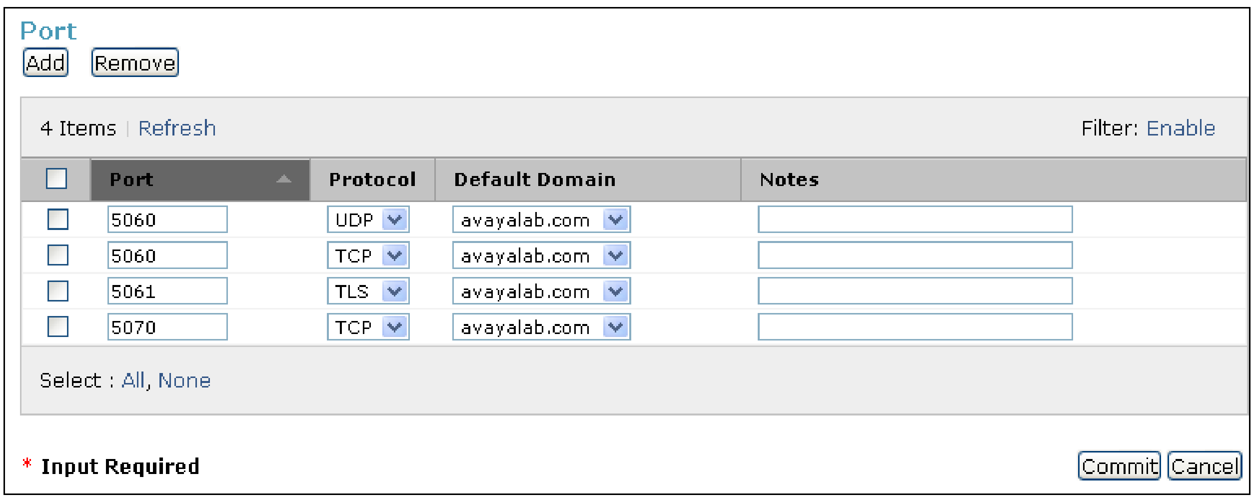
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that the Session Manager will use to listen for SIP requests, typically from registered SIP endpoints or other SIP Entities. The Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

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

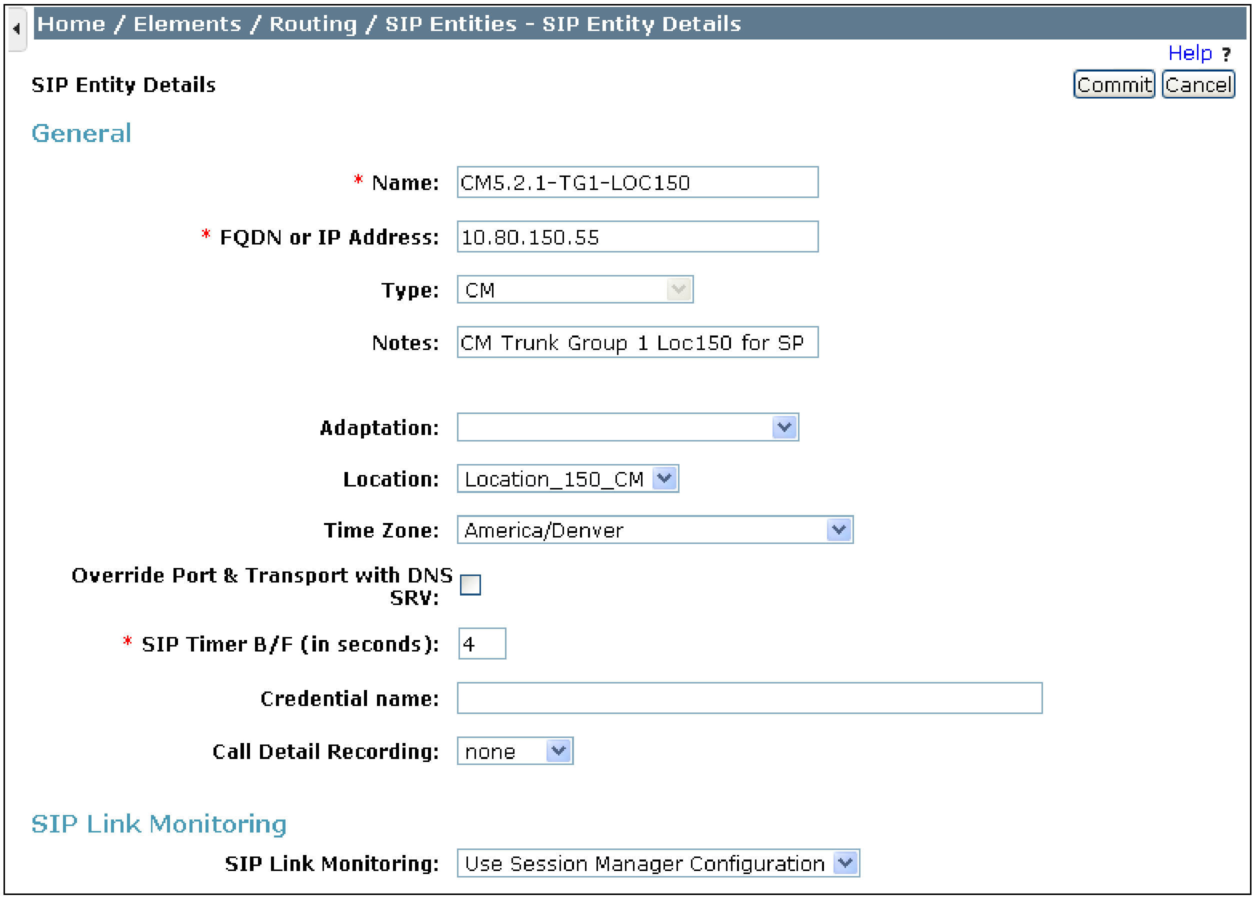
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

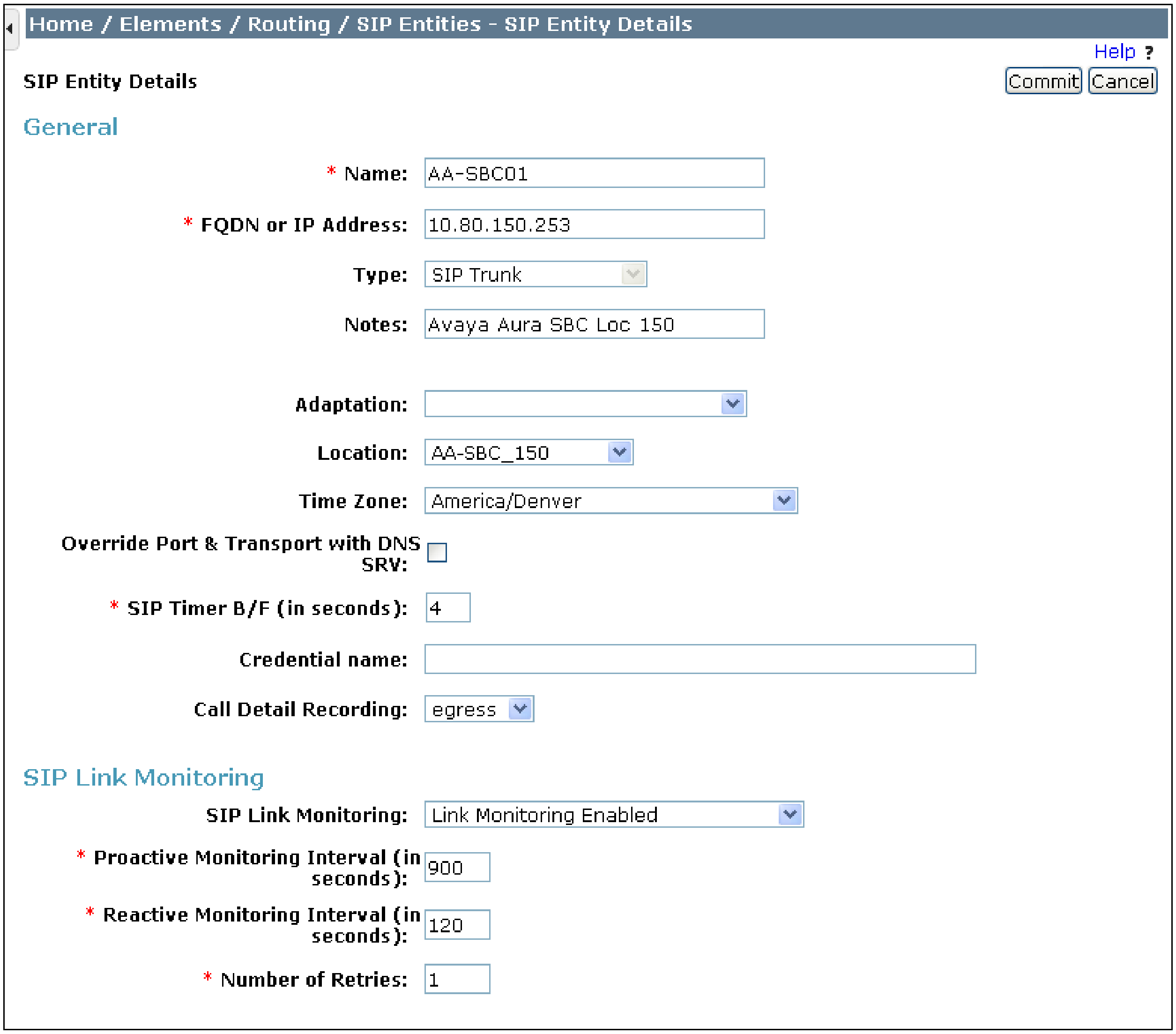
For the compliance test, four **Port** entries were added.



The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, a new SIP entity is created separate from the one created during the Session Manager installation for use with all other SIP traffic. The Location is set to the one defined for the Communication Manager in **Section 6.3.** The **FQDN or IP Address** field is set to the IP address of the Communication Manager Processor Ethernet.



The following screen shows the addition of the SBC SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for the SBC in **Section 6.3**. "**Link Monitoring Enabled"** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.



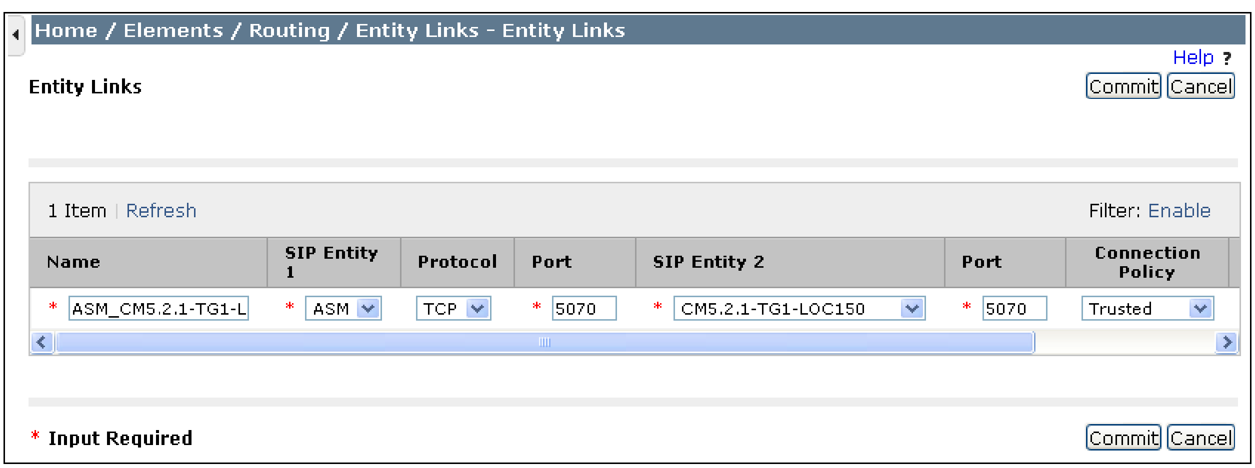
6.5. Add Entity Links

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

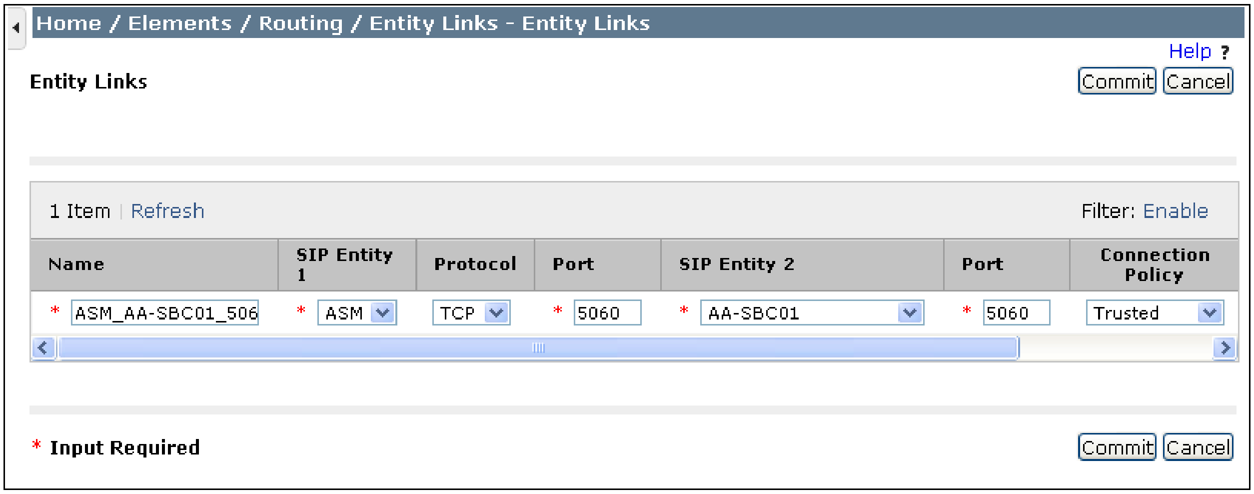
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group form in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group form in **Section 5.6**.
- **Trusted:** Check this box. ***Note**: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.*

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

Entity Link to Communication Manager:



Entity Link to the SBC:



6.6. Add Routing Policies

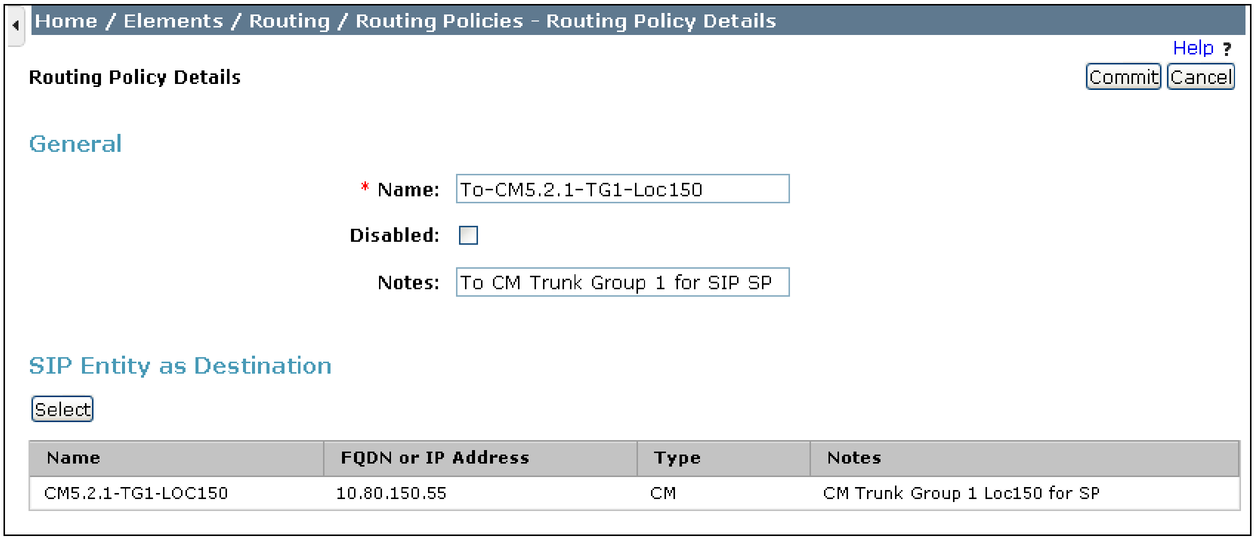
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added: One for Communication Manager and one for the SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

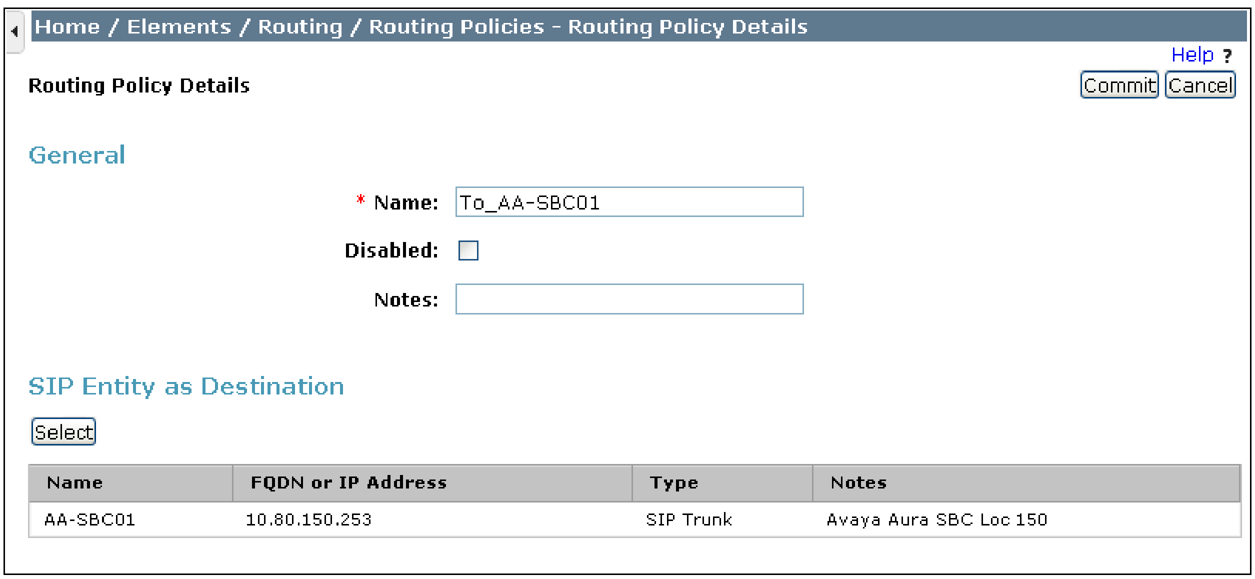
In the **General** section, enter the following values. Use default values for all remaining fields:

- **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** (not shown)**.** The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for the remaining fields. Click **Commit** to save.

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





6.7. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Level 3 Communications 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:

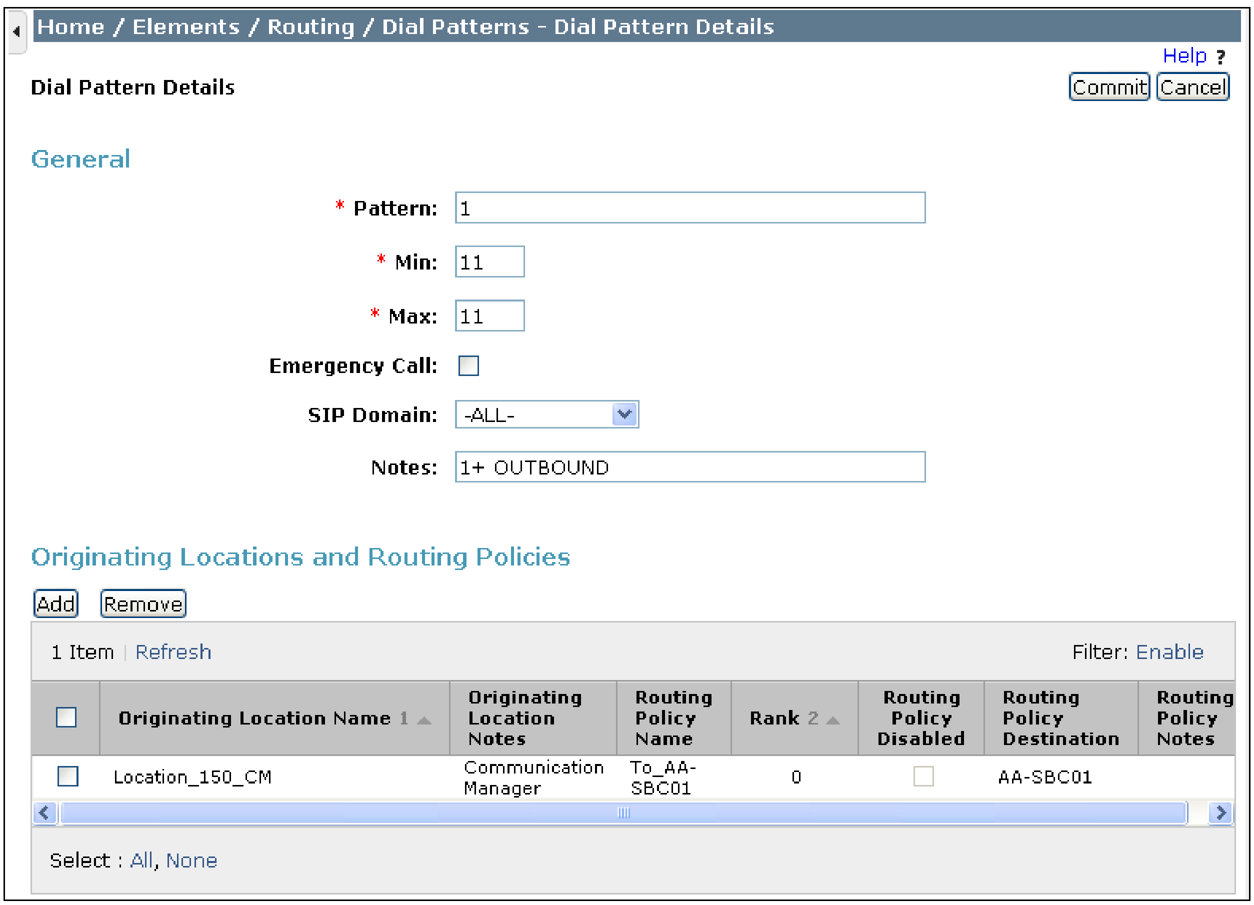
In the **General** section, enter the following values. Use default values for all remaining fields:

- **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, or select **-all-**.
- **Notes:** Add a brief description (optional).

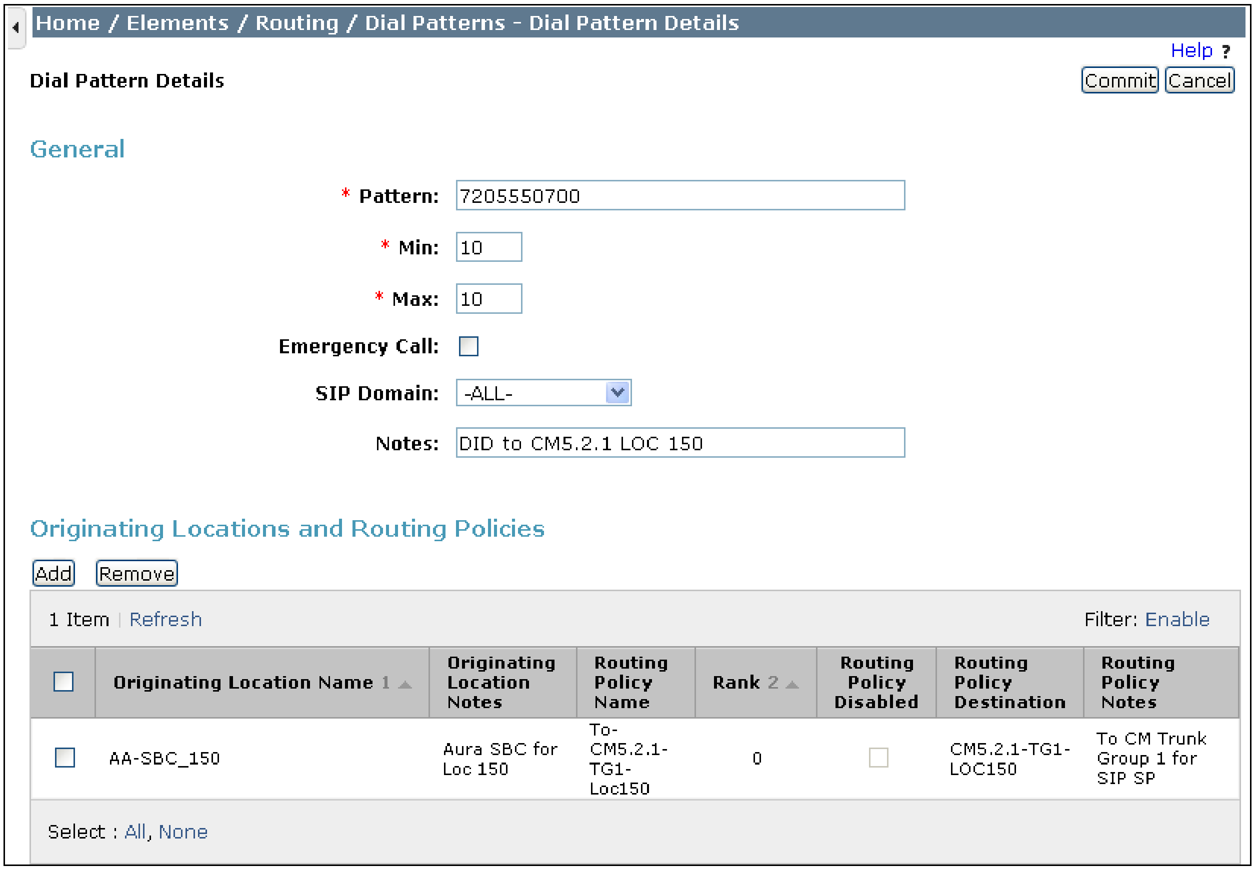
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that **11** digit dialed numbers that begin with **1** originating from **Location_150_CM** uses the route policy **To_AA-SBC01**.



The second example shows that a 10 digit number **"7205550700"** and originating from **AA-SBC_150** uses route policy **To-CM5.2.1-TG1-LOC150**. This is a DID number assigned to the enterprise from Level 3 Communications.



6.8. Verify Avaya Aura® Session Manager Instance

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

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

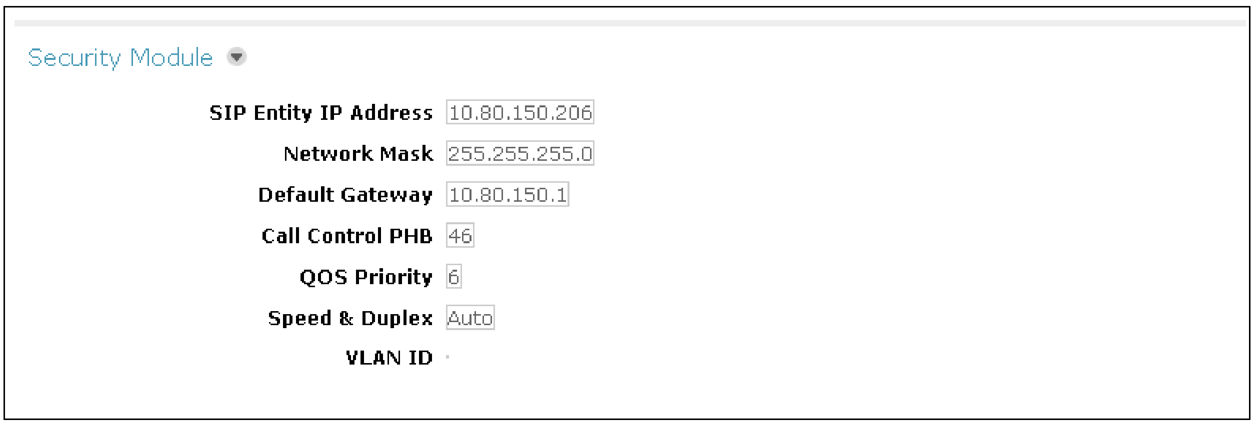
- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

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

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

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

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



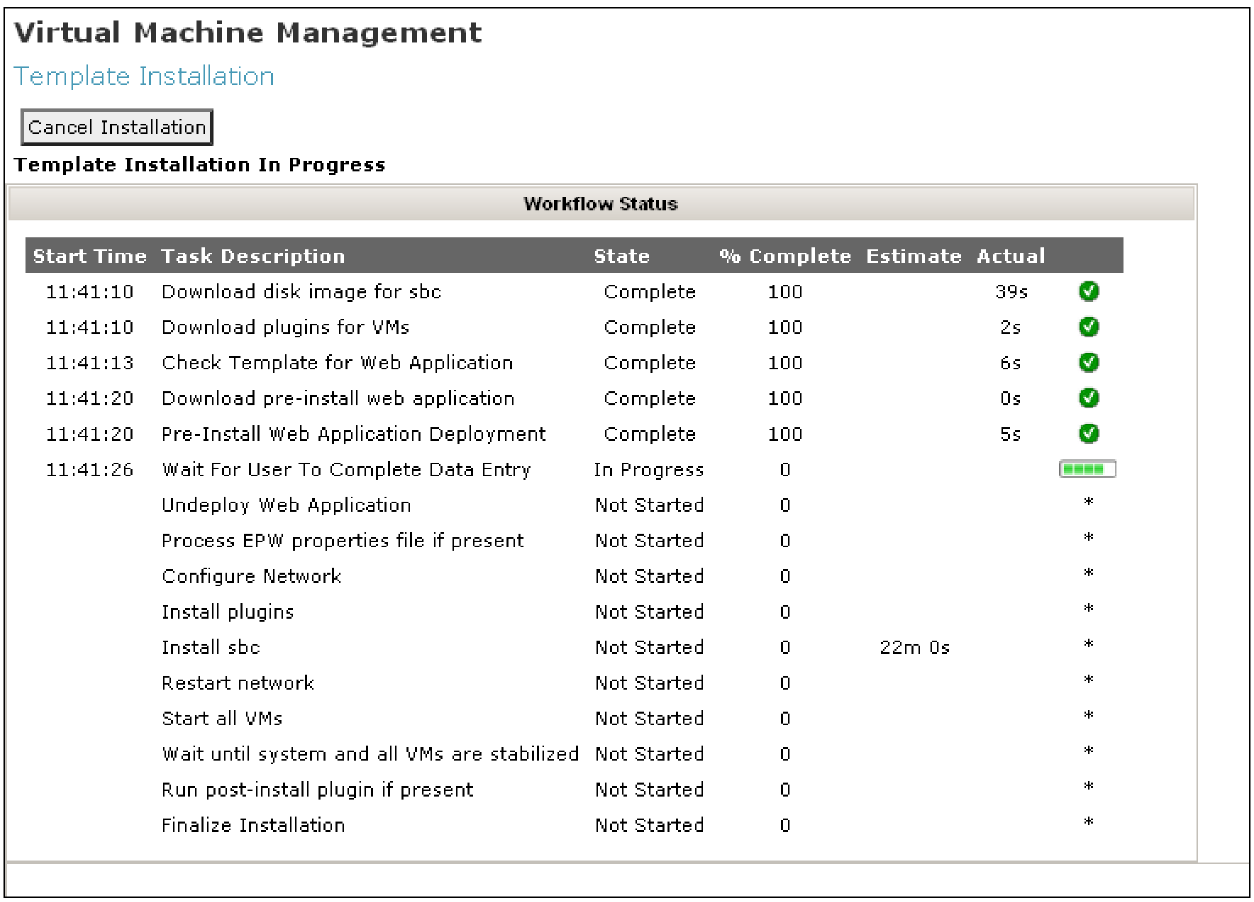
7. Configure Session Border Controller

This section describes the configuration of the Avaya Aura® Session Border Controller (SBC). This configuration is done in two parts. The first part is done during the SBC installation via the installation wizard. These Application Notes will not cover the 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 SBC template see [1] and [8].

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

7.1. Installation Wizard

During the installation of the SBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the SBC. When it gets to "Wait for User to Complete Data Entry" (shown below), it will open another window for input. It may be necessary to enable pop-ups to view.



Virtual Machine Management

Template Installation

Cancel Installation

Template Installation In Progress

Workflow Status

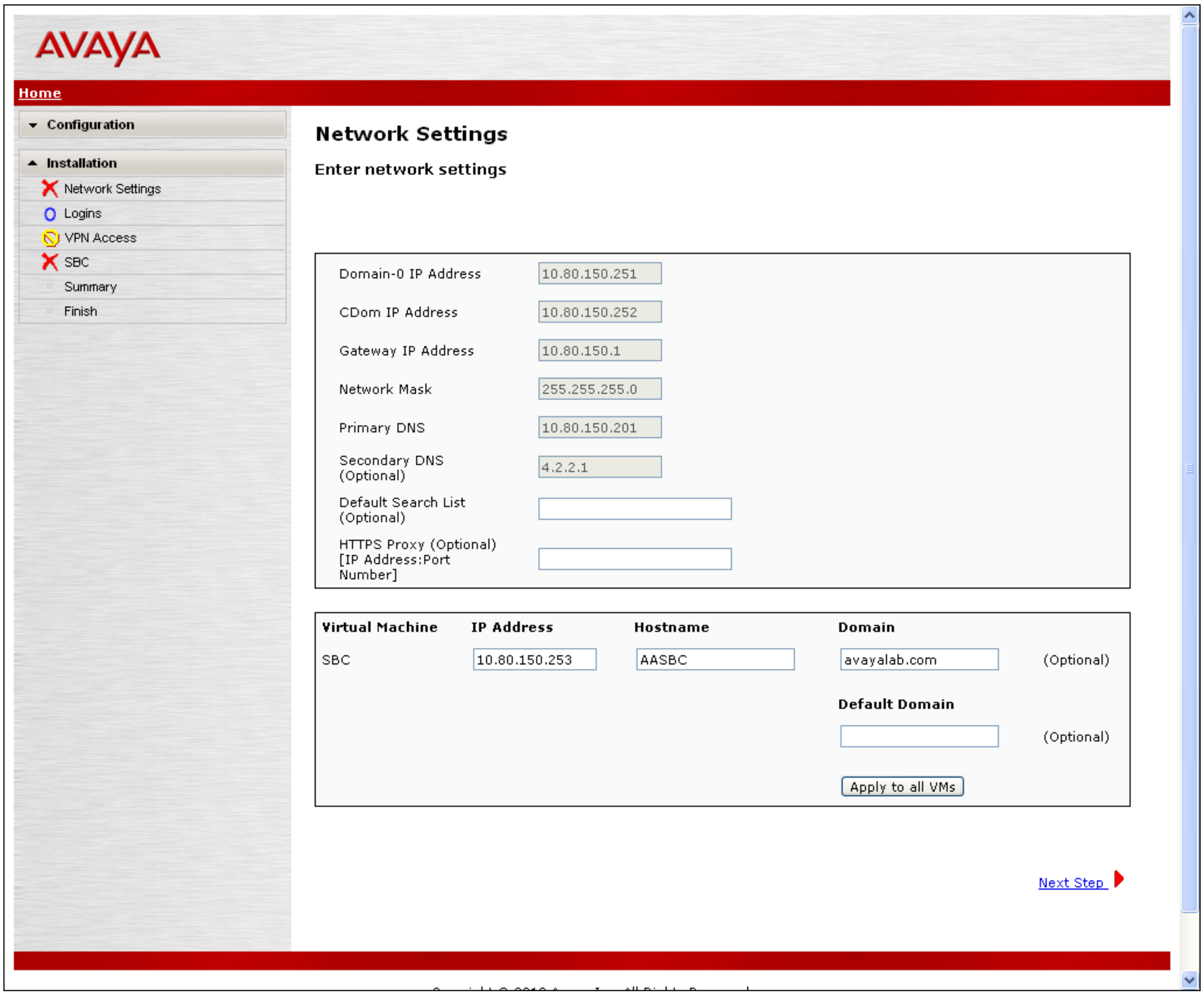
Start Time	Task Description	State	% Complete	Estimate	Actual	
11:41:10	Download disk image for sbc	Complete	100		39s	
11:41:10	Download plugins for VMs	Complete	100		2s	
11:41:13	Check Template for Web Application	Complete	100		6s	
11:41:20	Download pre-install web application	Complete	100		0s	
11:41:20	Pre-Install Web Application Deployment	Complete	100		5s	
11:41:26	Wait For User To Complete Data Entry	In Progress	0			
	Undeploy Web Application	Not Started	0			*
	Process EPW properties file if present	Not Started	0			*
	Configure Network	Not Started	0			*
	Install plugins	Not Started	0			*
	Install sbc	Not Started	0	22m 0s		*
	Restart network	Not Started	0			*
	Start all VMs	Not Started	0			*
	Wait until system and all VMs are stabilized	Not Started	0			*
	Run post-install plugin if present	Not Started	0			*
	Finalize Installation	Not Started	0			*

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 SBC.
- **Hostname**: Enter a host name for the SBC.
- **Domain**: Enter the domain used for the enterprise. This should match the Domain set in Session Manager (**Section 6.2**) and the Communication Manager signaling group Far-end Domain (**Section 5.6**).

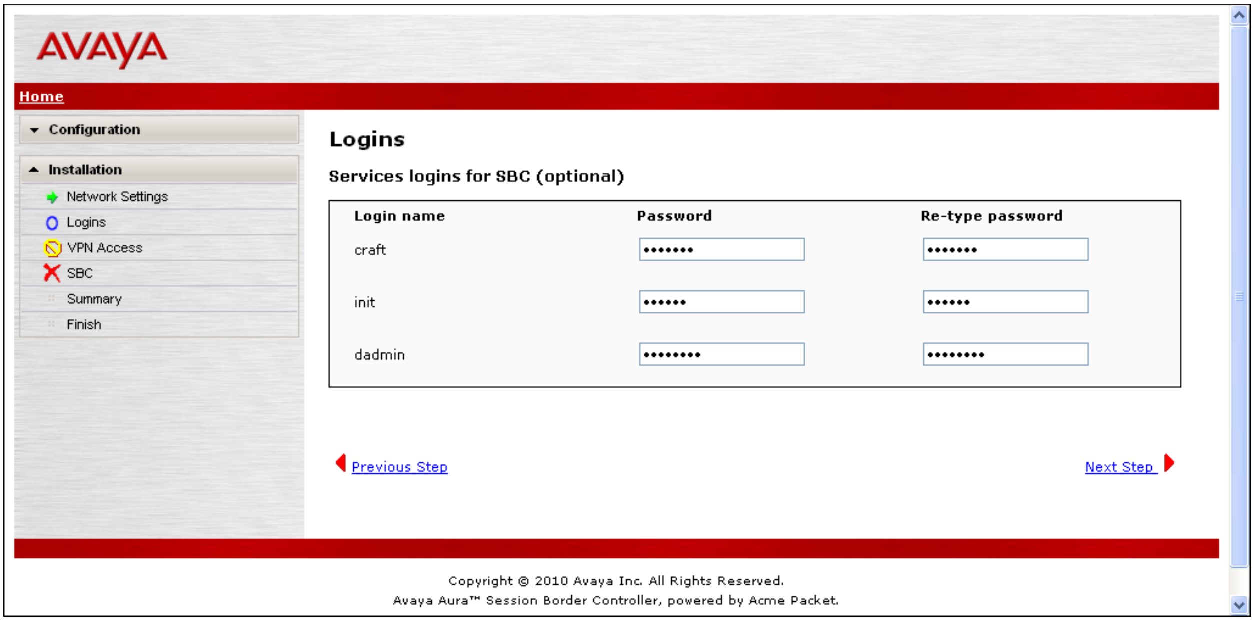
Click **Next Step** to continue.



7.1.2. Logins

The **Services Logins for SBC (optional)** screen is where passwords for the various User login credentials are set. Assign passwords for the different accounts.

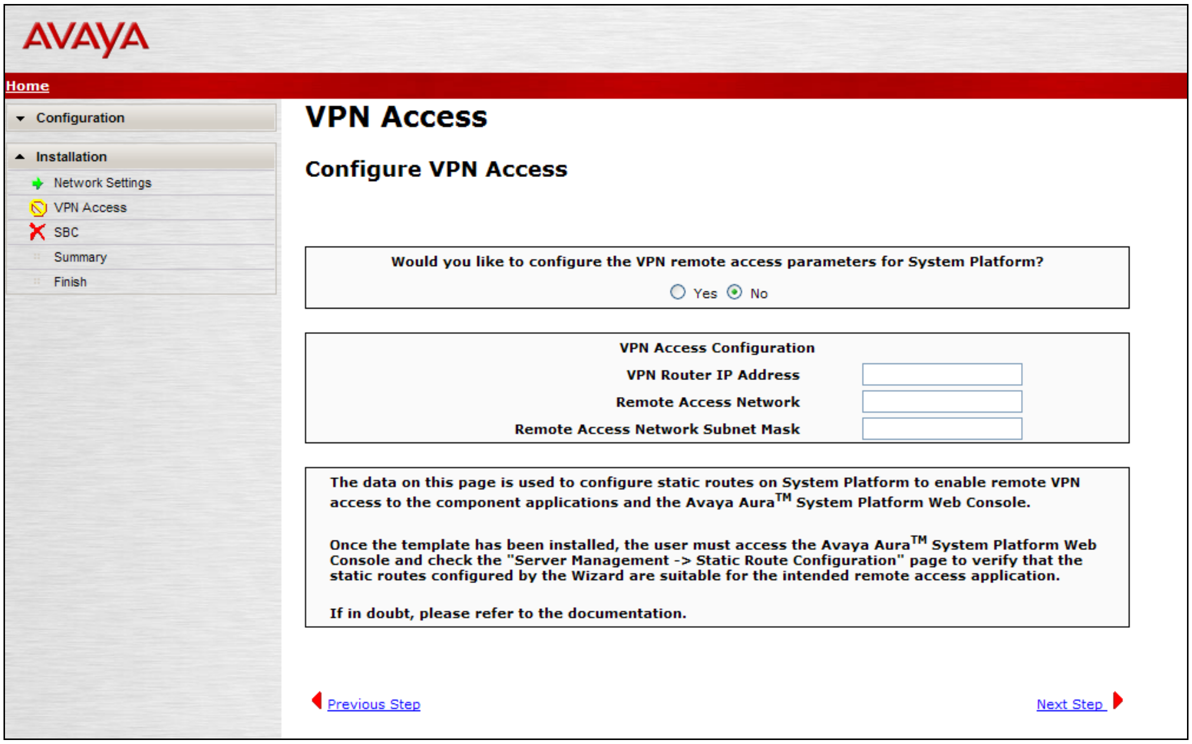
Click **Next Step** to continue.



7.1.3. VPN Access

VPN remote access to the 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.



7.1.4. 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 create a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for Level 3. Thus, "**Generic"** was chosen instead and further customization was done manually after the wizard was complete.
- **IP Address**: Enter the IP address of the SIP proxy of the service provider. If the service provider has multiple proxies, enter the primary proxy on this screen and additional proxies can be added after installation.
- **Port**: Enter the port number that the service provider uses to listen for SIP traffic.
- **Media Network**: Enter the network address of the network where media traffic will originate from the service provider. 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**.

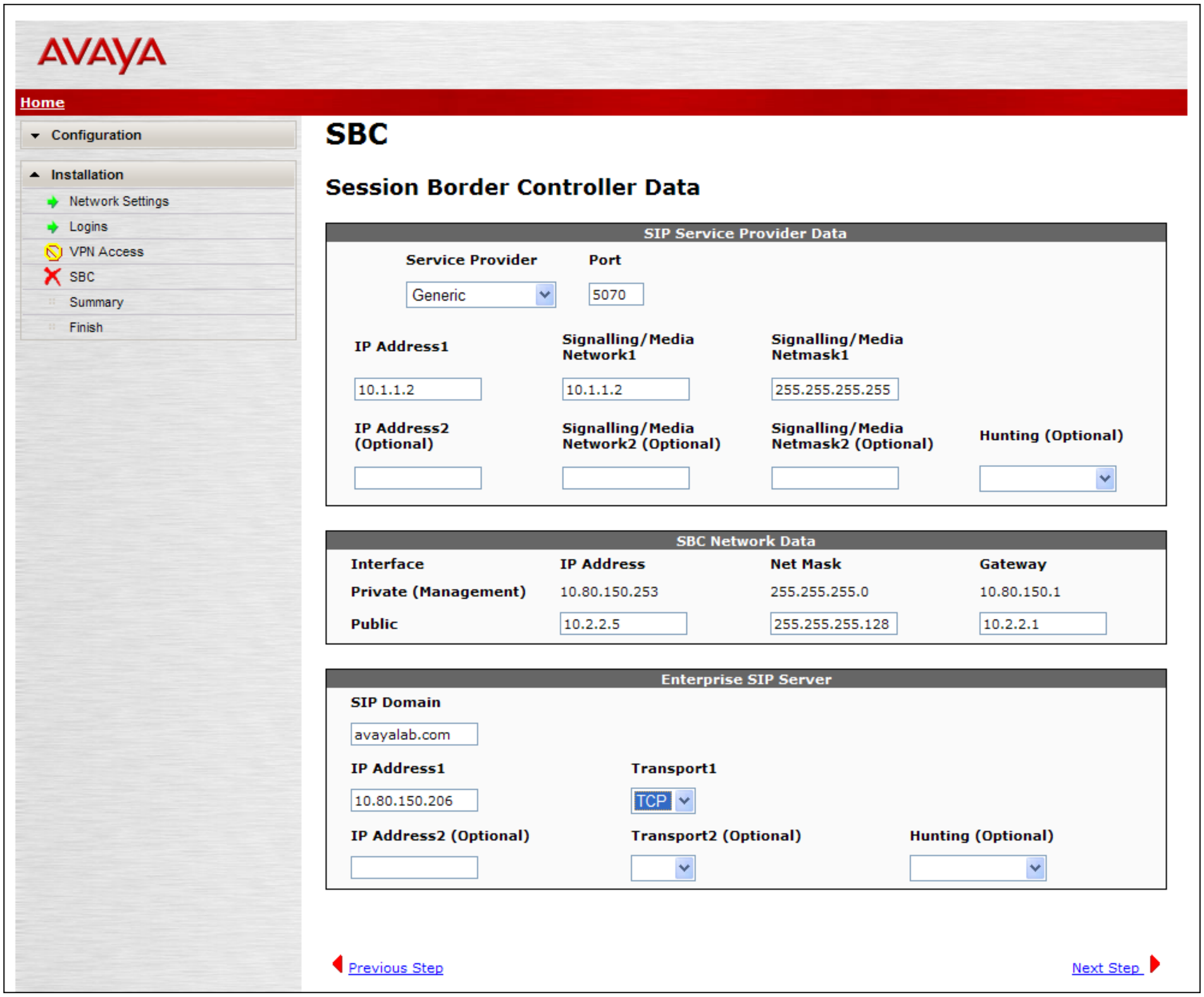
In the **SBC Network Data** section:

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

In the **Enterprise SIP Server** section:

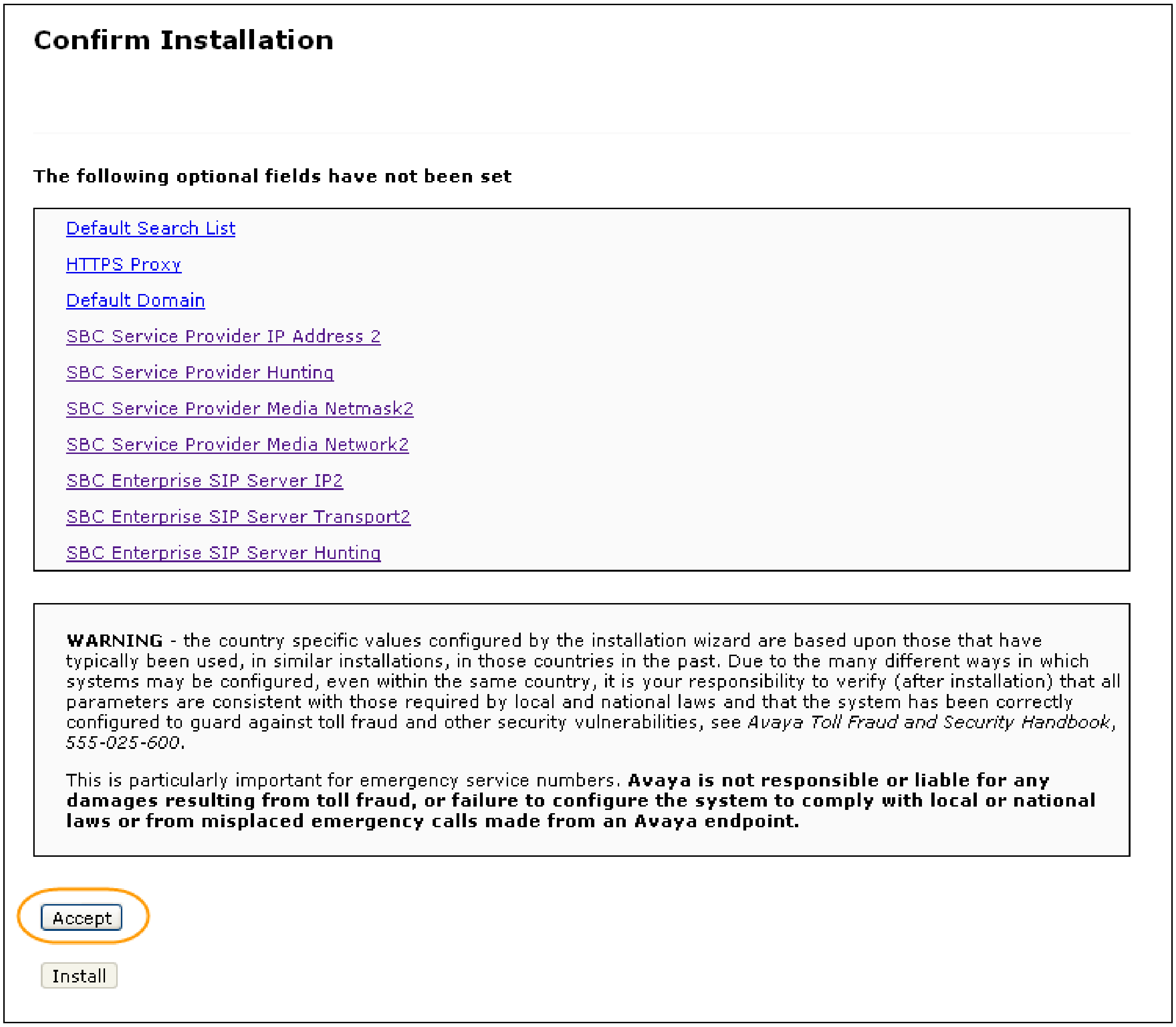
- **IP Address**: Enter the IP address of the Enterprise SIP Server to which the SBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface.
- **Transport**: From the pull-down menu, select the transport protocol to be used for SIP traffic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

Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to continue to the final step.


AVAYA
Home
Configuration
Installation
Network Settings
Logins
VPN Access
SBC
Summary
Finish
SBC
Session Border Controller Data
SIP Service Provider Data
Service Provider
Port
Generic
5070
IP Address1
Signalling/Media Network1
Signalling/Media Netmask1
10.1.1.2
10.1.1.2
255.255.255.255
IP Address2 (Optional)
Signalling/Media Network2 (Optional)
Signalling/Media Netmask2 (Optional)
Hunting (Optional)
SBC Network Data
Interface
IP Address
Net Mask
Gateway
Private (Management)
10.80.150.253
255.255.255.0
10.80.150.1
Public
10.2.2.5
255.255.255.128
10.2.2.1
Enterprise SIP Server
SIP Domain
avayalab.com
IP Address1
Transport1
10.80.150.206
TCP
IP Address2 (Optional)
Transport2 (Optional)
Hunting (Optional)
Previous Step
Next Step

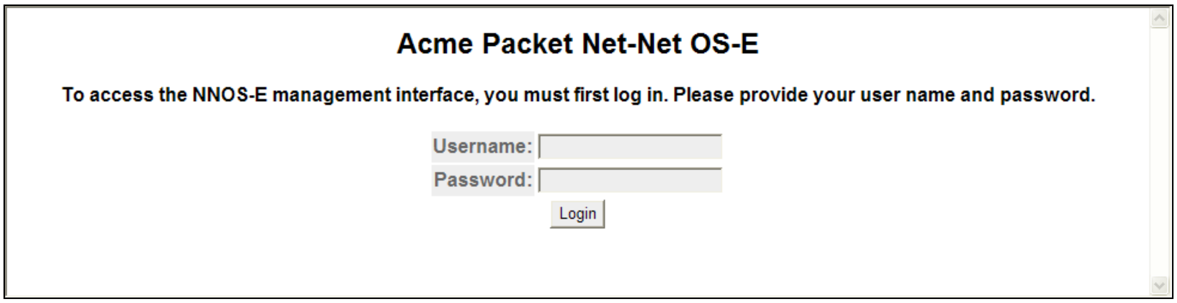
7.1.5. Confirm Installation

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.



7.2. Post Installation Configuration

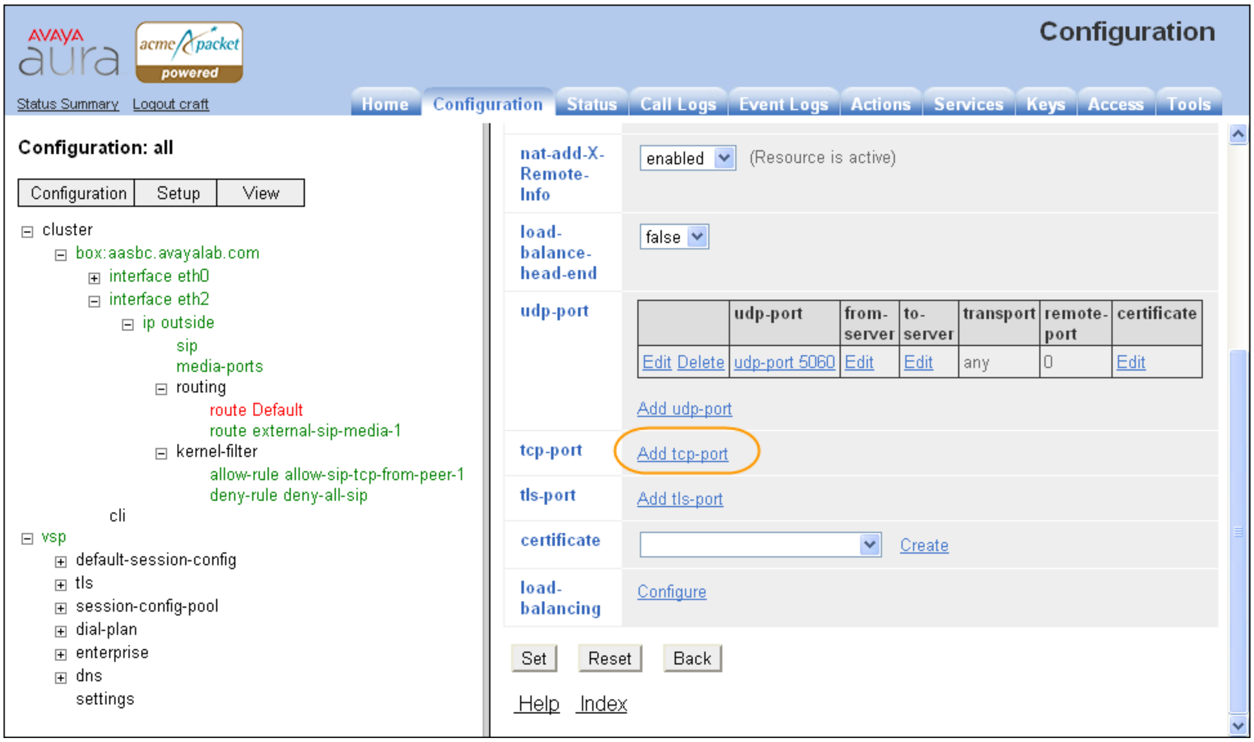
The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 7.1.4.** Since the "**Generic"** template had to be selected in the installation wizard, additional manual changes must also be performed. These changes are performed by accessing the browser-based GUI of the Session Border Controller, using the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 7.1.1**. Log in with the appropriate credentials set in **Section 7.1.2**.



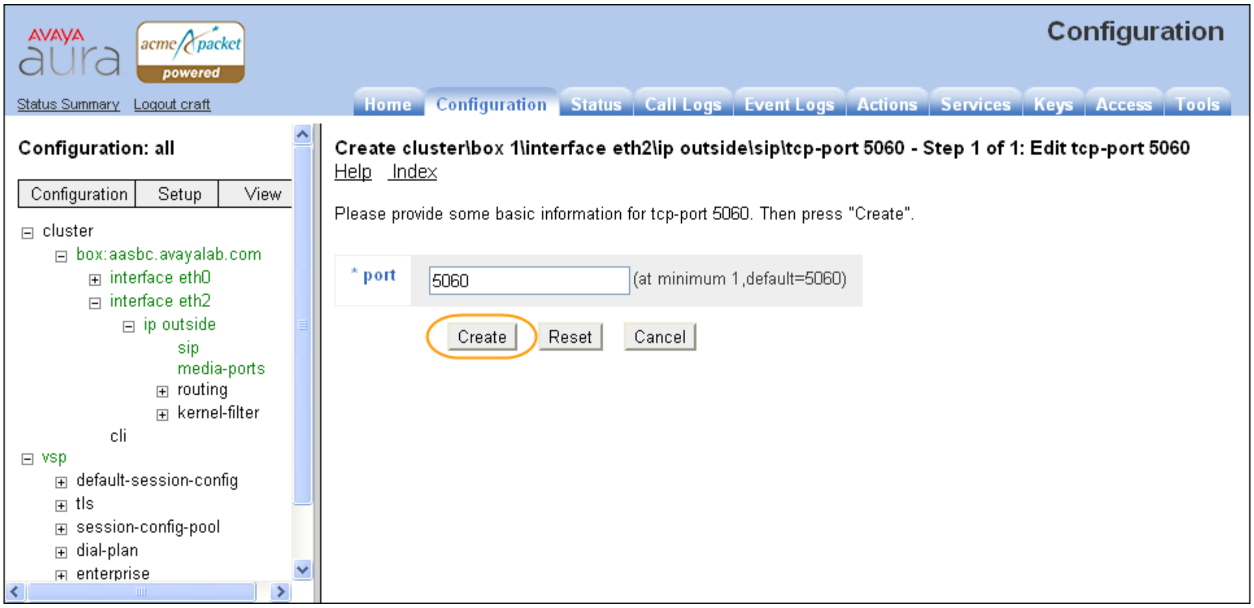
7.2.1. TCP Transport

Level 3 Communications requires SIP calls that are routed over the public Internet to use TCP transport. The installation wizard sets the SIP transport to UDP, thus changes to the configuration are necessary to send SIP over TCP.

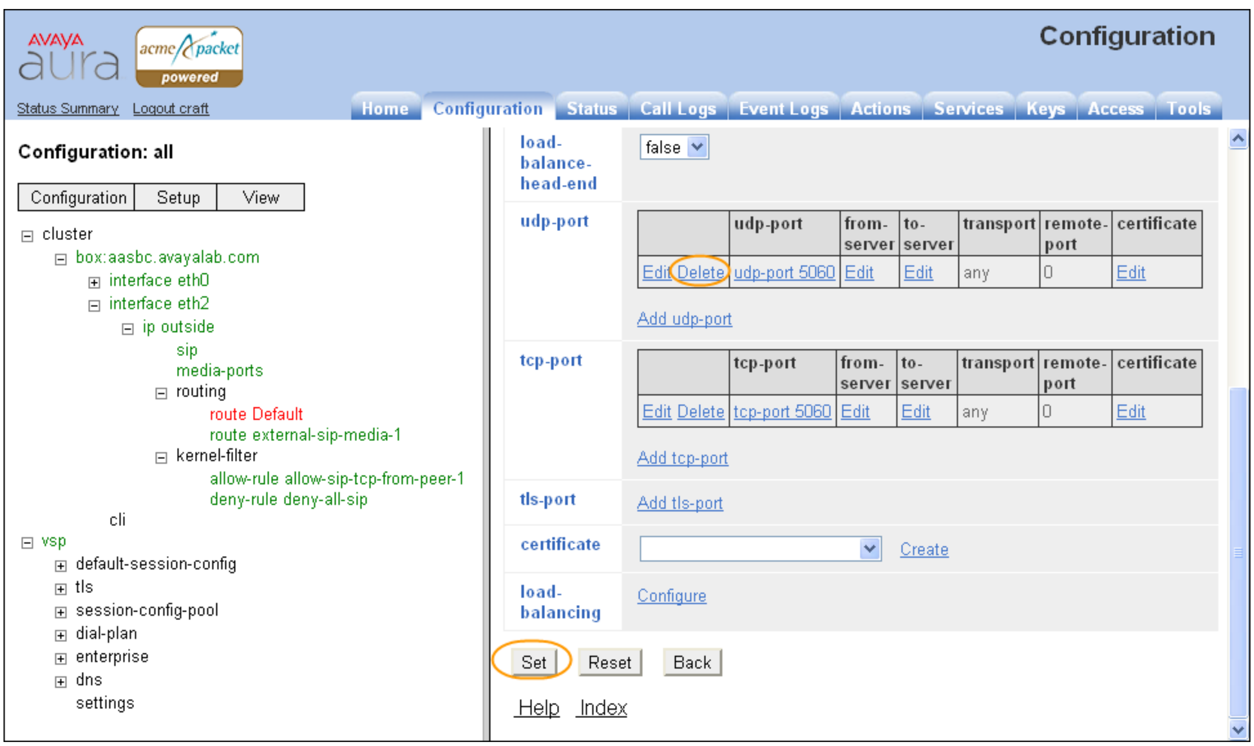
To change the transport to TCP, first navigate to **cluster → box:<server> → interface eth2 → ip outside → sip,** where <**server**> is the FQDN of the server created during the installation process. Scroll down and click **Add tcp-port**.



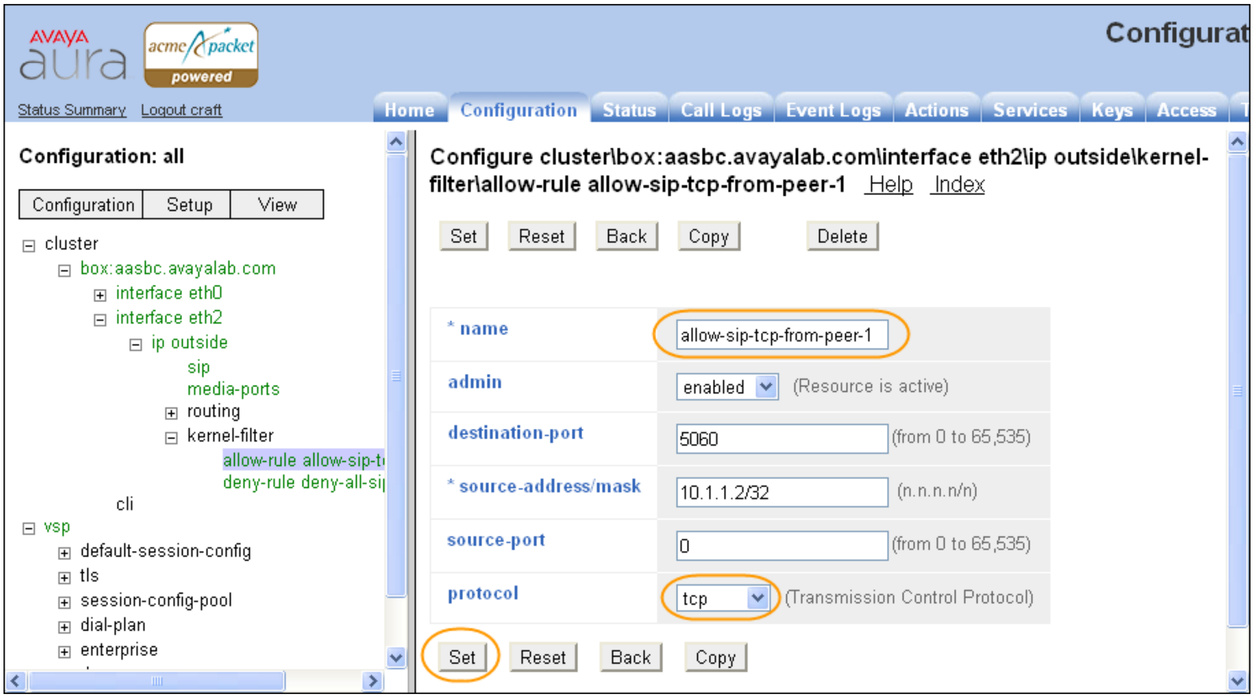
Keep the default "**5060**" in the **port** field and click **Create**.



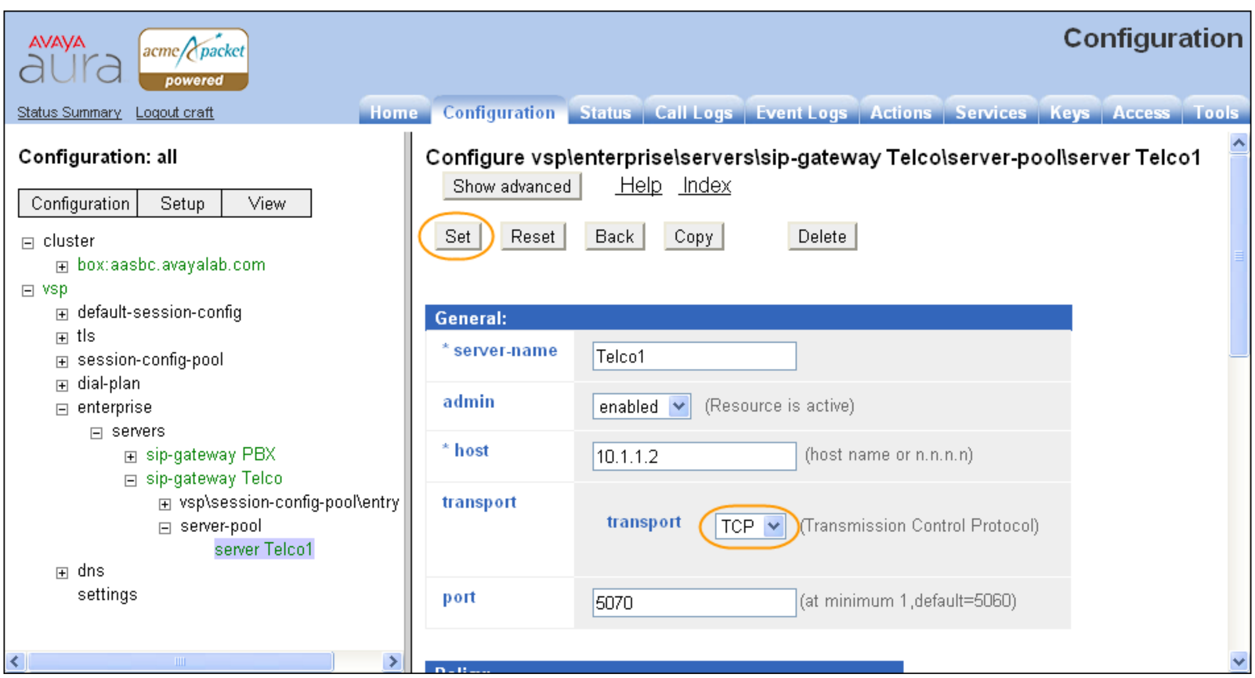
In the right pane that appears, scroll down and click **Delete** next to the **udp-port** field. Click OK to confirm deletion in the popup box (not shown). Click **Set** to complete the configuration.



Next navigate to **cluster → box <server> → interface eth2 → ip outside → kernel-filter → allow-rule allow-sip-udp-from-peer-1.** Change the name to "**allow-sip-tcp-from-peer-1**". Set the **protocol** field to "**tcp**". Click **Set** to complete the configuration.

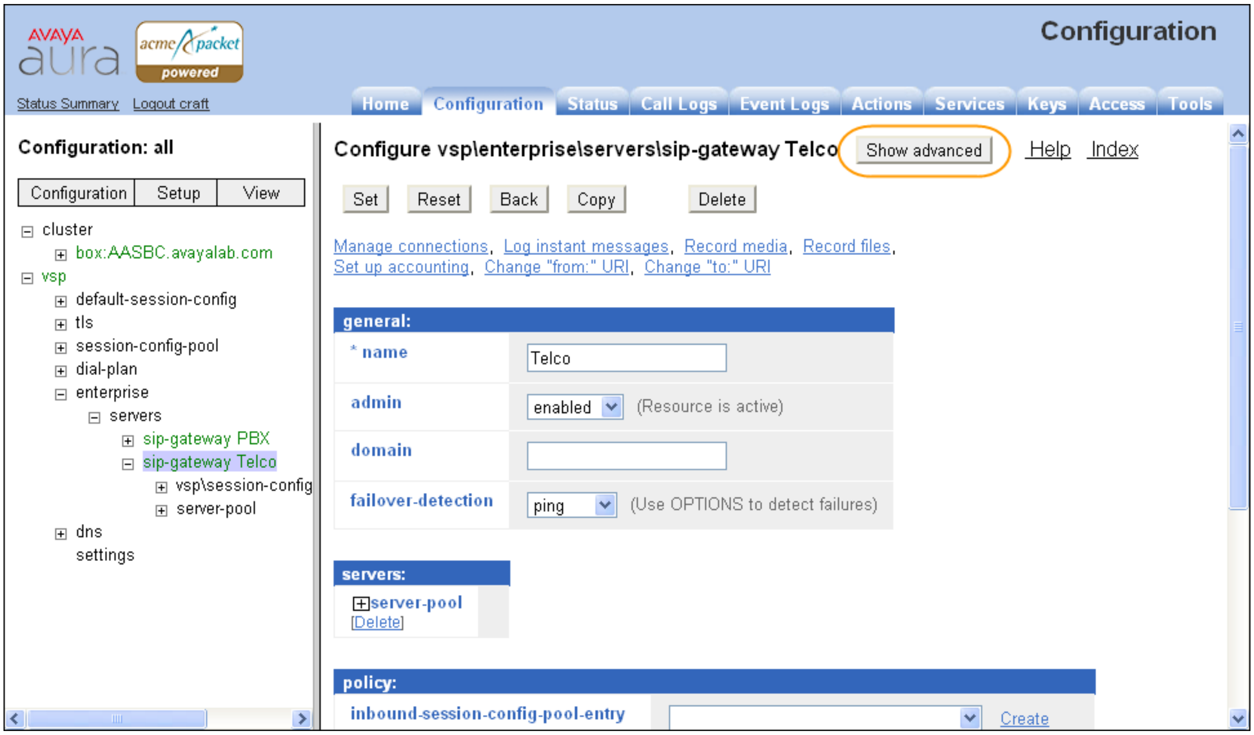


Next navigate to **vsp → enterprise → servers → sip-gateway Telco → server-pool → server Telco1.** Change the transport field to "**TCP**". Click **Set** to complete the configuration.

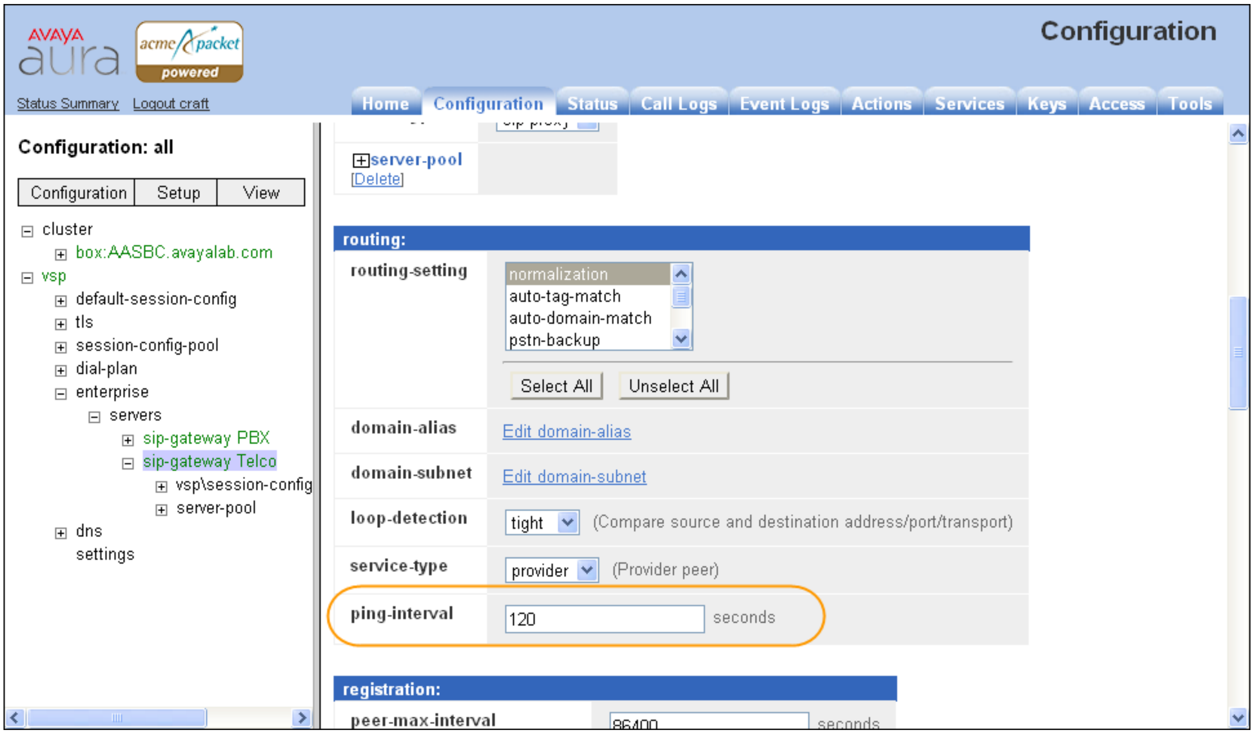


7.2.2. Options Frequency

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

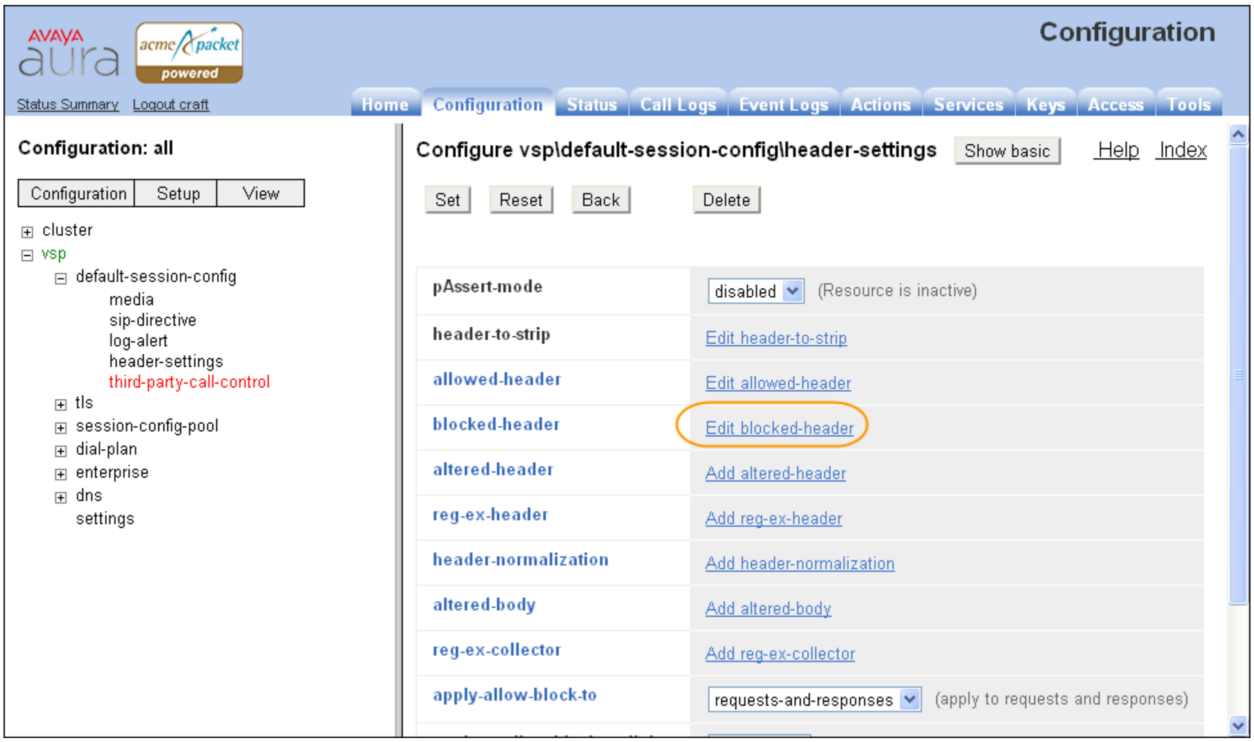


Scroll down to the **routing** section of the form. Enter the desired SIP OPTION ping interval in the **ping-interval** field, in seconds. Click **Set** at the top of the form (shown in previous figure).

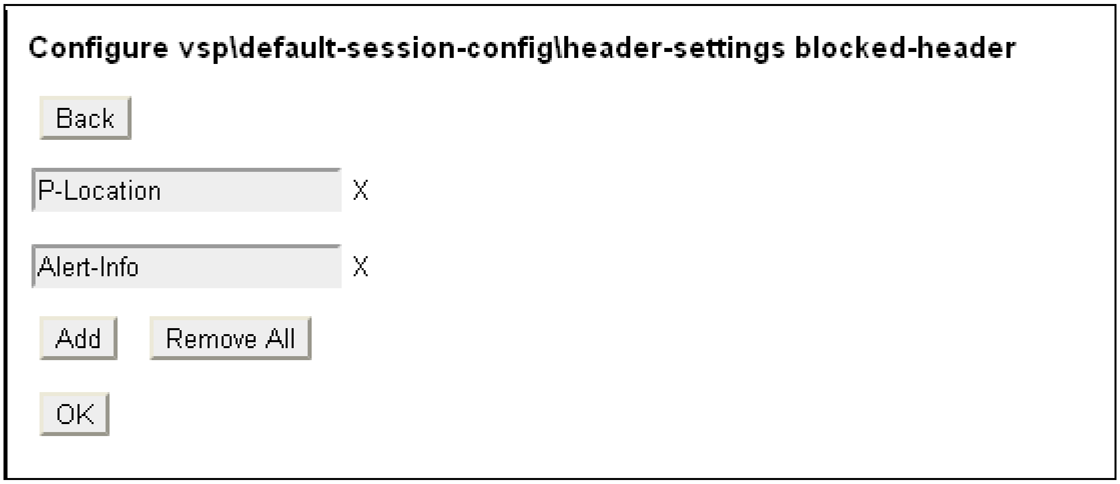


7.2.3. Blocked Headers

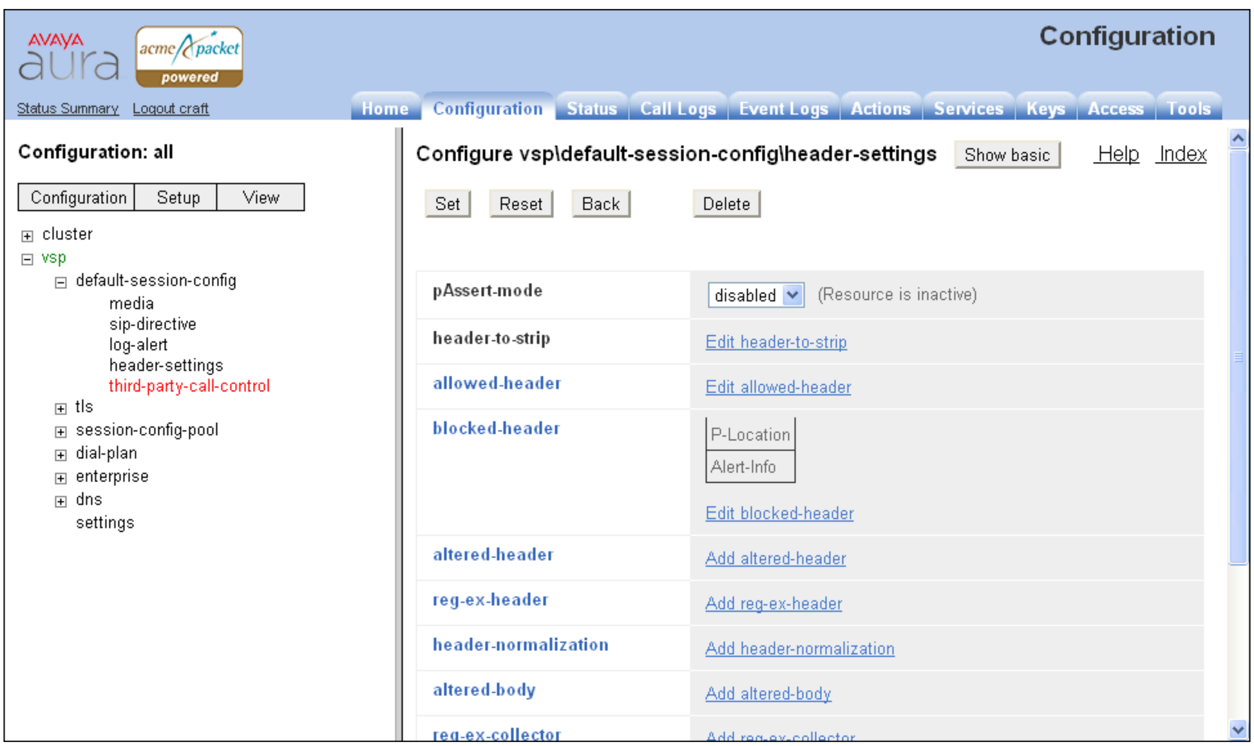
The P-Location and Alert-Info headers are sent in SIP messages from Session Manager to the Level 3 network. These headers contain either private IP addresses or private domains from the enterprise. These should not be exposed externally. For simplicity, these headers were simply removed (blocked) from both requests and responses for both inbound and outbound calls. To create a rule for blocking headers, first navigate to **vsp → default-session-config → header-settings**. Click **Edit blocked-header**.



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

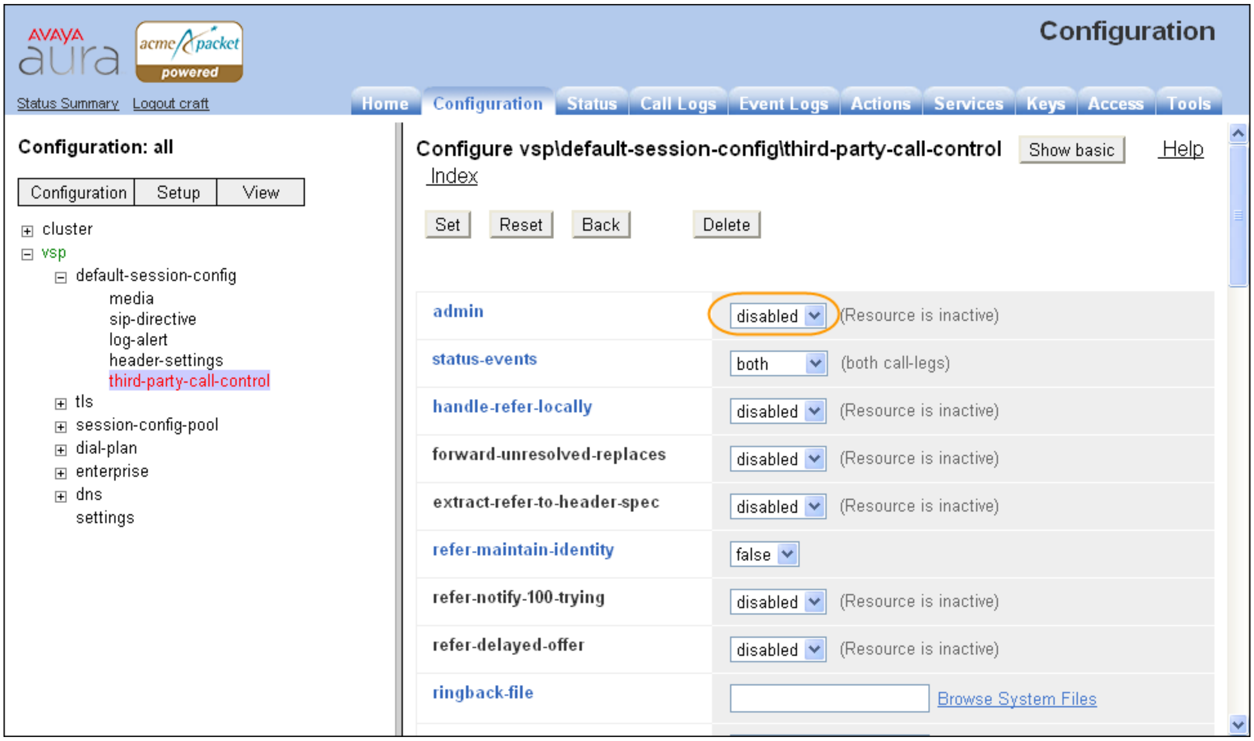


The list of blocked headers for outbound calls will appear in the right pane as shown below. Click **Set** to complete the configuration.



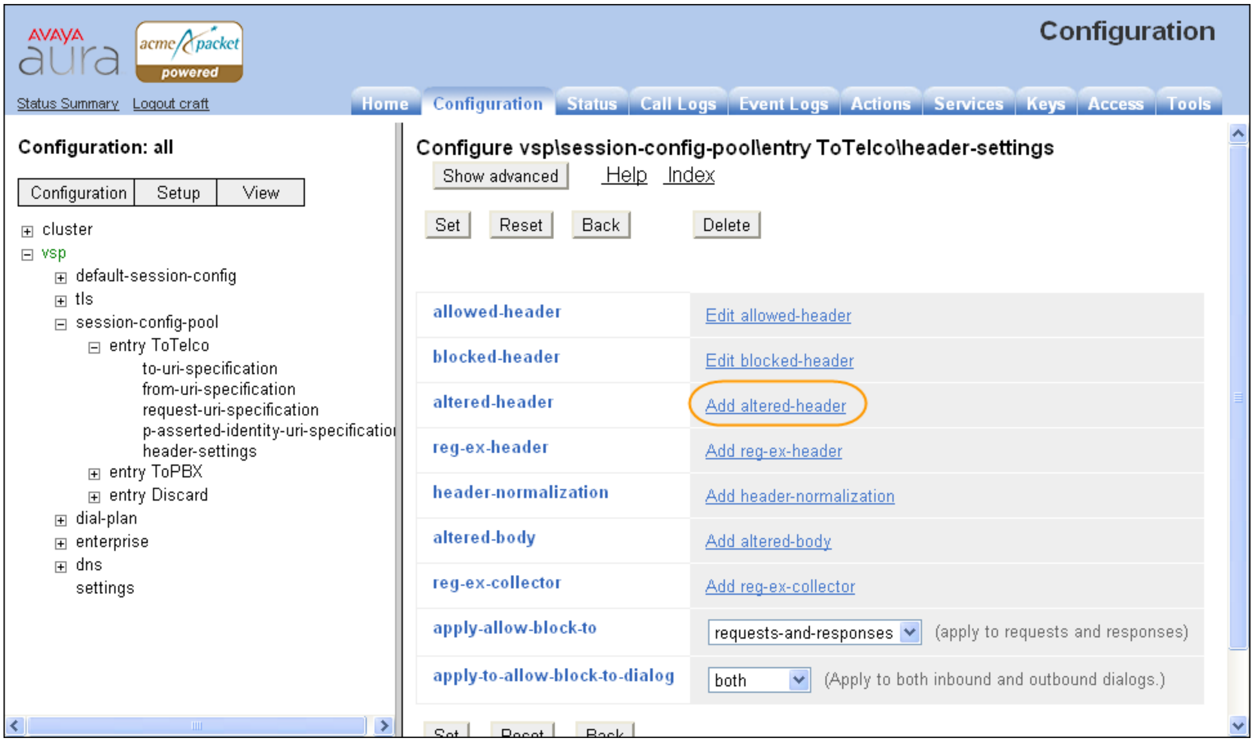
7.2.4. Third Party Call Control

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



7.2.5. Diversion Header

A Diversion Header is applied to forwarded off-net calls when the SIP trunk group on Communication Manager has Send Diversion Header set to "yes" (**Section 5.7**). The Diversion Header will contain the number associated with the Enterprise user, allowing Level 3 Communications to admit the call, and the From Header will be populated with the true calling party identity, allowing the forwarded destination to see the true caller ID. For the host portion of the header, Communication Manager sends the information entered in the signaling group Far-end Domain field **(Section 5.6).** To prevent this information from being exposed externally, the SBC can modify the header and replace the Domain name with the IP address of the Level 3 Communication's Managed IP Telephony Service. To create a rule to modify the Diversion Header, first navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. Click **Add altered-header**.

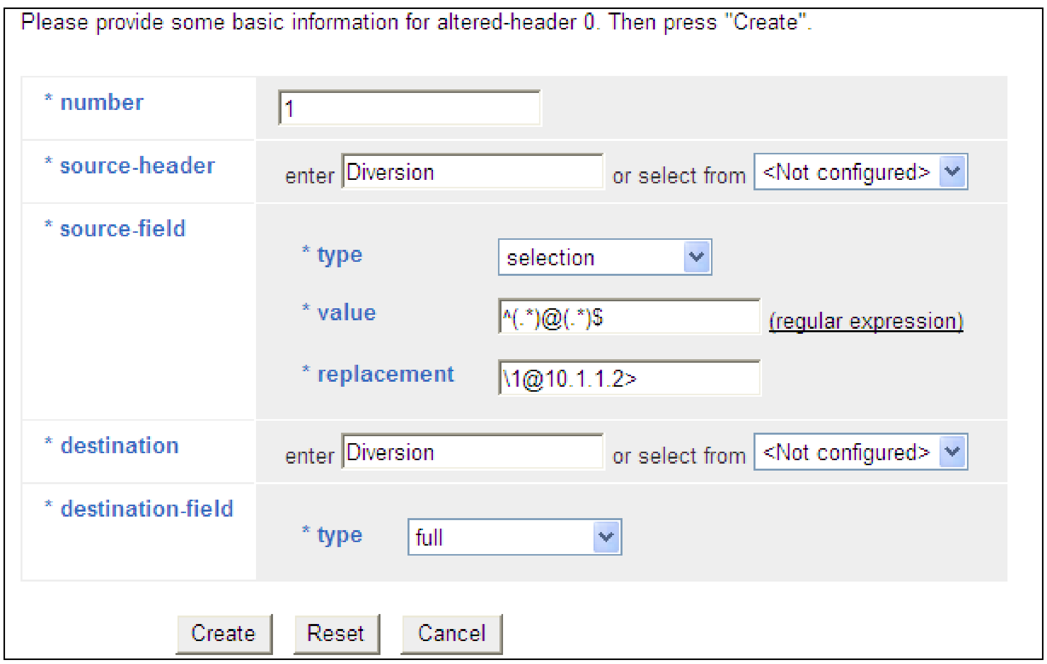

Configuration
Status Summary
Logout craft
Home
Configuration
Status
Call Logs
Event Logs
Actions
Services
Keys
Access
Tools
Configuration: all
Configuration
Setup
View
cluster
vsp
default-session-config
tls
session-config-pool
entry ToTelco
to-uri-specification
from-uri-specification
request-uri-specification
p-asserted-identity-uri-specificatio
header-settings
entry ToPBX
entry Discard
dial-plan
enterprise
dns
settings
Configure vsp\session-config-pool\entry ToTelco\header-settings
Show advanced
Help
Index
Set
Reset
Back
Delete
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
altered-body
Add altered-body
reg-ex-collector
Add reg-ex-collector
apply-allow-block-to
requests-and-responses
(apply to requests and responses)
apply-to-allow-block-to-dialog
both
(Apply to both inbound and outbound dialogs.)

In the right pane that appears, enter “**1”** in the **number** field and enter **“Diversion”** in the s**ource-header** field. In the **source-field** area, next to **type** choose “**selection”** from the drop-down list.

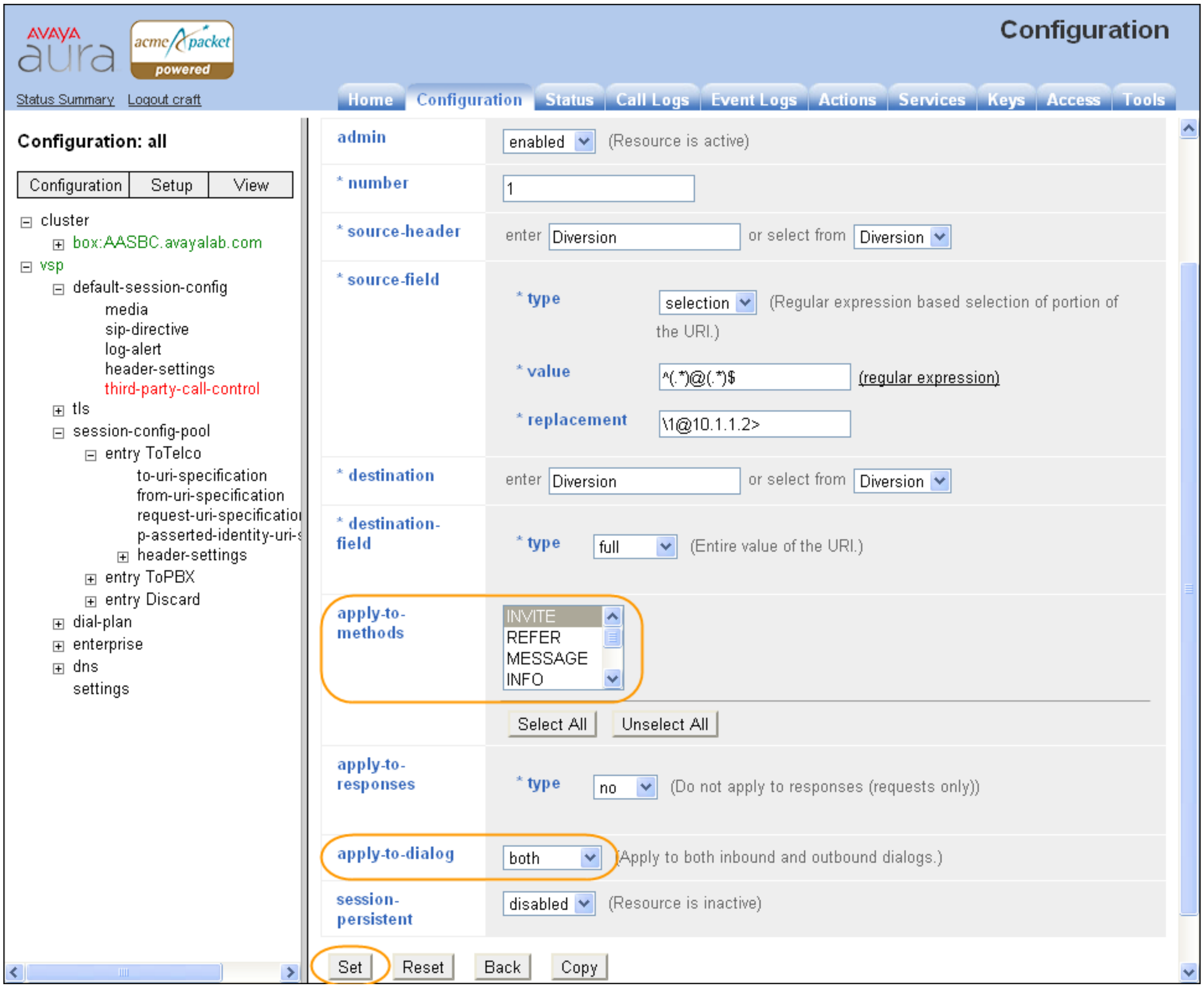
In the **value** field, enter a regular expression to match. In the sample configuration, **“^(.*)@(.*)$”** was entered. In this expression, the first (.*) will match and store any user part of the Diversion header. The second instance of (.*) matches and stores any host part of the header.

In the **replacement** field, **“\1@10.1.1.2>”** was entered in the sample configuration. The variable “\1” is the stored user part from the original Diversion header containing the number associated with the DID. The IP Address 10.1.1.2 is the IP Address of Level 3 Communications SIP Trunk and will be added as the Host part replacement string for the Diversion header.

In the **destination** field enter **“Diversion”**. Select “**full**” for **type** in the **destination-field** section and click **Create**.



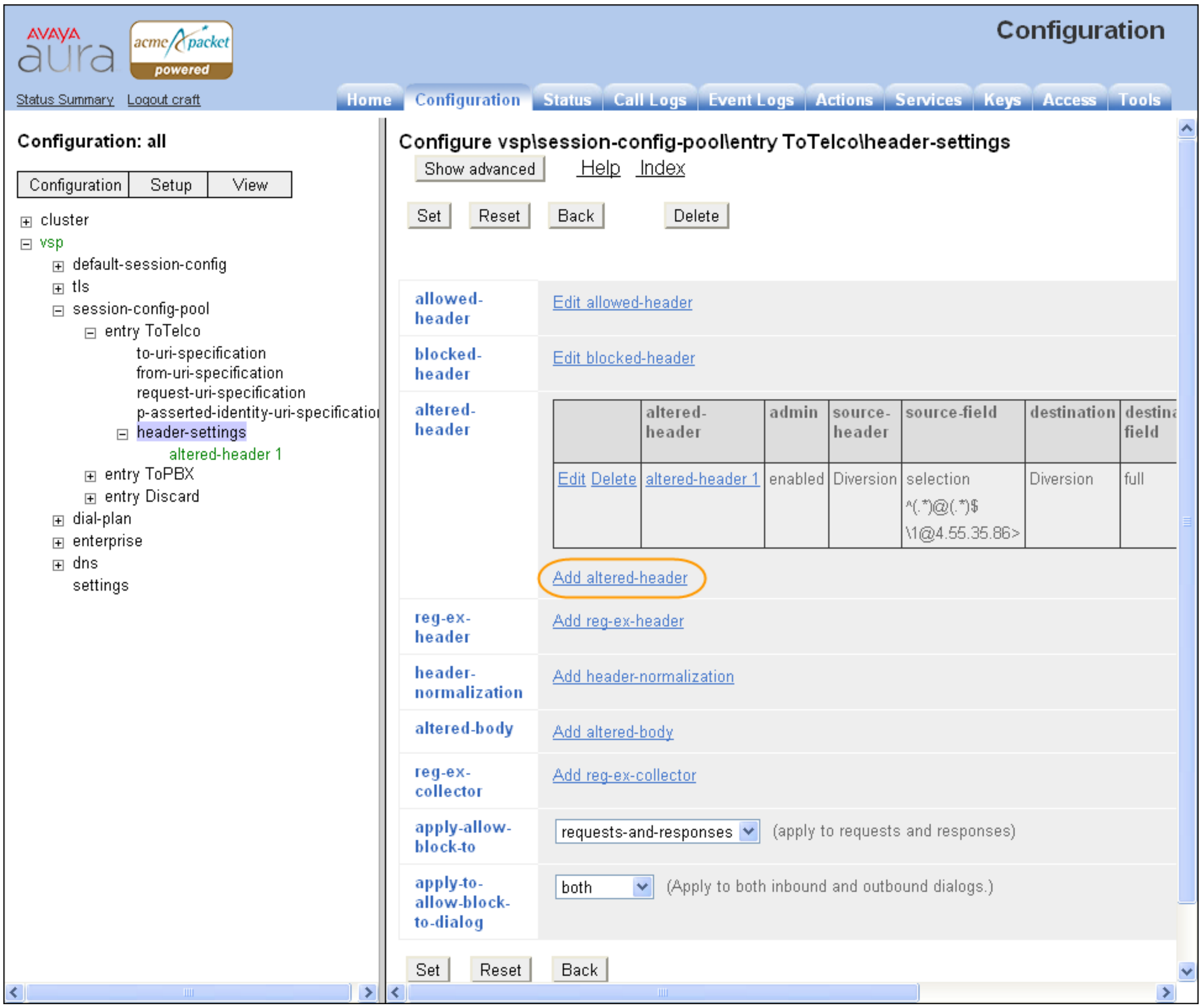
The following screen is presented, select "**INVITE**" for **apply-to-methods** and "**both**" in the **apply-to-dialog** section. Click **Set** to complete the configuration.



7.2.6. Remote-Party-ID

When the Calling Party Number is blocked by Communication Manager, Level 3 Communications needs to see a valid number in the Remote Party-ID header to allow the call to go through. Communication Manager sends a valid number in the P-Asserted-Identity header instead of the Remote-Party-ID header. The SBC can be used to take the information sent in the P-Asserted-Identity header and create a Remote-Party-ID header.

To have the SBC create a Remote-Party-ID header, first navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. Click **Add altered-header**.

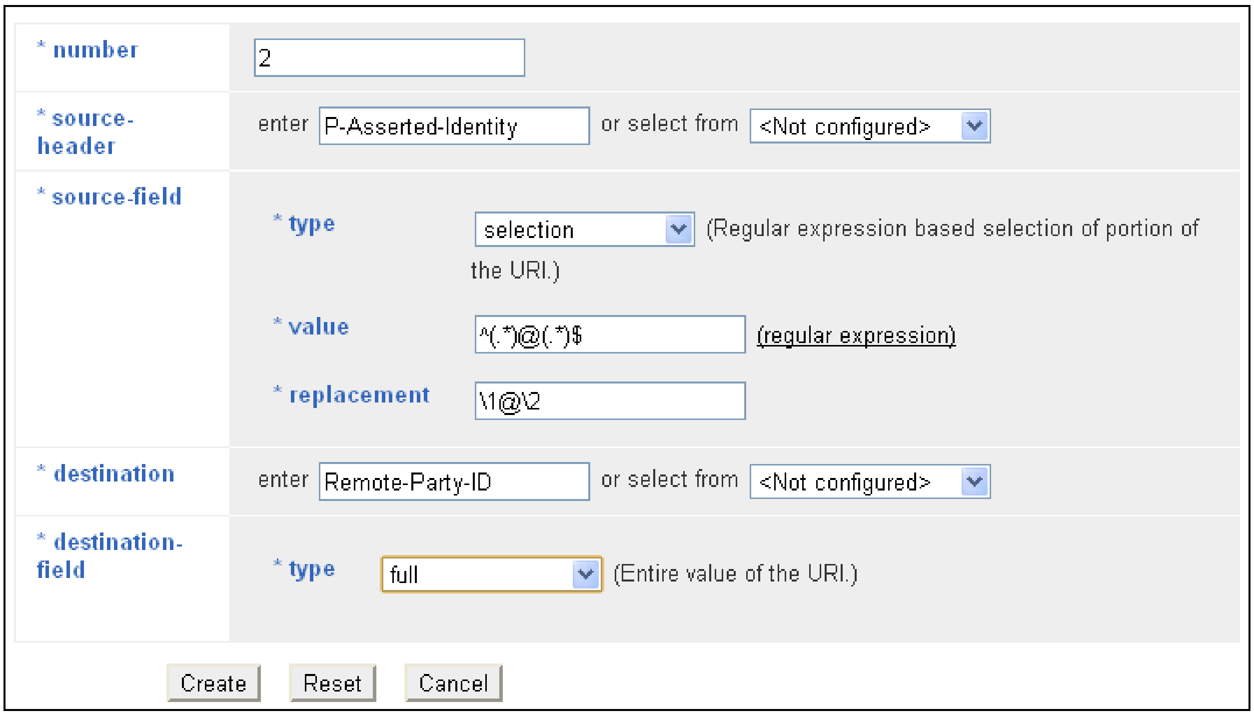


In the right pane that appears, enter "**2**" in the **number** field and enter **"P-Asserted-Identity"** in the s**ource-header** field. In the **source-field** area, next to **type** choose "**selection"** from the drop-down list.

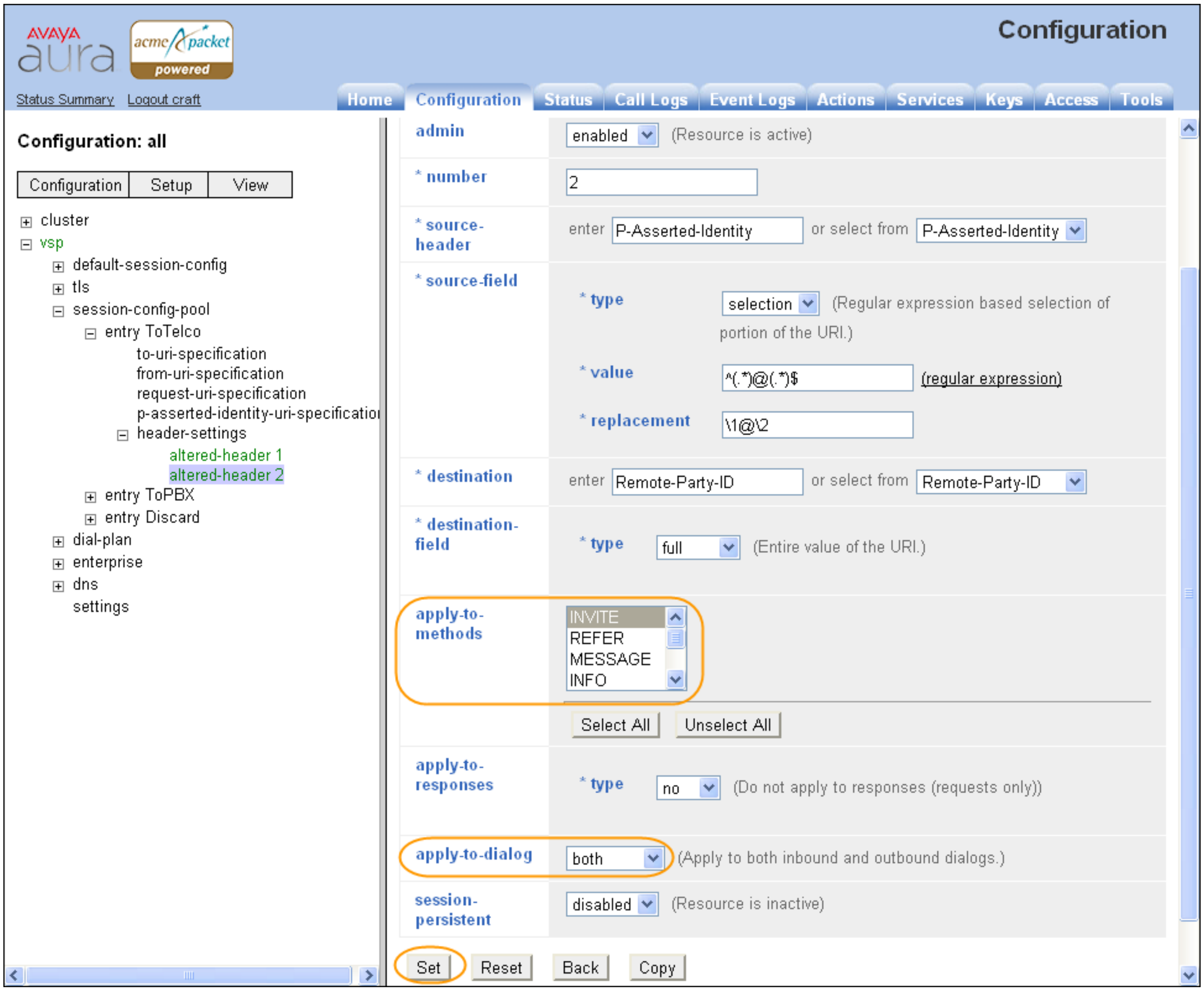
In the **value** field, enter a regular expression to match. In the sample configuration, **"^(.*)@(.*)$"** was entered. In this expression, the first (.*) will match and store any user part of the P-Asserted-Identity header. The second instance of (.*) matches and stores any host part of the header.

In the **replacement** field, **"\1@\2"** was entered in the sample configuration. The variable "**\1**" is the stored user part from the original P-Asserted-Identity header containing the number associated with the DID. The variable "**\2**" is the stored host portion of the P-Asserted-Identity header.

In the **destination** field enter **"Remote-Party-ID"**. Select "**full**" for **type** in the **destination-field** section and click **Create**.

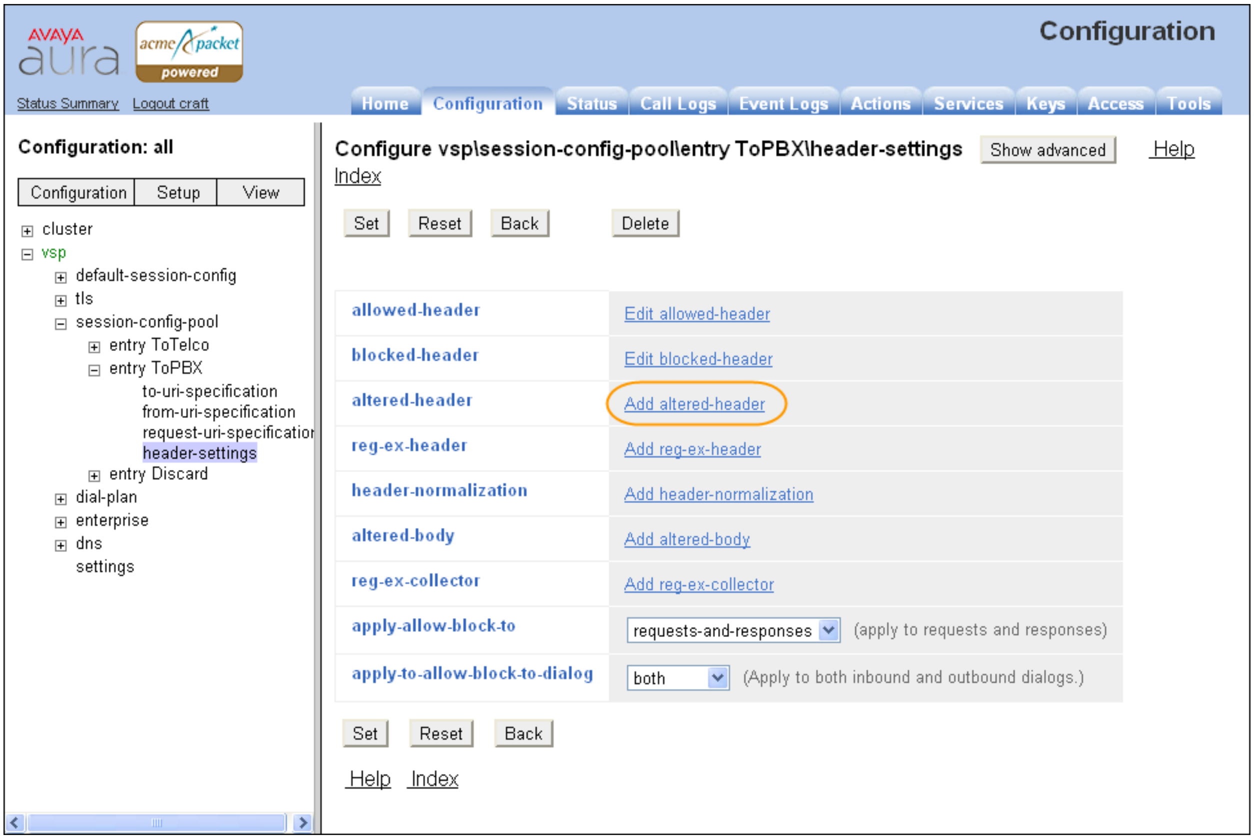


The following screen is presented. Select "**INVITE**" for **apply-to-methods** and "**both**" in the **apply-to-dialog** section. Click **Set** to complete the configuration.



7.2.7. Max-Forwards Value

On incoming PSTN calls that are forwarded back out to another PSTN 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 PSTN phone. Thus, the SBC was used to increase this value when the INVITE arrived at the SBC from the network. To do this, navigate to **vsp → session-config-pool → entry ToPBX → header-settings** and click **Add altered-header**.

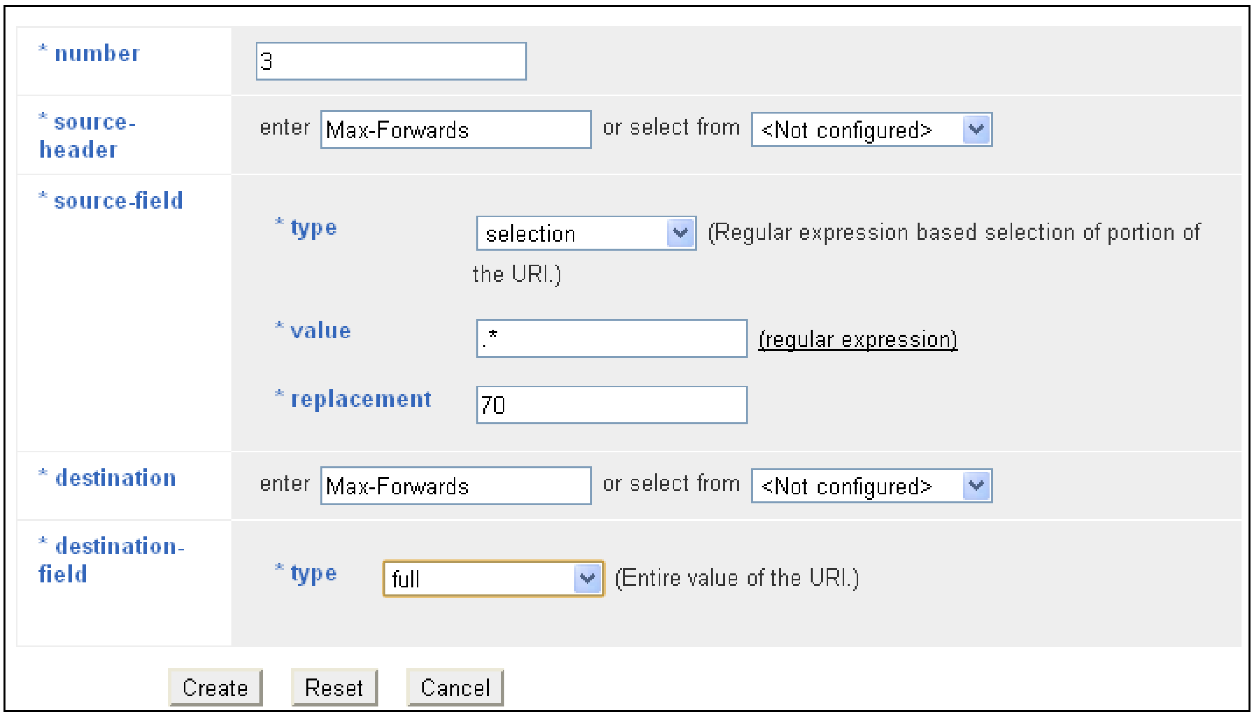


In the right pane that appears, enter "**3**" in the **number** field and enter **"Max-Forwards"** in the **source-header** field. In the **source-field** area, next to **type** choose "**selection**" from the drop-down list.

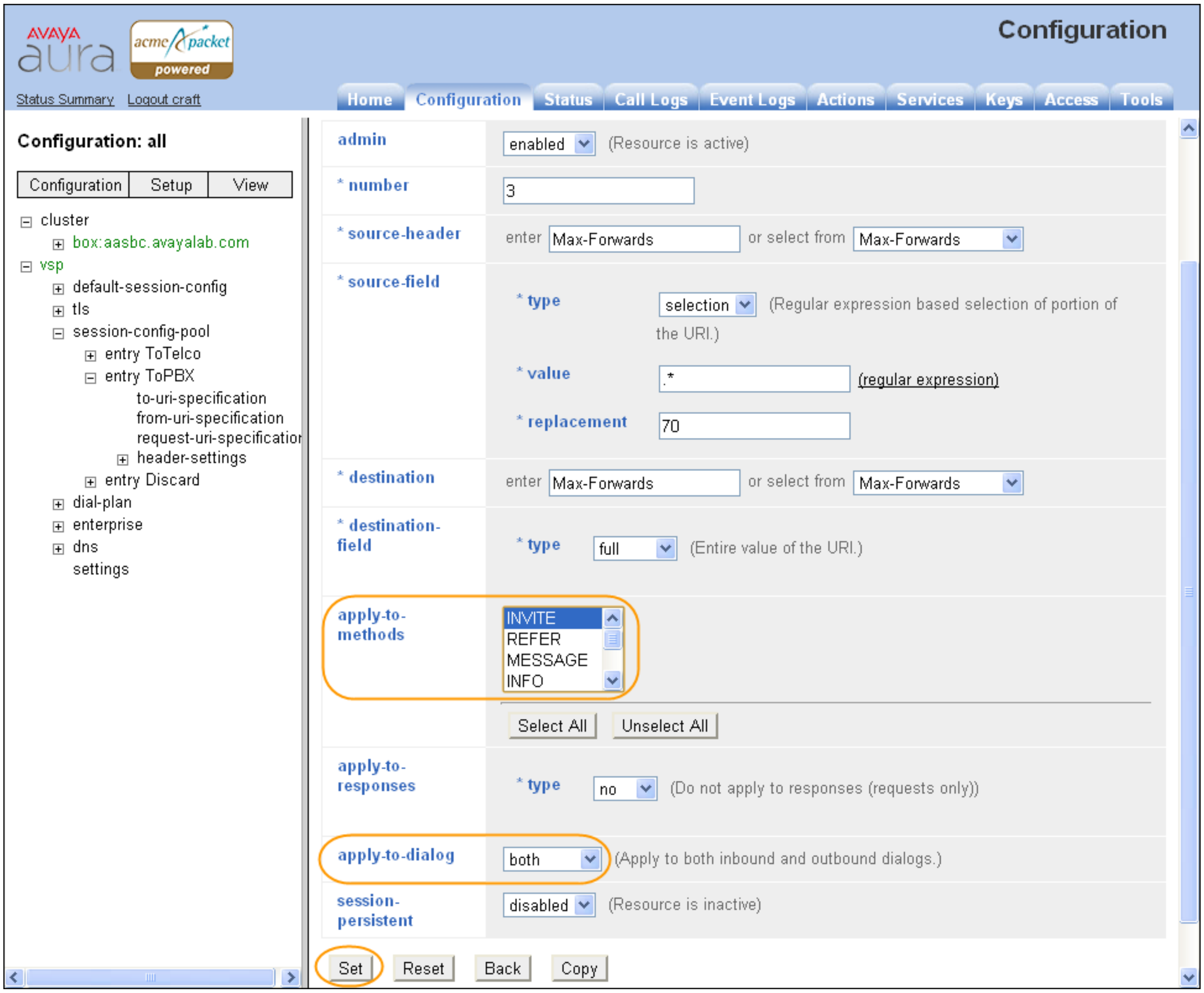
In the **value** field, enter **".*"** as the value. This is a regular expression that allows the system to match on any value.

In the **replacement** field, **"70"** was entered in the sample configuration.

In the **destination** field enter **"Max-Forwards".** Select "**full**" for **type** field in **destination-field** section and click **Create**.



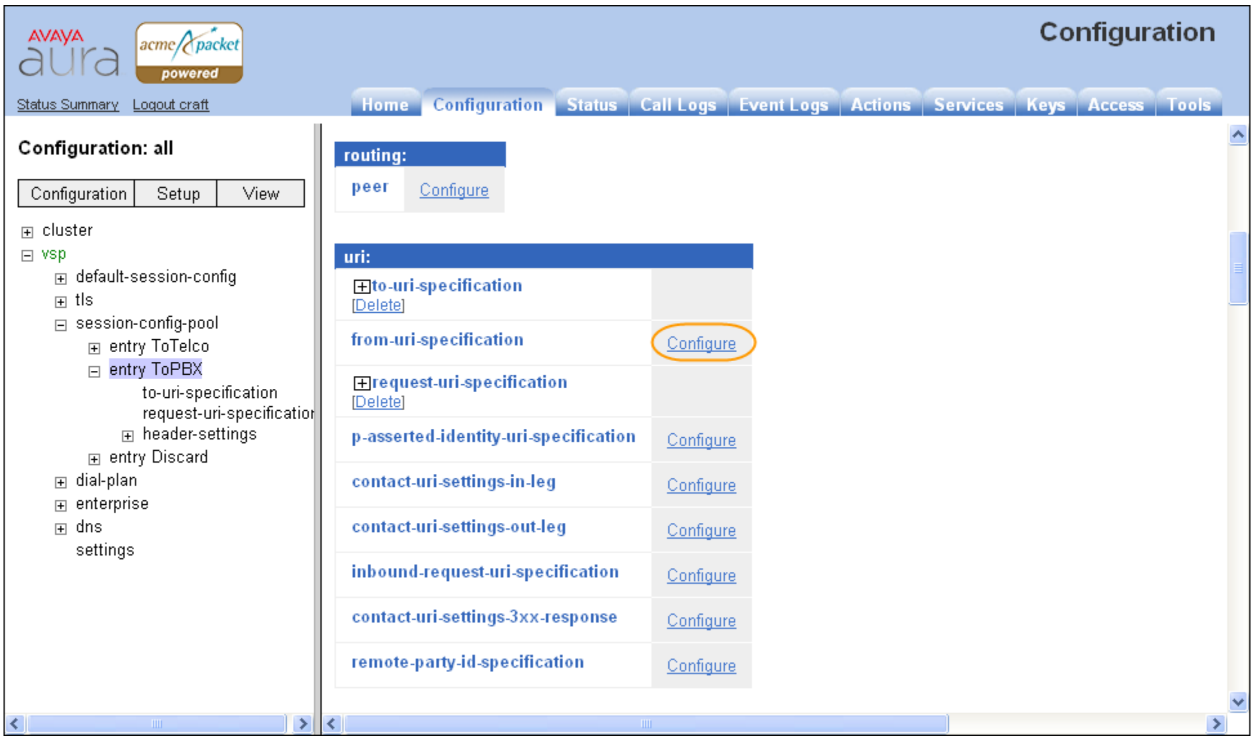
The following screen is presented, select “**INVITE**” for **apply-to-methods** and “**both**” for **type** field in **apply-to-responses** section. Click **Set** to complete the configuration.



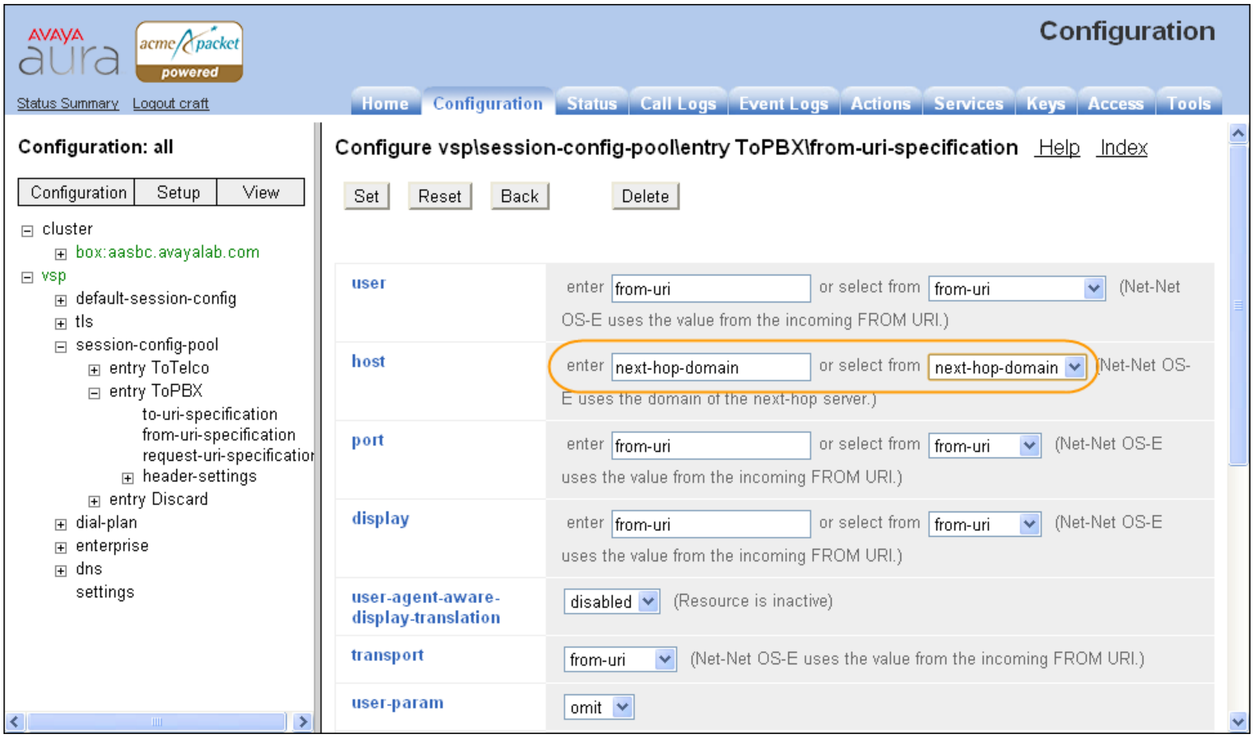
7.2.8. From URI

When calls are presented to SIP clients registered to Session Manager the Caller ID and Call Log displays the entire URI in the format user@domain (e.g. 303-555-1234@10.1.1.2). When returning a call from the Call Log by pressing the "Call" button, the Domain in the display needs to be one that is authorized on the Session Manager for the call to route properly. Therefore it is necessary to change the host portion of the From header to the enterprise domain.

In the left side menu, navigate to **vsp → session-config-pool → entry ToPBX.** Scroll down and click on **Configure** next to **from-uri-specification.**

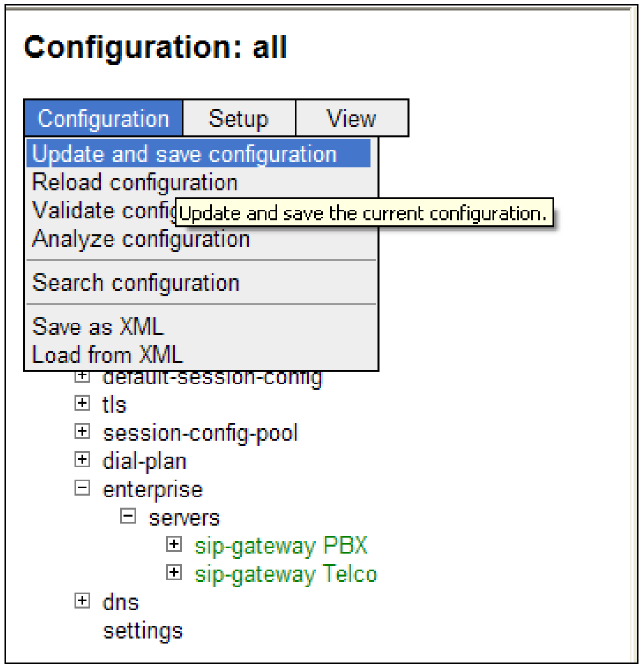


In the new right pane that appears, choose "**next-hop-domain**" from the drop-down list in the **host** field and click **Set**. This will set the host portion of the From header to the enterprise domain set in **Section 7.1.1**.



7.2.9. 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. Configure Level 3 Communications SIP Trunking

To use Level 3 Communications SIP Trunking service, a customer must request the service from Level 3 Communications using their sales process. This process can be initiated by contacting Level 3 Communications via the corporate web site at www.Level3.com and requesting information via the online sales links or telephone numbers.

9. Verification Steps

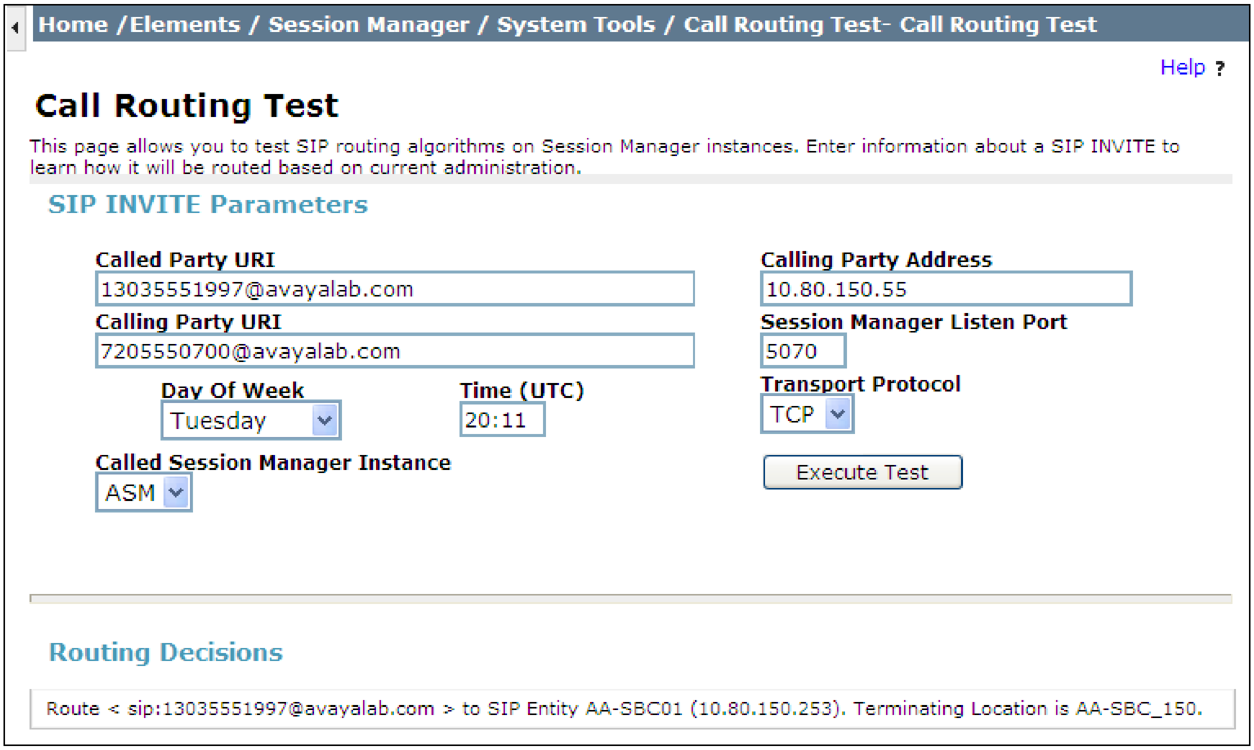
This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

9.1. Verification

The following steps may be used to verify the configuration:

1. Verify the call routing administration on Session Manager by logging in to System Manger and executing the Call Routing Test. Expand **Elements → Session Manager → System Tools → Call Routing Test**. Populate the field for the call parameters of interest. For example, the following screen shows an example call routing test for an

outbound call to the PSTN via Level 3 Communications. Under **Routing Decisions**, observe the call will route via the SBC to Level 3 Communications. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



2. 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 the SIP protocol timers.
3. 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.
4. Verify that a user on the PSTN can end an active call by hanging up.
5. Verify that a user at the enterprise site can end an active call by hanging up.

Use **status trunk "n"** to verify the active call has ended. Where **n** is the trunk group number used for Level 3 Communications SIP Trunking service.

Below is an example of an active call.

```
status trunk 1

                              TRUNK GROUP STATUS

Member    Port     Service State      Mtce Connected Ports
                                      Busy

0001/001 T00001   in-service/active  no   S00000
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

Verify that the port returns to **in-service/idle** after the call has ended.

```
status trunk 1

                              TRUNK GROUP STATUS

Member    Port     Service State      Mtce Connected Ports
                                      Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

9.2. Troubleshooting

1. Session Border Controller:
   - **Call Logs** - On the web user interface of the SBC, the **Call Logs** tab can provide useful diagnostic or troubleshooting information.
2. Communication Manager:
   - **list trace station** <extension number> - Traces calls to and from a specific station.
   - **list trace tac** <trunk access code number> - Traces calls over a specific trunk group.
   - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
   - **status trunk** <trunk access code number> - Displays trunk group information.
3. Session Manager:
   - **traceSM -x** - Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Boarder Controller 6.0 to the Level 3 Communications SIP Trunking service. The Level 3 Communications SIP Trunking service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The Level 3 Communications SIP Trunking service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.0.3, February 2011.
[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
[3] *Administering Avaya Aura® Communication Manager*, Release 5.2, May 2009, Document Number 03-300509.
[4] *Avaya Aura™ Communication Manager Feature Description and Implementation,* June 2010, Document Number 555-245-205.
[5] *Installing and Upgrading Avaya Aura™ System Manager 6.1 GA Version*, November 2010.
[6] *Installing and Configuring Avaya Aura® Session Manager*, April 2011, Document Number 03-603473
[7] *Administering Avaya Aura® Session Manager*, November 2010, Document Number 03-603324.
[8] *Installing and Configuring Avaya Aura® Session Border Controller*, November 2010.
[9] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, April 2010, Document Number 16-601443.
[10] *4600 Series IP Telephone LAN Administrator Guide*, July 2008, Document Number 555-233-507.
[11] *Avaya one-X Deskphone H.323 Administrator Guide*, May 2011, Document Number 16-300698.
[12] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1,* December 2010, Document Number 16-603838
[13] *Administering Avaya one-X Communicator*, July 2011
[14] *RFC 3261 SIP: Session Initiation Protocol,* http://www.ietf.org/
[15] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method,* http://www.ietf.org/

[16] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/
[17] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method,* http://www.ietf.org/
[18] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information*, http://www.ietf.org/

Appendix A: Avaya Aura® SBC Configuration File

```
#
#  Copyright (c) 2004-2010  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 14:44:02 Thu 2011-09-15
#
config cluster
 config box 1
  set hostname aasbc.avayalab.com
  set timezone America/Denver
  set name aasbc.avayalab.com
  set identifier 00:ca:fe:01:53:06
  config interface eth0
   config ip inside
    set ip-address static 10.80.150.253/24
    config ssh
    return
    config snmp
     set trap-target 10.80.150.252 162
     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 Default
      set gateway 10.80.150.1
     return
     config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.80.150.251
     return
     config route Static1
      set admin disabled
     return
     config route Static2
      set admin disabled
```

```
      return
      config route Static3
       set admin disabled
      return
      config route Static4
       set admin disabled
      return
      config route Static5
       set admin disabled
      return
      config route Static6
       set admin disabled
      return
      config route Static7
       set admin disabled
      return
     return
    return
   return
   config interface eth2
    config ip outside
     set ip-address static 10.2.2.5/25
     config sip
      set udp-port 5060 "" "" any 0
      set tcp-port 5060 "" "" any 0
     return
     config media-ports
     return
     config routing
      config route Default
       set admin disabled
      return
      config route external-sip-media-1
       set destination network 10.1.1.2/32
       set gateway 10.2.2.1
      return
     return
     config kernel-filter
      config allow-rule allow-sip-tcp-from-peer-1
       set destination-port 5060
       set source-address/mask 10.1.1.2/32
       set protocol tcp
      return
      config deny-rule deny-all-sip
       set destination-port 5060
      return
     return
    return
   return
   config cli
    set prompt aasbc.avayalab.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
  set apply-to-methods-for-filtered-logs
 return
 config header-settings
  set blocked-header P-Location
  set blocked-header Alert-Info
 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 header-settings
   config altered-header 1
    set source-header Diversion
    set source-field selection ^(.*)@(.*)$ "\1@10.1.1.2>"
    set destination Diversion
    set destination-field full
   return
   config altered-header 2
    set source-header P-Asserted-Identity
    set source-field selection ^(.*)@(.*)$ "\1@\2"
    set destination Remote-Party-ID
    set destination-field full
   return
  return
 return
 config entry ToPBX
  config to-uri-specification
   set host next-hop-domain
  return
```

```
   config from-uri-specification
    set host next-hop-domain
   return
   config request-uri-specification
    set host next-hop-domain
   return
   config header-settings
    config altered-header 3
     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 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 avayalab.com
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
     config server PBX1
      set host 10.80.150.206
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
     config server Telco1
      set host 10.1.1.2
```

```
      set transport TCP
      set port 5070
     return
    return
   return
  return
 return
 config dns
  config resolver
   config server 10.80.150.201
   return
  return
 return
 config settings
  set read-header-max 8191
 return
return

config external-services
return

config preferences
 config gui-preferences
  set enum-strings SIPSourceHeader Diversion
  set enum-strings SIPSourceHeader P-Asserted-Identity
  set enum-strings SIPSourceHeader Remote-Party-ID
  set enum-strings SIPSourceHeader Max-Forwards
 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 0x00574cae364b18bce3eda60aa4e9e6fc12f52fac23534762d2542ff361
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x003295b1cc18c0df86ed6c67a4033d2447c3015b7e59ca63591bb1ce3a
   set permissions access\permissions read-only
  return
  config user init
   set password 0x00506d66c68d8b364ee7d9c9ebd37da6a8b587bfc5a929fedfdb726c6a
   set permissions access\permissions superuser
  return
  config user craft
   set password 0x003699d8d952b8dee3f3d853336af125198096e73375f1e37cf72fffe1
   set permissions access\permissions superuser
  return
  config user dadmin
```

```
   set password 0x007d9e4162f99158de3b532b4bd5a1bb6dc19f47ee162937f9d184493d
   set permissions access\permissions read-only
  return
 return
return

config features
return
```

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