Avaya Solution & Interoperability Test Lab

Application Notes for Configuring XO SIP Trunking with Avaya Aura® Communication Manager Evolution Server, Avaya Aura® Session Manager, and Avaya Aura® Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between XO 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 Evolution Server, and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya Aura® Session Border Controller or Avaya Aura® Session Manager.

XO 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.

1. Introduction

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

Customers using this Avaya SIP-enabled enterprise solution with XO SIP Trunking 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.

1.1. Interoperability Compliance Testing

A simulated enterprise site using Communication Manager, Session Manager and the SBC was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to XO SIP Trunking.

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. Only the H.323 version of one-X Communicator was tested.
- Various call types including: local, long distance, international, outbound toll-free, inbound toll-free, operator assisted calls, local directory assistance (411) and emergency calls (911).
- Codec G.711MU and G.729A.
- 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
- Off-net call forwarding and mobility (extension to cellular)
- T.38 Fax

Items not supported or not tested included the following:

- Network Call Redirection using the SIP REFER method or a 302 response was not tested.
- G.711 pass-through fax was not tested as it is not recommended by Avaya for use over SIP trunks

Interoperability testing of XO SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Max-Forwards**: On incoming PSTN calls to an enterprise SIP 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 SIP phone. Thus, the SBC was used to increase this value when the INVITE arrived at the SBC from the network. (See **Section 6.2.3**)
- **DTMF digits detection**: By default, XO sends DTMF digits as both out-of-band RTP events as per RFC 2833 and as in-band tones. For interoperability, XO must disable the sending of in-band digits and only send DTMF digits as out-of-band RTP events. The XO National Activations Center (NAC) technician will disable this at the time of service activation. Otherwise, the detection of incoming DTMF digits from the network is unreliable. In-band tones must be disabled when using either the G.711 or G.729A codec. In rare cases if problems persist, the workaround described in **Appendix B** can also be applied. However, this is not recommended unless absolutely necessary since it burdens the media resources of the Communication Manager with additional processing.
- **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. Communication Manager provides the new connected party information by updating the Contact header in an UPDATE message. XO does not use the UPDATE message for this purpose but instead uses the contents of the INVITE From header for the calling party display information.
- **EC500 Extend**: EC500 is the Communication Manager mobility feature which allows a user to have incoming calls ring his desk phone as well as a remote number such as a cell phone. The Extend feature allows this same user to "extend" to the remote number an active call that was answered at the desk phone. The user can then hang up the desk phone and continue the call on the cell phone. In the case of the compliance test using XO SIP Trunking, when the extended call was hung up at the desk phone, the active call to the remote number was also disconnected.
- **EC500 Confirmed Answer**: The EC500 confirmed answer feature requires the user to enter a digit when the call is answered on the remote number. This prevents the call from being answered inadvertently by voicemail on the cell phone account, since the call is not recognized as answered until a digit is entered. In the case of the compliance test using XO SIP Trunking, the user is still not connected after the digit is entered and the call to the remote number is dropped while the desk phone continues to ring. It is not recommended to use confirmed answer with this solution.

1.2. Support

For technical support on XO SIP Trunking, contact XO using the Customer Care links at www.xo.com.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Selecting the **Support Contact Options** link followed by **Maintenance Support** provides the worldwide support directory for Avaya Global Services. Specific numbers are provided for both customers and partners based on the specific type of support or consultation services needed. Some services may require specific Avaya service support agreements. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

2. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to XO SIP Trunking. This is the configuration used for compliance testing.

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

- Avaya S8300D Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running 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 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 can not be routed by the PSTN.

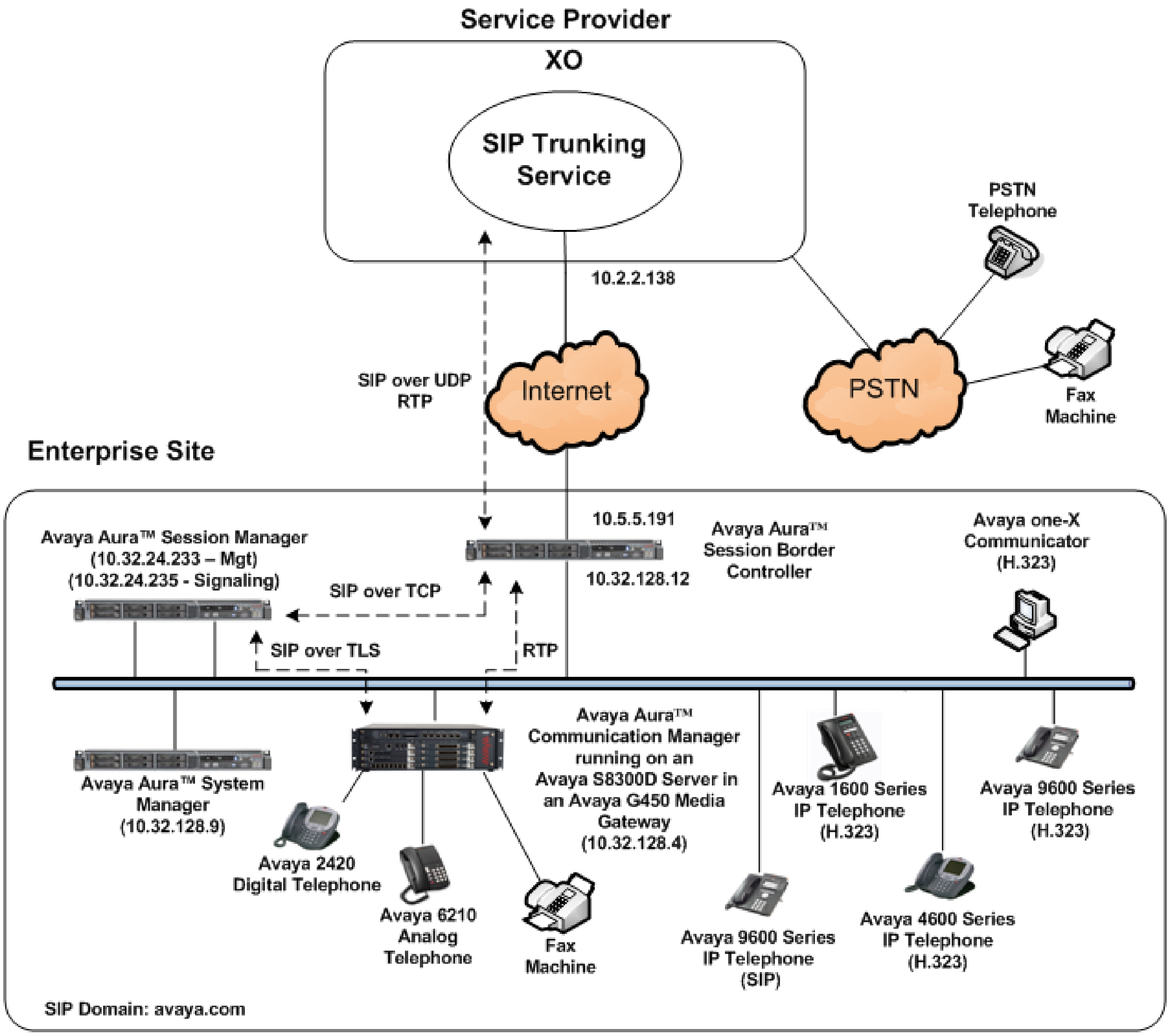


Figure 1: Avaya IP Telephony Network using XO SIP Trunking

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 the Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN 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. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the SBC. From the SBC, the call is sent to XO SIP Trunking.

3. 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 Manager running on an Avaya S8300D Server	6.0 SP0 (R016x.00.0.345.0-18246)
Avaya G450 Media Gateway	30.14.0
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.0 (Build asm-6.0.0.0.600020)
Avaya Aura® System Manager running on an Avaya S8800 Server	6.0 (Build 6.0.0.0.556-3.0.6.1)
Avaya 1608 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.2
Avaya 4621SW IP Telephone (H.323)	2.9.1
Avaya 9640 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.1.1
Avaya 9630 IP Telephone (H.323)	Avaya one-X Deskphone SIP Edition 2.6
Avaya one-X Communicator (H.323)	6.0
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura® Session Border Controller	6.0 (Build SBCT_6.0.0.1.4)
XO SIP Trunking Solution Components	
Component	Release
Sonus Networks Network Border Switch (NBS) Sonus Networks PSX Routing Server	07.03.01 R006 07.03.01 R005
Sonus Networks GSX Gateway Sonus Networks PSX Routing Server	06.04.12 F001 06.04.17 R001
Broadsoft BroadWorks VoIP Applications Platform including: • Broadsoft Application Server (AS) • Broadsoft Network Server (NS)	Release 14 Rel_14.sp9_1.123 Rel_14.sp4_1.165

Table 1: Equipment and Software Tested

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

4. Configure Communication Manager

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

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

The 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 public IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

4.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 licenses are available and 20 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  36
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  20
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                            Maximum TN2501 VAL Boards: 10    0
                    Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
```

4.2. System Features

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

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

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

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

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

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

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

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

4.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8300D Server running Communication Manager ***(procr***) and for Session Manager (***sessionMgr***). These node names will be needed for defining the service provider signaling group in **Section 4.6**.

```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
cmm                 10.32.128.4
default             0.0.0.0
procr               10.32.128.4
procr6              ::
sessionMgr          10.32.24.235
```

4.4. 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. XO SIP Trunking supports G.711MU and G.729A. Thus, these codecs were included in this set. Enter ***G.711MU*** and ***G.729A*** 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.711MU          n          2        20
 2: G.729A           n          2        20
 3:
```

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

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

4.5. IP Network Region

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

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***avaya.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 4.4**.
- Default values can be used for all other fields.

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

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

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

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

4.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to ***tcp*** The transport method specified here is used between the Communication Manager and Session Manager. The transport method used between the Session Manager and the SBC is specified as TCP in **Sections 5.6** and **6.1.3**. Lastly, the transport method between the SBC and XO is UDP. This is defined in **Section 6.1.3** when the service provider name is selected.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5062***. (For TCP, the well-known port value is 5060).
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and can not be changed via administration. Later, the **Peer-Server** field will automatically change to ***SM*** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Avaya S8300D Server running Communication Manager as defined in **Section 4.3**.

- Set the **Far-end Node Name** to ***sessionMgr***. This node name maps to the IP address of Session Manager as defined in **Section 4.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 4.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- 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 3                                            Page   1 of   1
                                SIGNALING GROUP

 Group Number: 3             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                    Far-end Node Name: sessionMgr
 Near-end Listen Port: 5062                   Far-end Listen Port: 5062
                                           Far-end Network Region: 2

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

4.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 4.6**. For the compliance test, trunk group 3 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 3                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 3                   Group Type: sip          CDR Reports: y
  Group Name: SP Trunk                  COR: 1        TN: 1        TAC: 1003
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk         Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     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 3                                               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

                                      Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with XO. Thus, the **Numbering Format** was set to ***private*** and the **Numbering Format** in the route pattern was set to ***unk-unk*** (see **Section 4.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 4.2**, 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 3                                                Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

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

Set the **Telephone Event Payload Type** to ***101***, the value preferred by XO.

```
add trunk-group 3                                               Page   4 of  21
                              PROTOCOL VARIATIONS

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


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
                             Enable Q-SIP? n
```

4.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 4.7**), use the **change private-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, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 40003, 40005 and 40010. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change private-numbering 0                                          Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private      Total
Len Code             Grp(s)     Prefix        Len
                                                    Total Administered: 4
 5  4                                        5         Maximum Entries: 240
 5  40003           3         2145551234      10
 5  40005           3         2145551235      10
 5  40010           3         2145551236      10
```

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 4 will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 0                                          Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private      Total
Len Code             Grp(s)     Prefix        Len
                                                    Total Administered: 1
 5  4               3         21455           10      Maximum Entries: 240
```

Even though private numbering was selected, currently the number used in the SIP Diversion header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table.

```
change public-unknown-numbering 0                                 Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 4
 5  4                                       5        Maximum Entries: 240
 5  40003         3         2145551234      10
 5  40005         3         2145551235      10    Note: If an entry applies to
 5  40010         3         2145551236      10    a SIP connection to Avaya
                                                  Aura(tm) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.
```

4.9. Outbound Routing

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

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

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           4   dac
   4           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   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:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       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: *01    All: *02    Deactivation: *03
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 which contains the SIP trunk to the service provider (as defined next).

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

          Dialed           Total      Route     Call   Node   ANI
          String          Min  Max  Pattern    Type   Num    Reqd
    0                     1    1      2        op            n
    0                     11   11     2        op            n
    00                    2    2      2        op            n
    011                   10   18     2        intl          n
    1800                  11   11     2        fpna          n
    1877                  11   11     2        fpna          n
    1908                  11   11     2        fpna          n
    411                   3    3      2        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 2 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 3 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: ***1*** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format**: ***unk-unk*** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 4.7**.
- **LAR**: ***next***

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2   Pattern Name: SP route
                             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: 3    0       1                                                     n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

5. Configure Avaya Aura® Session Manager

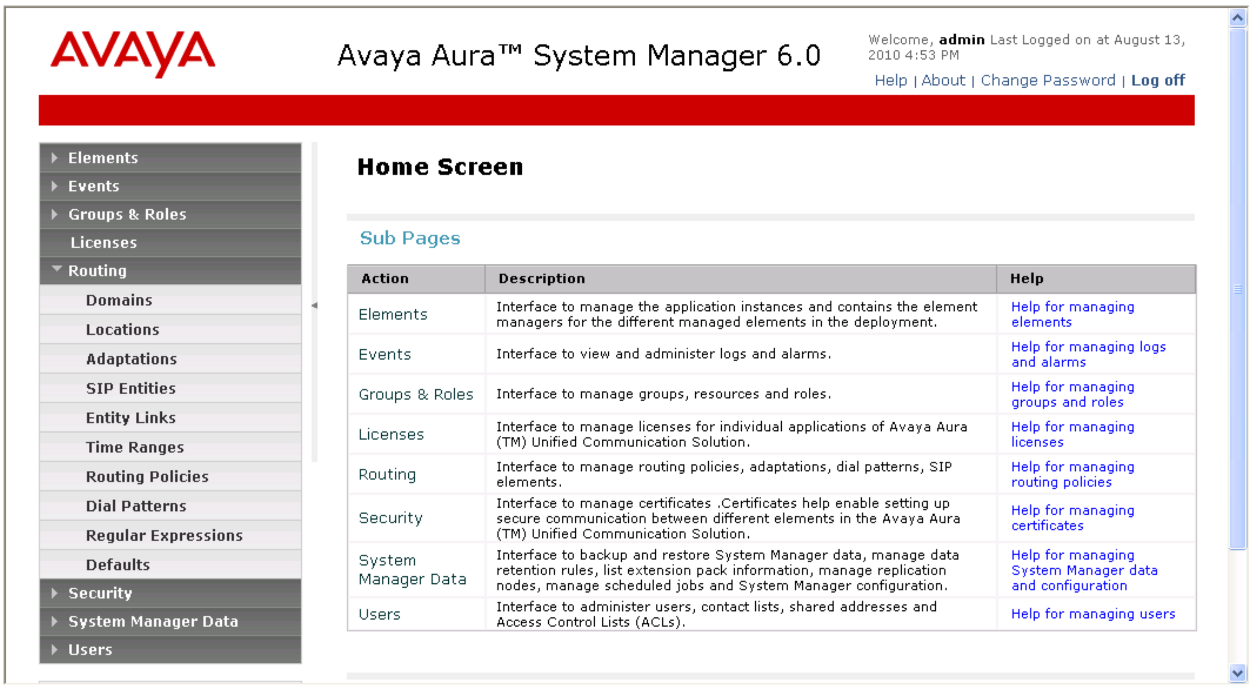
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

It may not be necessary to create all the items above when creating a connection to the service provider since some of 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.

5.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The screen shown below is then displayed. The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Routing** link shown below.

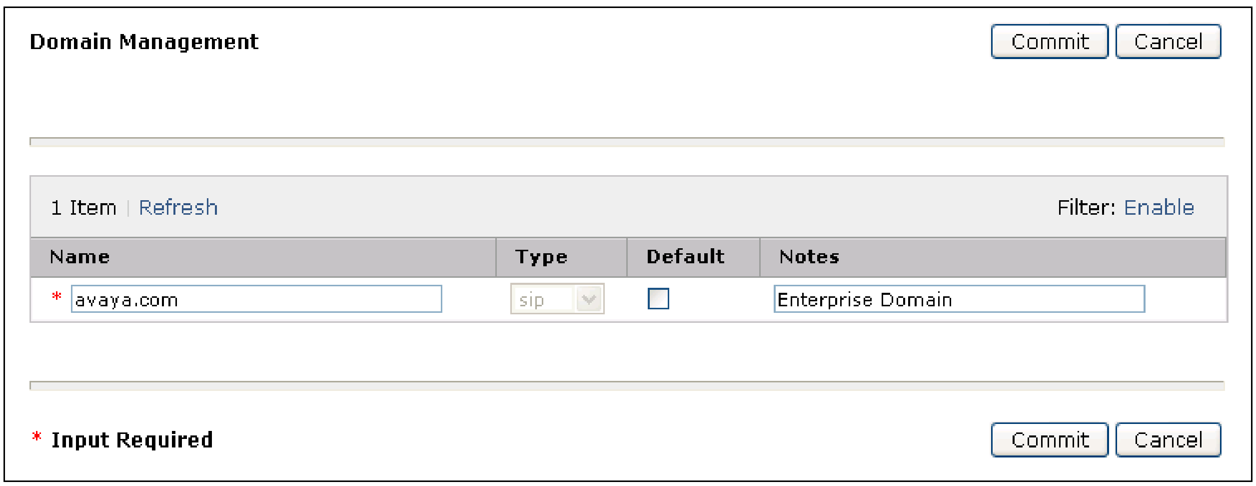


5.2. Specify SIP Domain

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 (***avaya.com***). Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 5.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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



5.3. 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 (**Section 5.1**) and click the **New** button in the right pane (not shown).

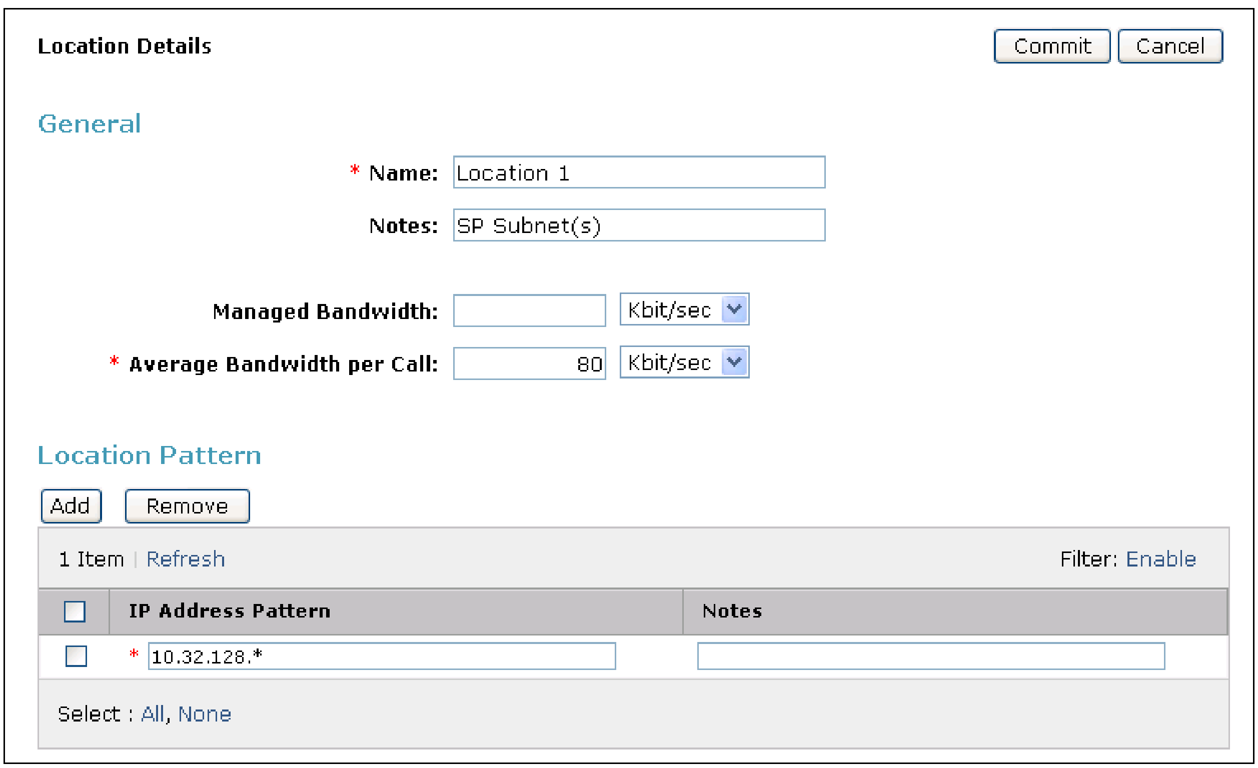
In the **General** section, enter the following values. Use default values for all remaining fields:

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

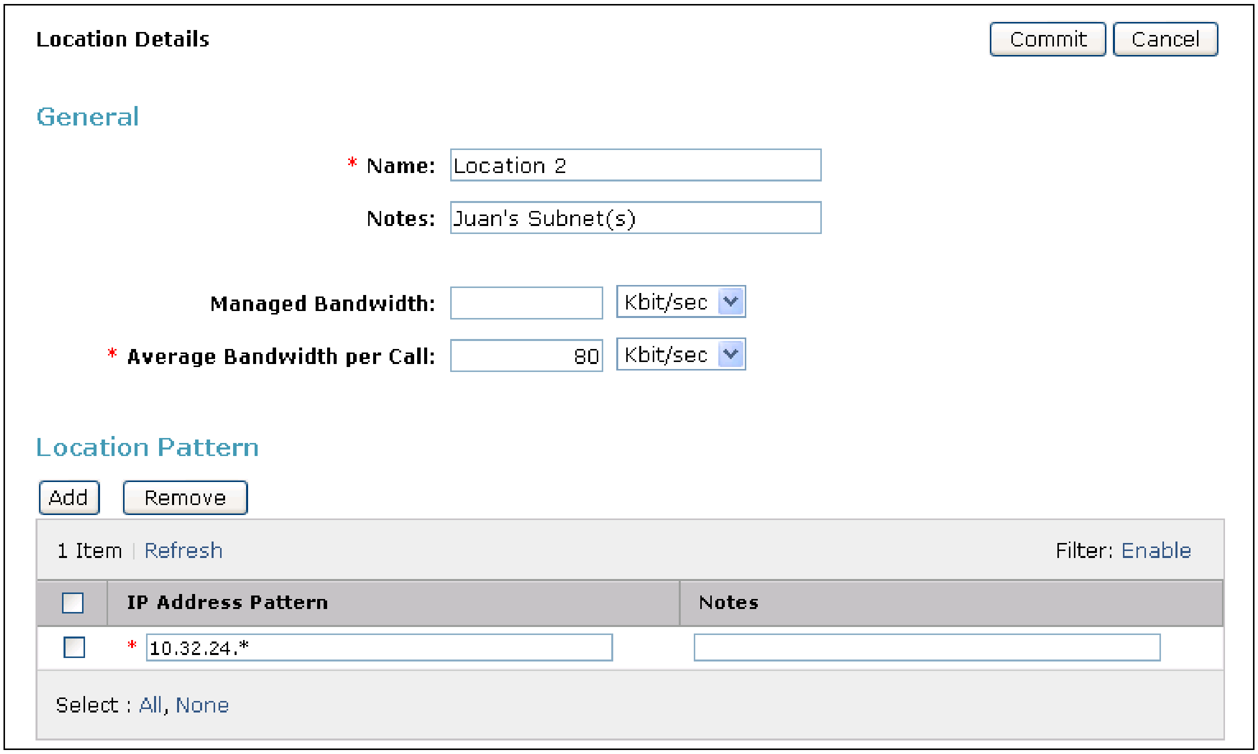
In the **Location Pattern** section, click **Add** and enter the following values. Use default values for all remaining fields:

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

The screen below shows the addition of the ***Location 1***, which includes all equipment on the ***10.32.128.x*** subnet including Communication Manager, and the SBC. Click **Commit** to save.



Repeat the preceding procedure to create **Location 2** which includes all equipment on the ***10.32.24.x*** subnet which includes the Session Manager.



5.4. Add Adaptation Module

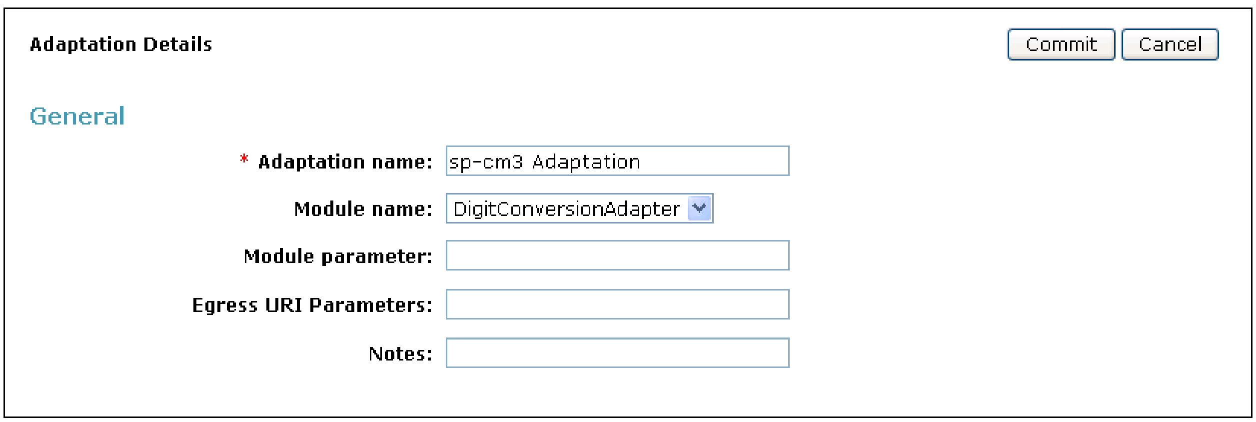
Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules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

For XO interoperability, one adaptation is needed and maps inbound DID numbers from XO to local Communication Manager extensions. The adaptation is applied to the Communication Manager SIP entity.

To create the adaptation, navigate to **Routing → Adaptations** 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:

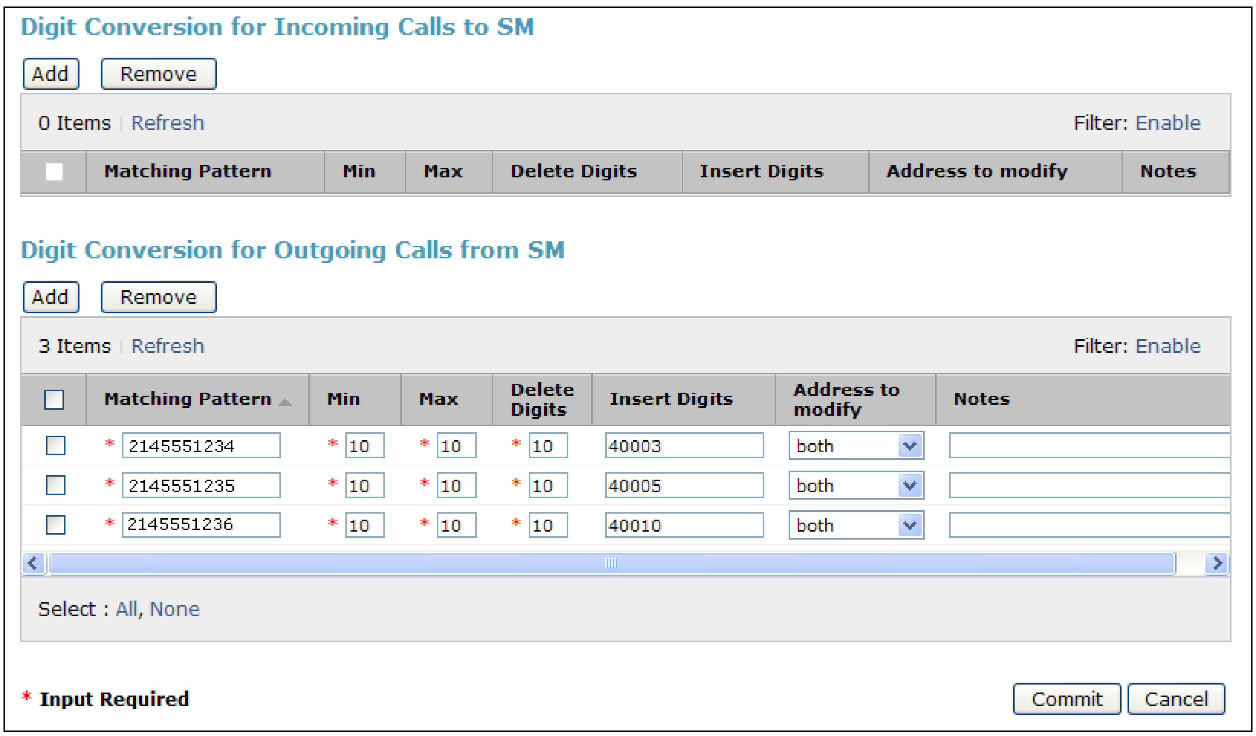
- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter ***DigitConversionAdapter***.



To map inbound DID numbers from XO to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields:

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select **both**.

Click **Commit** to save.



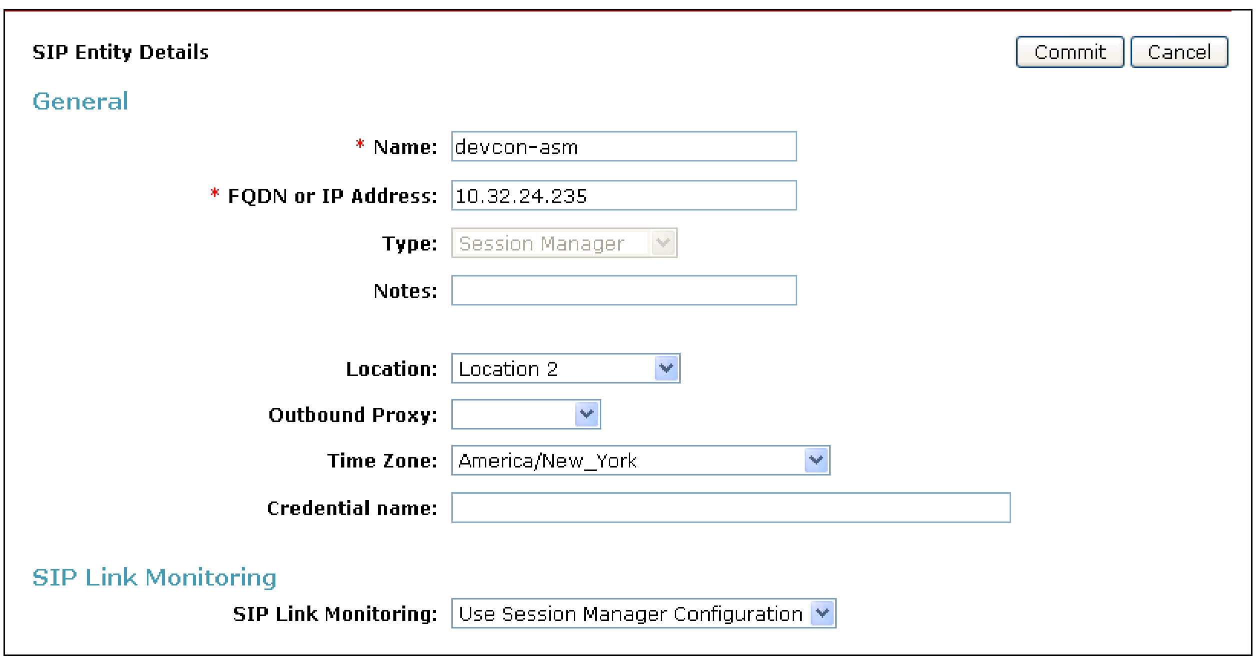
5.5. Add SIP Entities

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 (**Section 5.1**) 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** created in **Section 5.4** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

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



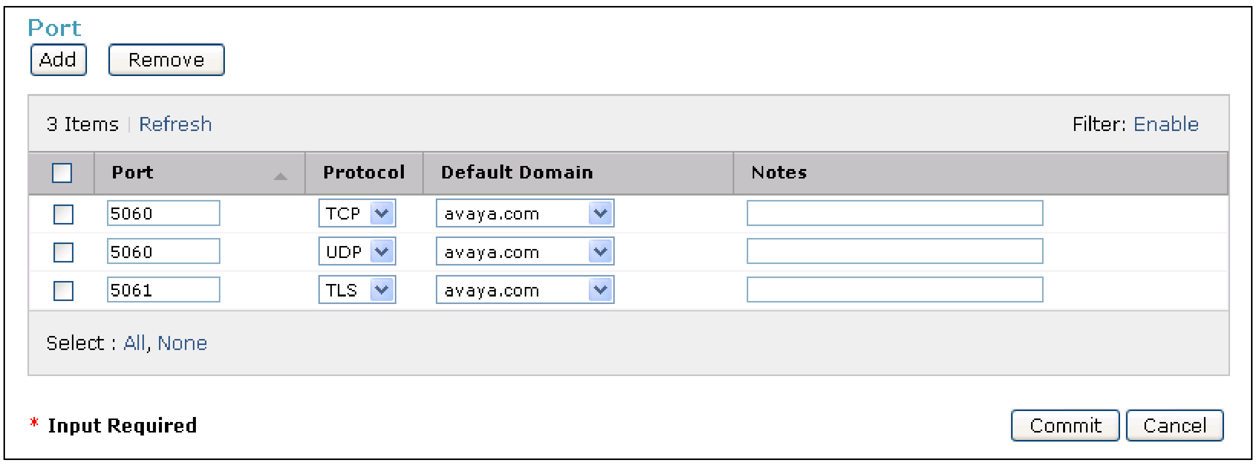
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

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

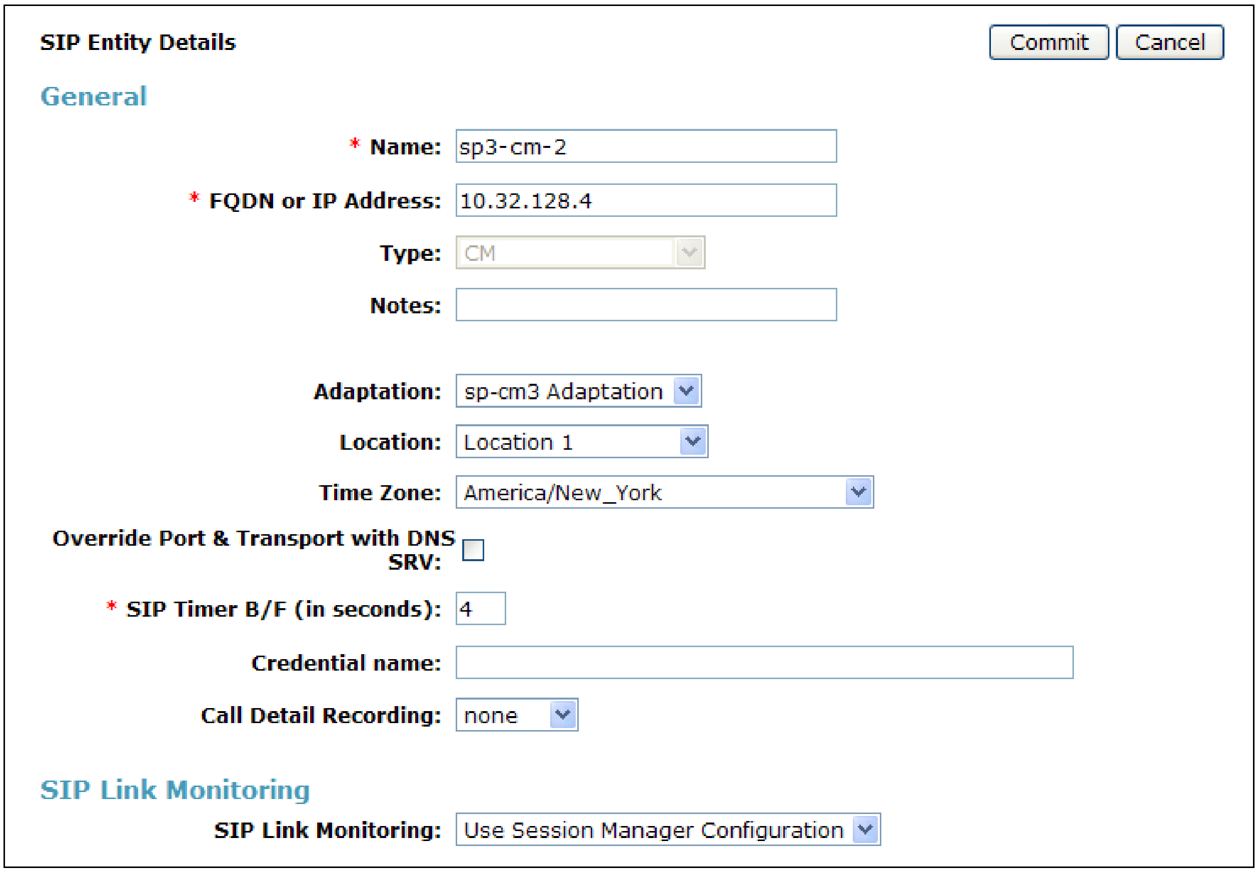
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

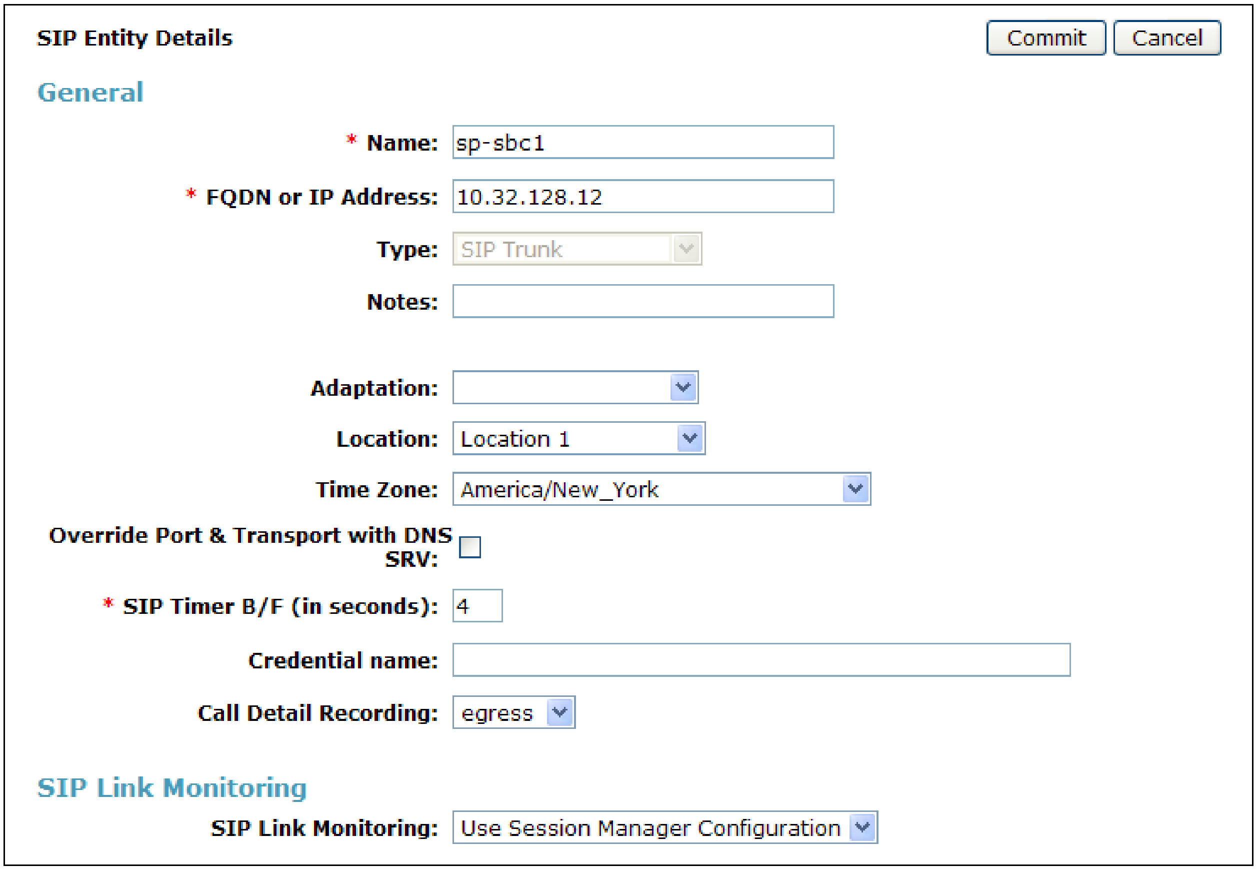
For the compliance test, three **Port** entries were added.



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, this requires the creation of a separate SIP entity for Communication Manager than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the Avaya S8300D Server running Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 5.4**.



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



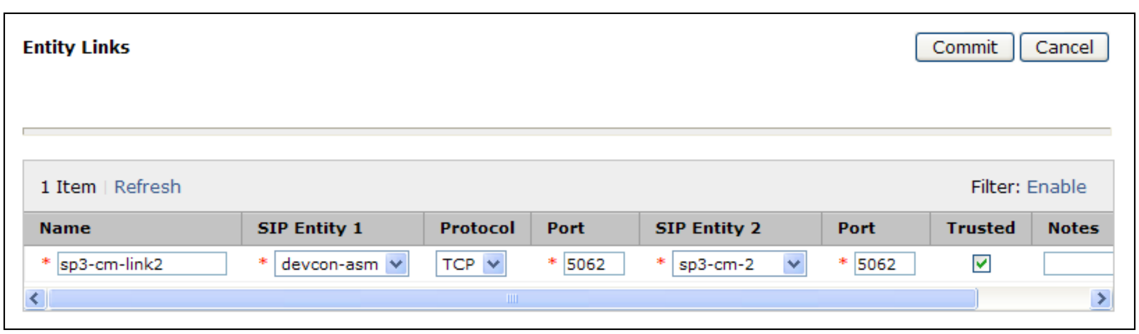
5.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

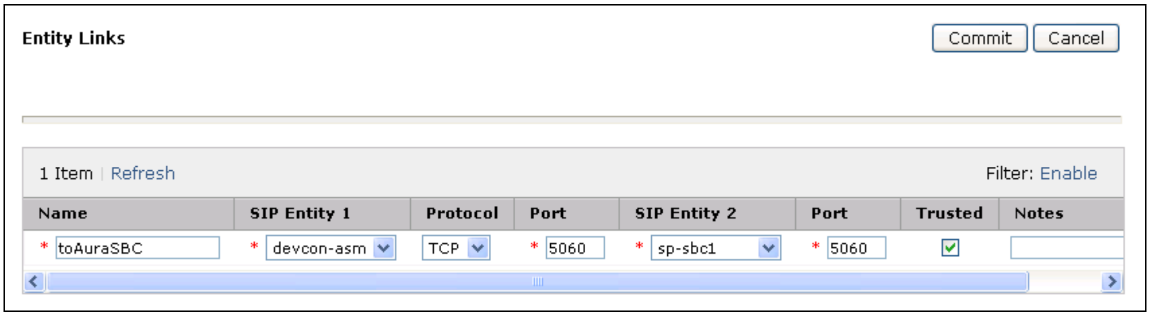
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 4.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager, select the Communication Manager SIP Entity defined in **Section 5.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 4.6**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 5.5** will be denied.*

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and the SBC. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 4.6**.

Entity Link to Communication Manager:



Entity Link to the SBC:



5.7. Add Routing Policies

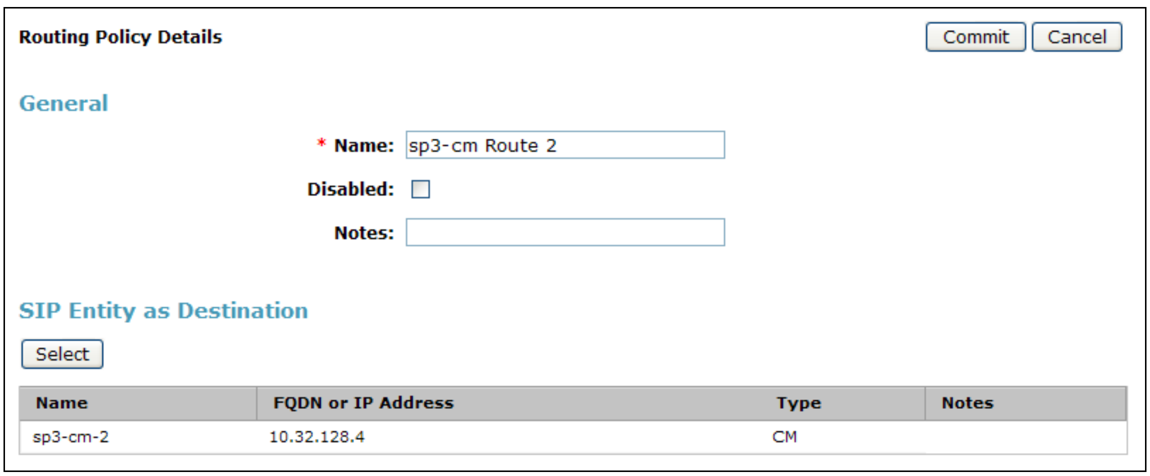
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5.5**. Two routing policies must be added: one for Communication Manager and one for the SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

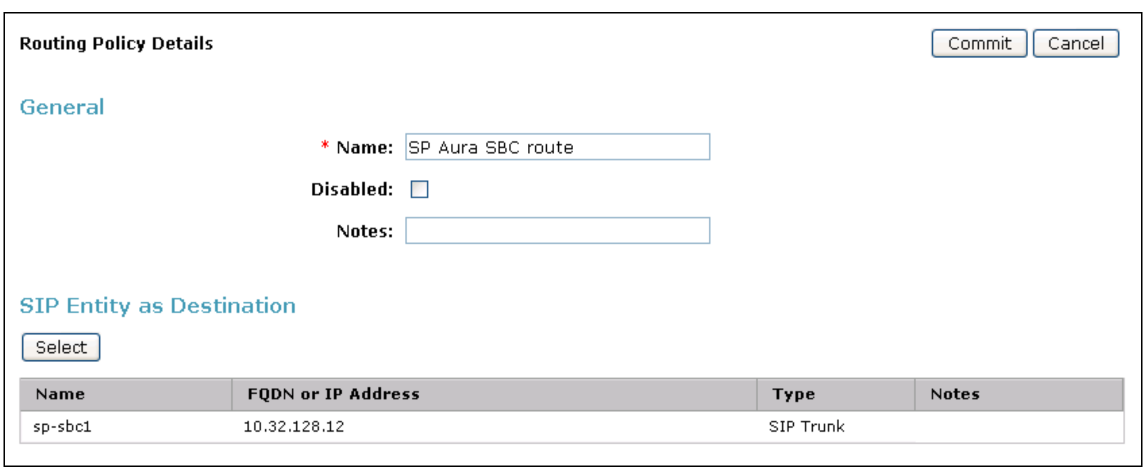
In the **General** section, enter the following values. Use default values for all remaining fields:

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

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

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





5.8. 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 XO 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 (**Section 5.1**) and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

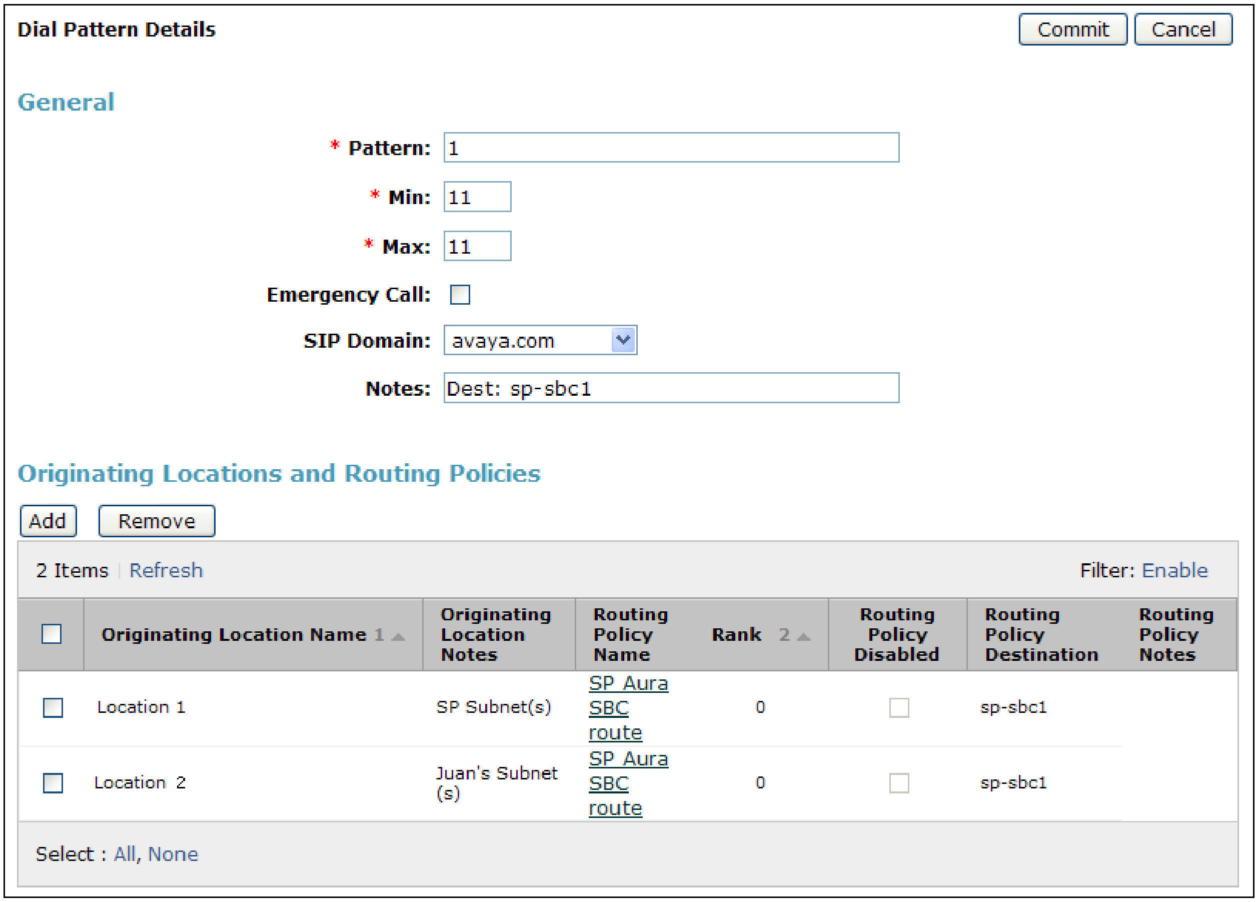
In the **General** section, enter the following values. Use default values for all remaining fields:

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

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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that 11 digit numbers that begin with a 1 and have a destination domain of ***avaya.com*** from ***Location 1*** or ***Location 2*** uses route policy ***SP AuraSBC route***.



Dial Pattern Details

Commit | Cancel

General

* **Pattern:** 1

* **Min:** 11

* **Max:** 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Dest: sp-sbc1

Originating Locations and Routing Policies

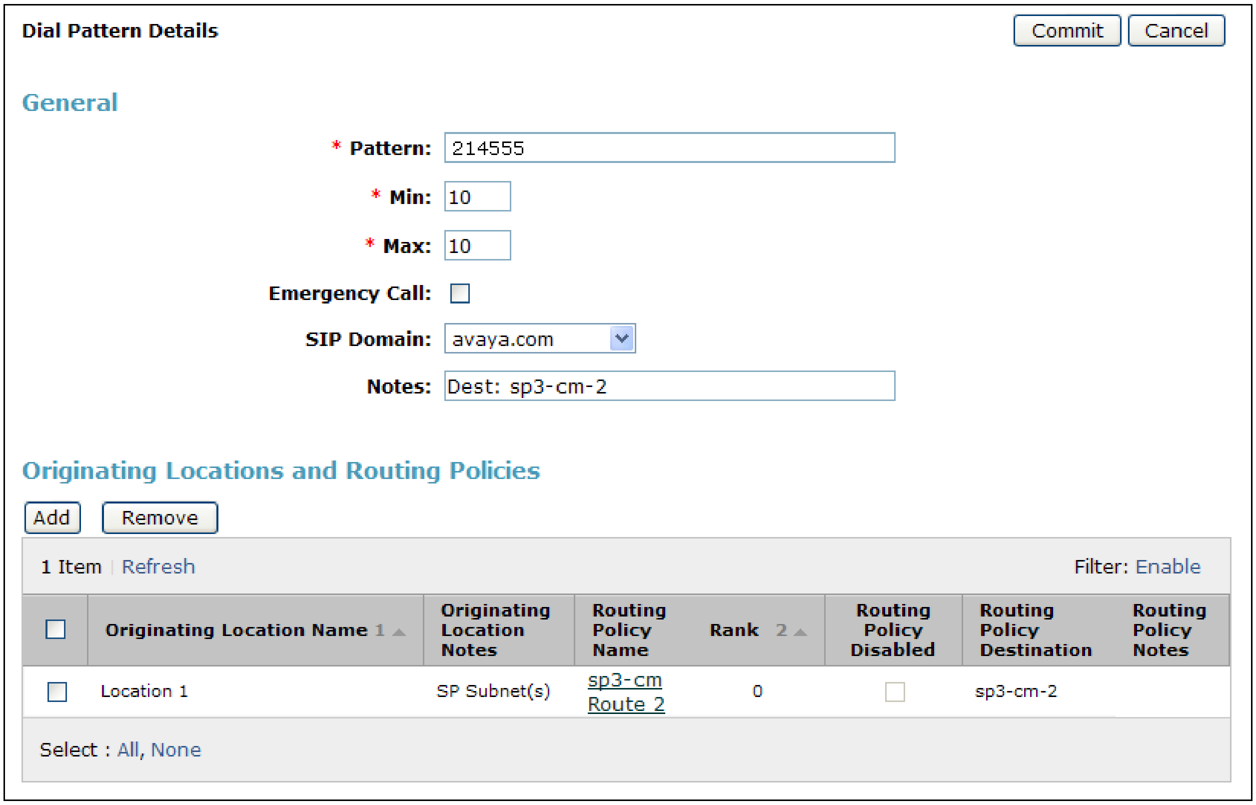
Add | Remove

2 Items | Refresh   Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Location 1	SP Subnet(s)	SP Aura SBC route	0	☐	sp-sbc1	
☐	Location 2	Juan's Subnet (s)	SP Aura SBC route	0	☐	sp-sbc1	

Select : All, None

The second example shows that 10 digit numbers that start with ***214555*** to domain ***avaya.com*** and originating from ***Location 1*** uses route policy ***sp3-cm Route***. These are the DID numbers assigned to the enterprise from XO. Location 1 is selected because these calls come from the SBC which resides in location 1.



Dial Pattern Details Commit Cancel

General

* Pattern: 214555

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Dest: sp3-cm-2

Originating Locations and Routing Policies

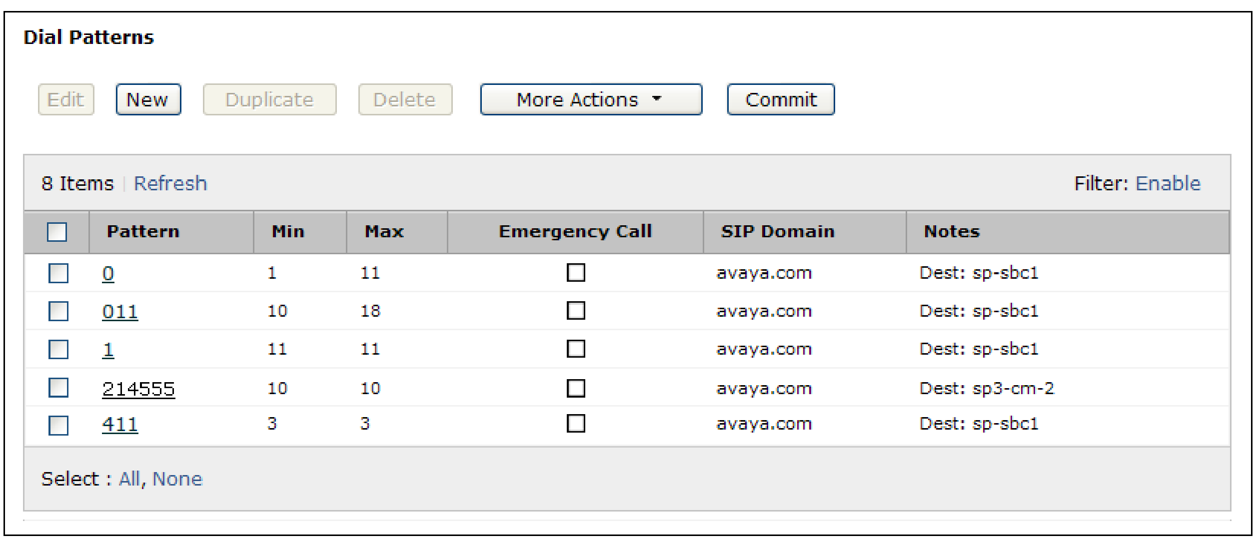
Add Remove

1 Item | Refresh Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Location 1	SP Subnet(s)	sp3-cm Route 2	0	☐	sp3-cm-2	

Select : All, None

The complete list of dial patterns defined for the compliance test is shown below.



Dial Patterns

Edit New Duplicate Delete More Actions Commit

8 Items | Refresh Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
☐	0	1	11	☐	avaya.com	Dest: sp-sbc1
☐	011	10	18	☐	avaya.com	Dest: sp-sbc1
☐	1	11	11	☐	avaya.com	Dest: sp-sbc1
☐	214555	10	10	☐	avaya.com	Dest: sp3-cm-2
☐	411	3	3	☐	avaya.com	Dest: sp-sbc1

Select : All, None

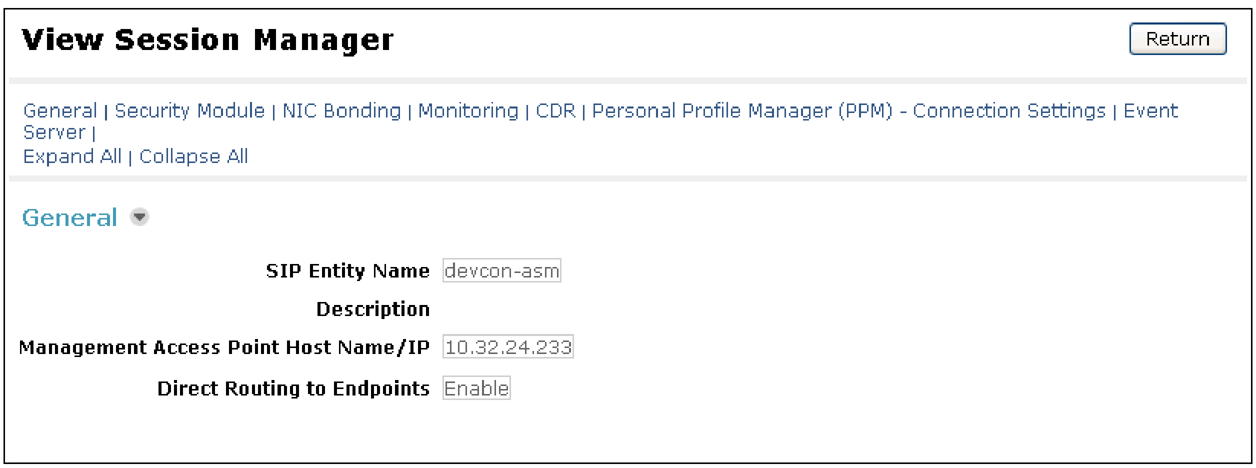
5.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

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

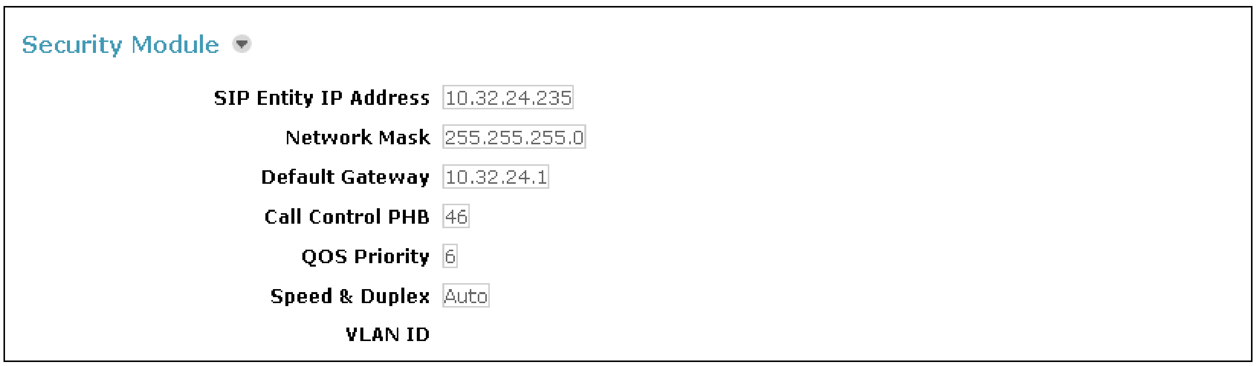
The screen below shows the Session Manager values used for the compliance test.



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

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

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



6. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® SBC. This configuration is done in two parts. The first part is done during the 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 Avaya Aura® SBC template see [1].

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**.

6.1. Installation Wizard

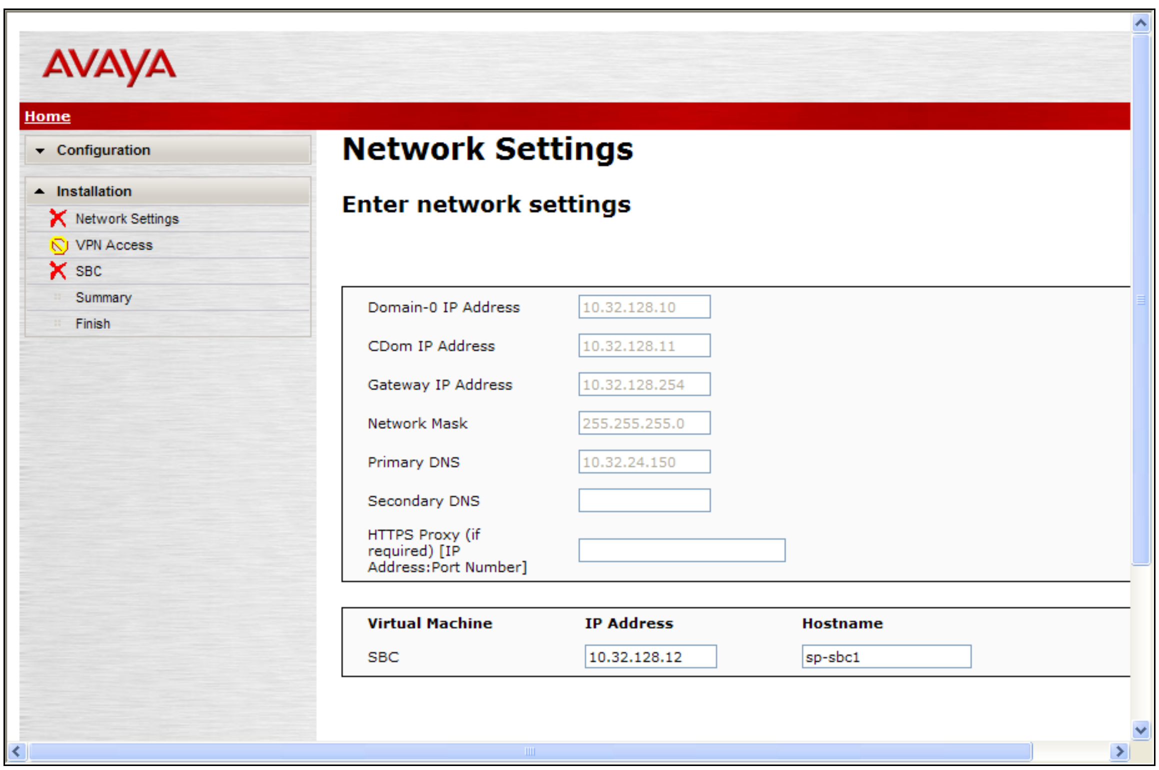
During the installation of the Avaya Aura® SBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the SBC.

6.1.1. 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.

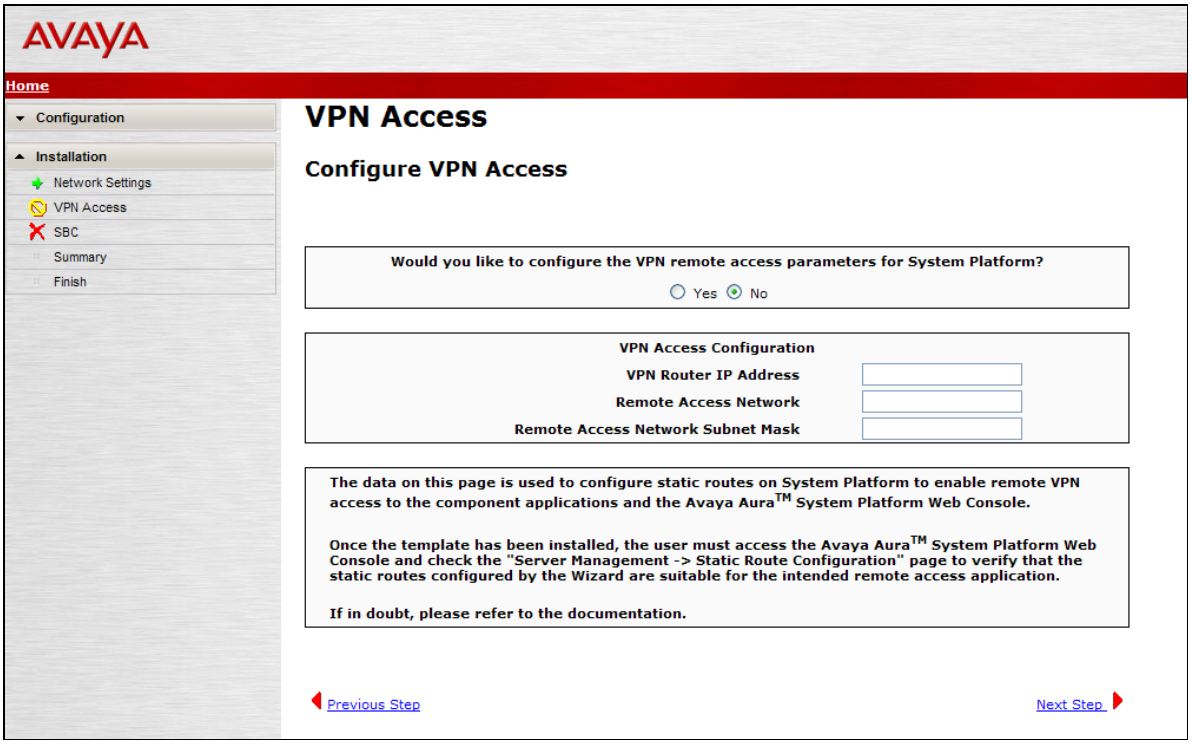
Click **Next Step** (not shown) to continue.



6.1.2. 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.



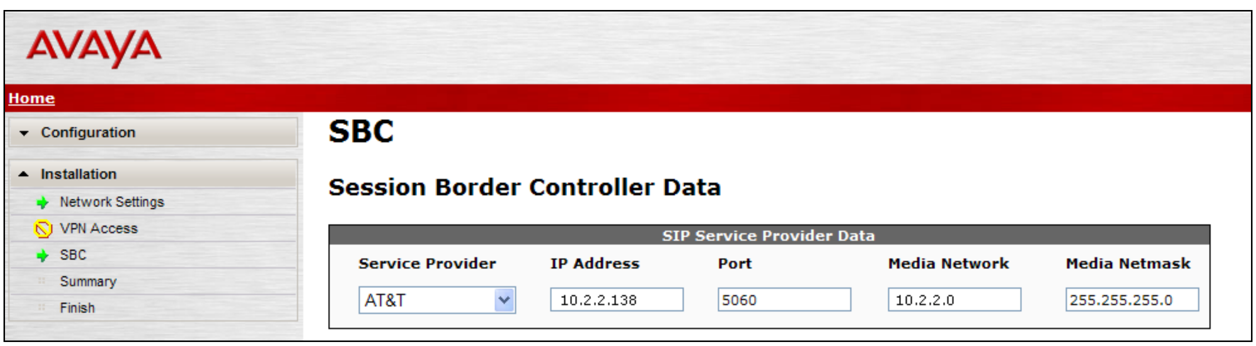
6.1.3. SBC

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

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

- **Service Provider**: From the pull-down menu, select the name of the service provider to which the SBC will connect. This will allow the wizard to select a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for XO. Thus, **AT&T** was chosen instead and further customization was done manually after the wizard was complete. A customized configuration file for XO should be available in a future SBC release.
- **IP Address**: Enter the XO provided IP address of the XO Sonus NBS. 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 XO provided subnet where media traffic will originate. If media can originate from multiple networks, enter one network address on this screen and additional networks can be added after installation.
- **Media Netmask**: Enter the netmask corresponding to the **Media Network**.

Scroll down to continue.



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

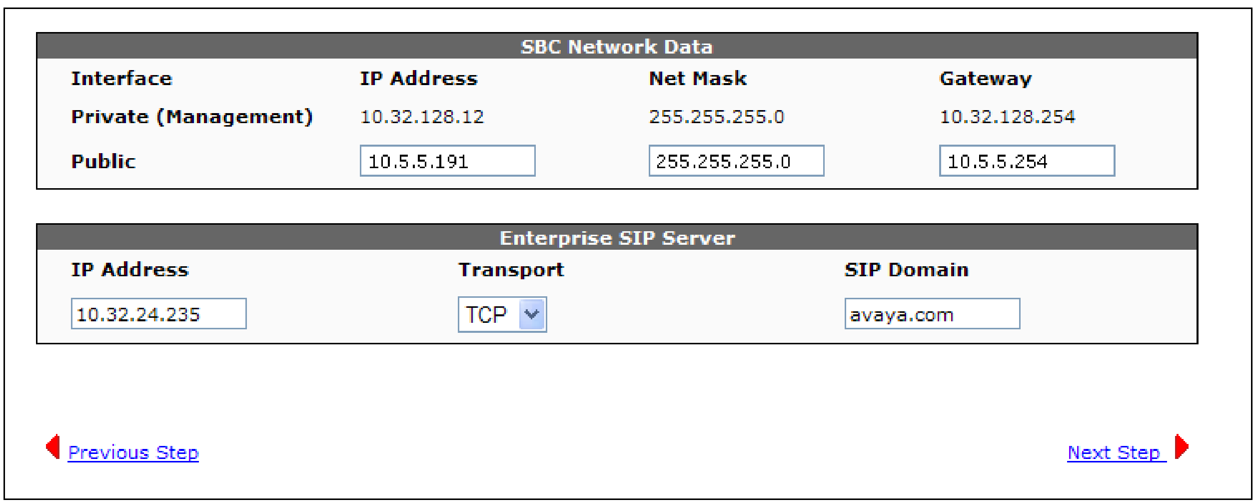
In the **SBC Network Data** section:

- **Public IP Address**: Enter the IP address of the public side of the 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:

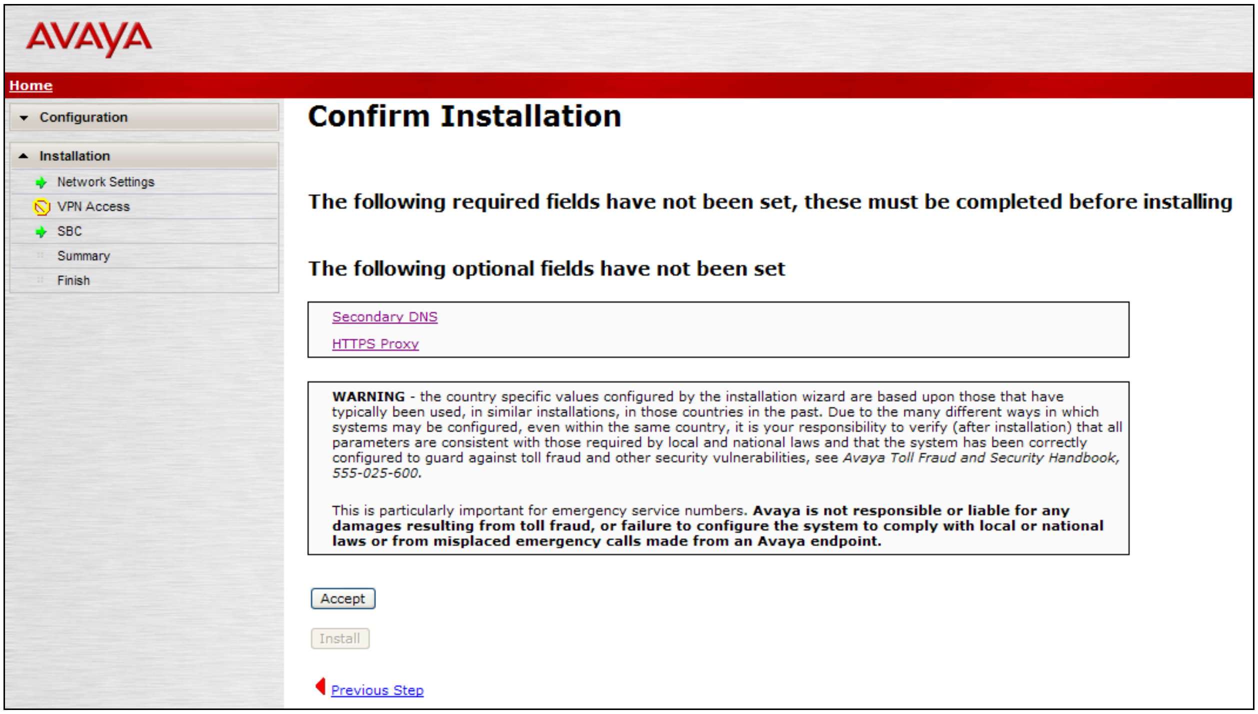
- **IP Address**: Enter the IP address of the Enterprise SIP Server to which the SBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface.
- **Transport**: From the pull-down menu, select the transport protocol to be used for SIP traffic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



6.1.4. Confirm Installation

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

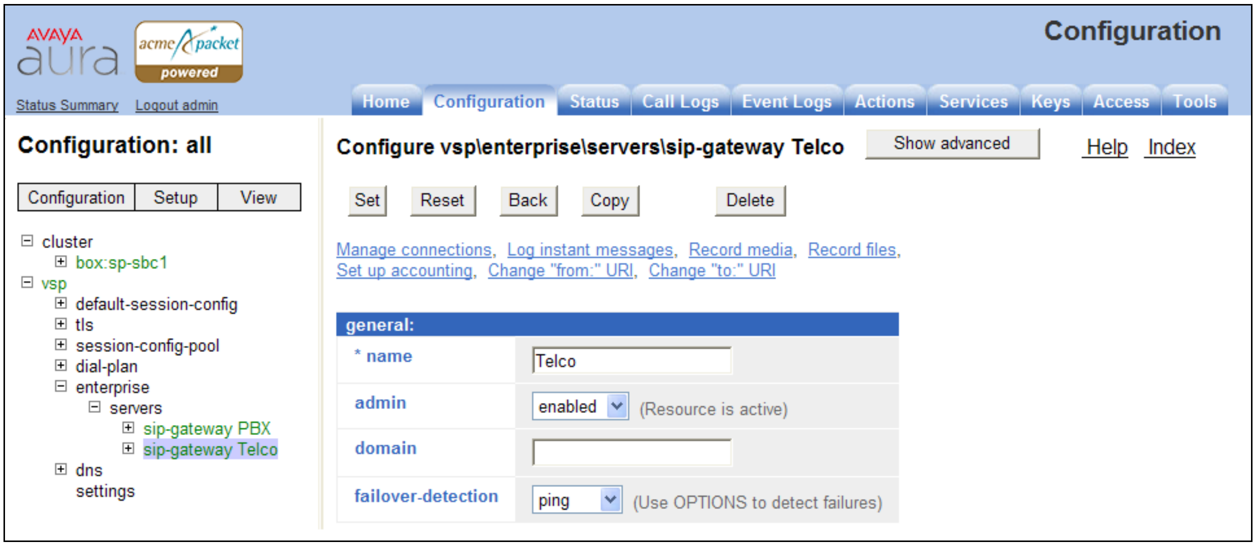


6.2. Post Installation Configuration

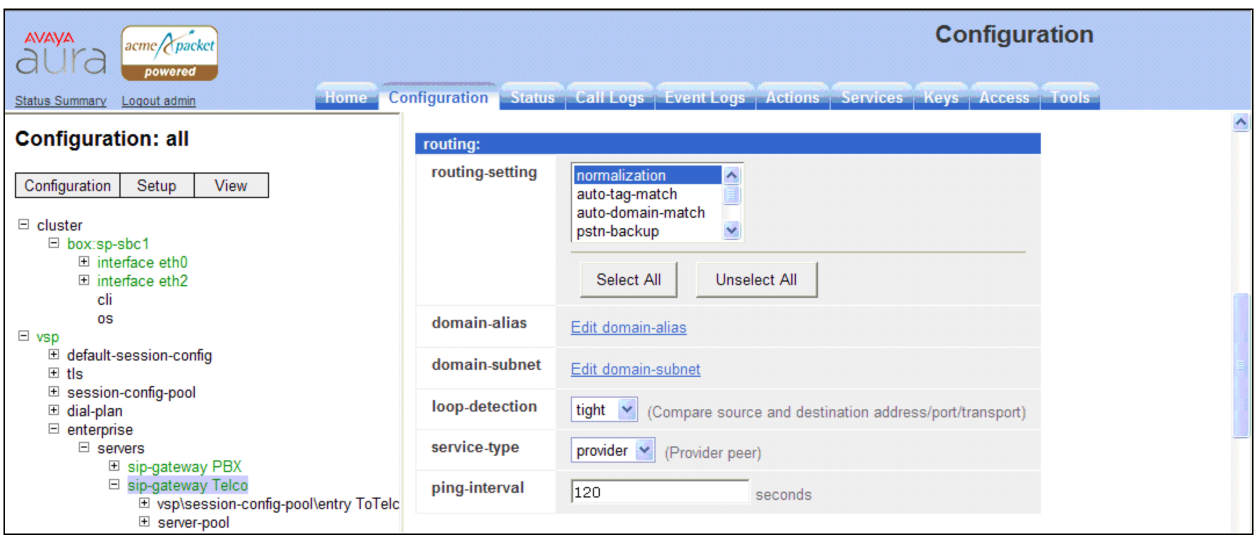
The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 6.1**. Since a different service provider other than XO had to be selected in the installation wizard then additional manual changes must also be performed. These changes are performed by accessing the browser-based GUI of the Session Border Controller, using the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 6.1**. Log in with proper credentials.

6.2.1. Options Frequency

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

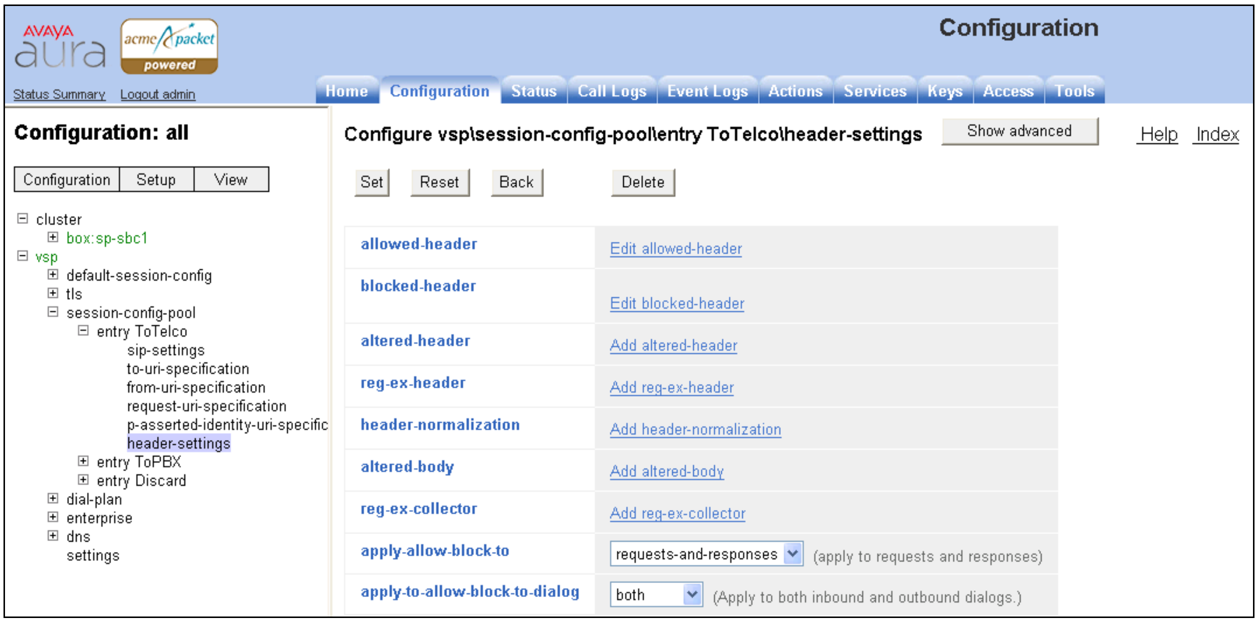


Scroll down to the **routing** section of the form. Enter the desired interval in the **ping-interval** field. Click **Set** at the top of the form (shown in previous figure).

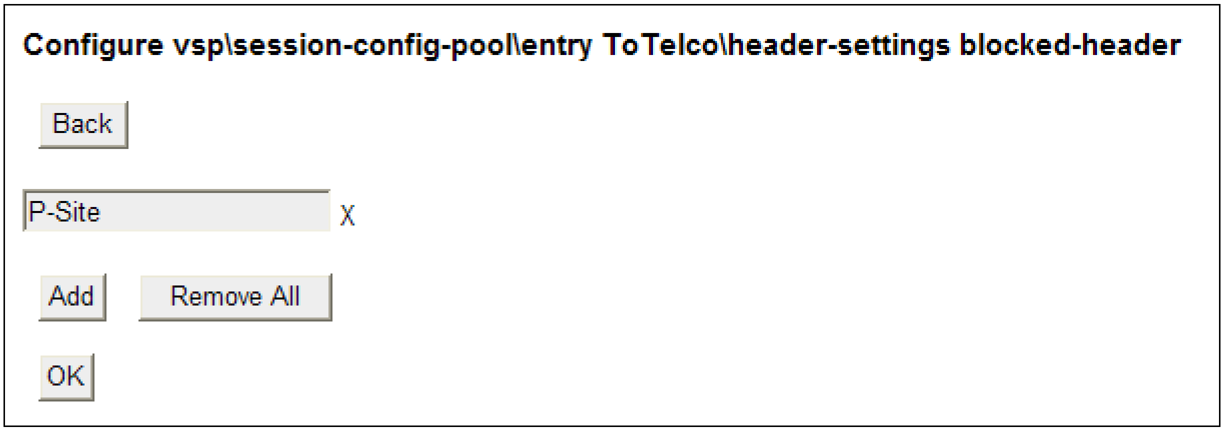


6.2.2. Blocked Headers

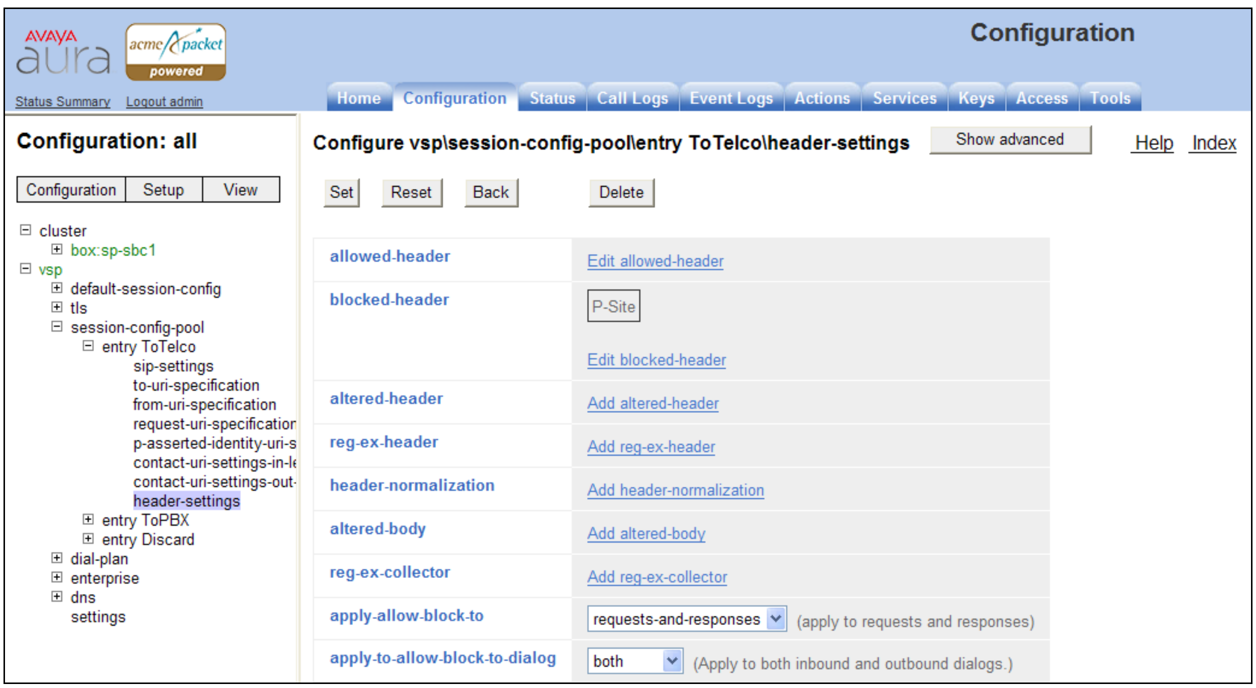
The P-Site header is sent in SIP messages from the Session Manager to the XO network. This header contains private IP addresses from the enterprise. These private IP addresses should not be exposed external to the enterprise. For simplicity, this header was simply removed (blocked) from both requests and responses for both inbound and outbound calls. To create a rule for blocking a header on an outbound call, first navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. Click **Edit blocked-header**.



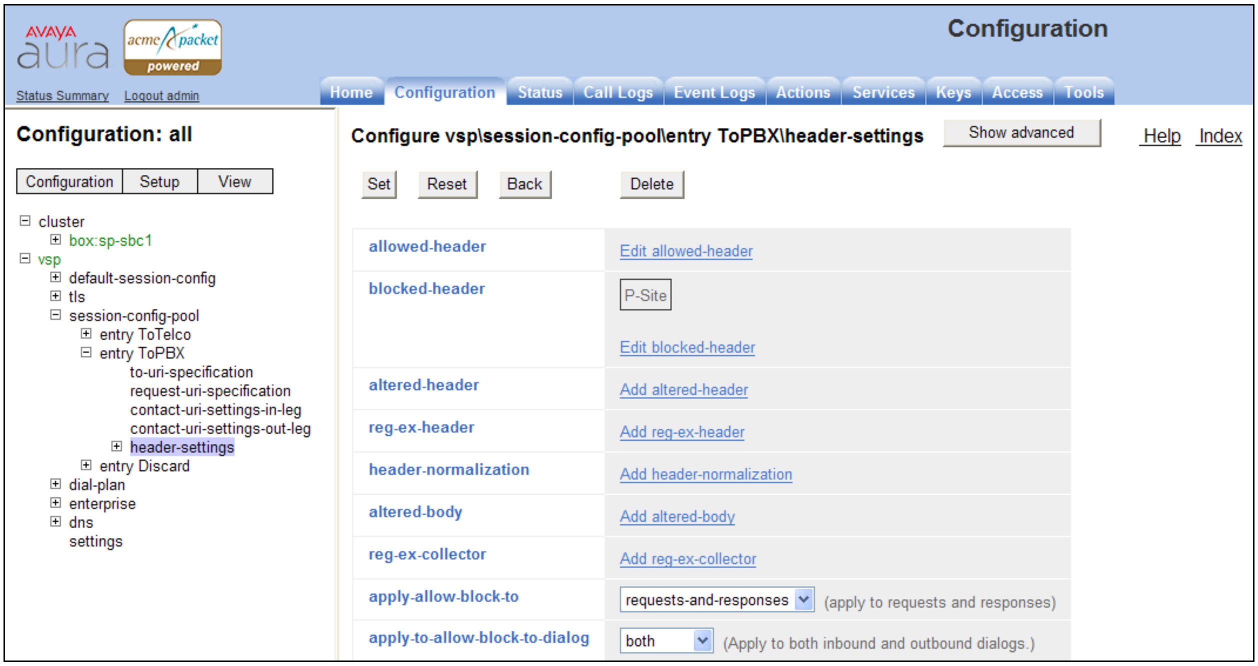
In the right pane that appears, click **Add.** In the blank field that appears, enter the name of the header to be blocked. Click **OK**. The screen below shows the **P-Site** header blocked for the compliance test.



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

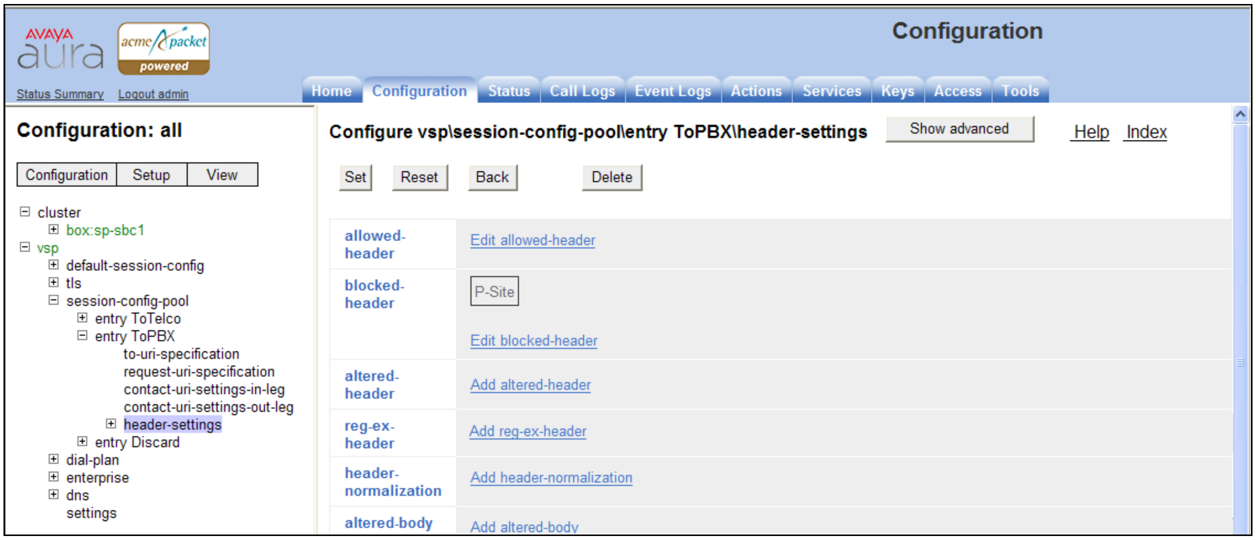


To create a rule for blocking a header on an inbound call, first navigate to **vsp → session-config-pool → entry ToPBX → header-settings**, then repeat the procedure described earlier in this section. The list of blocked headers for inbound calls is shown below.



6.2.3. Max-Forwards Value

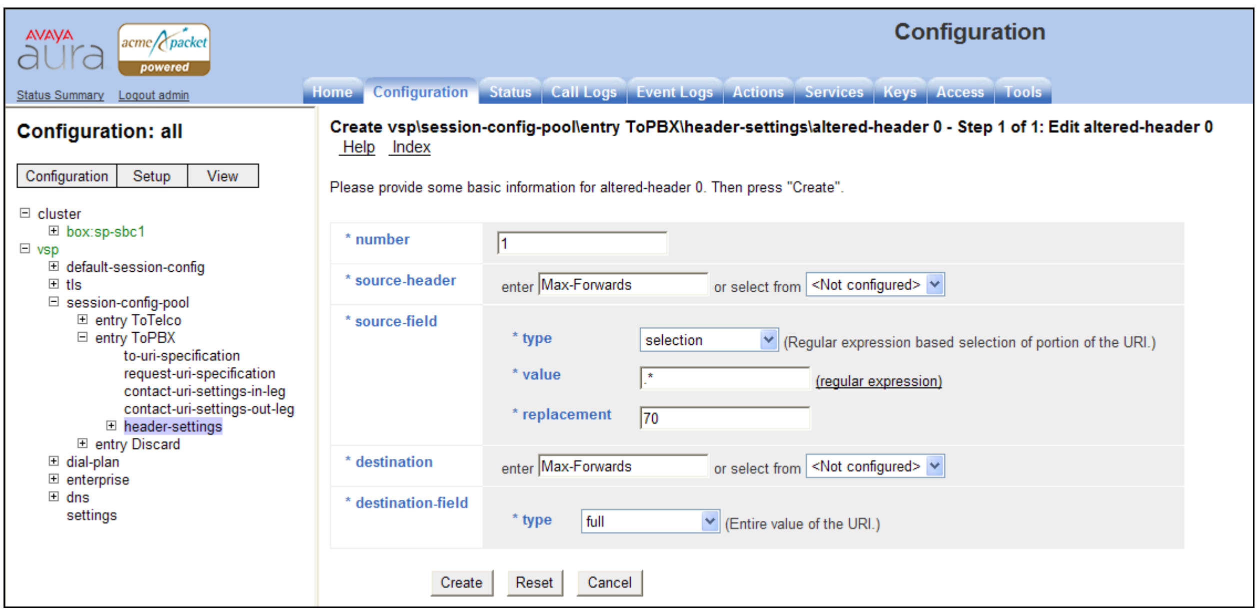
On incoming PSTN calls to a enterprise SIP phone, the Max-Forwards value in the incoming SIP INVITE is too small to allow the message to traverse all the SIP hops internal to the enterprise to reach the SIP phone. Thus, the SBC was used to increase this value when the INVITE arrived at the SBC from the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



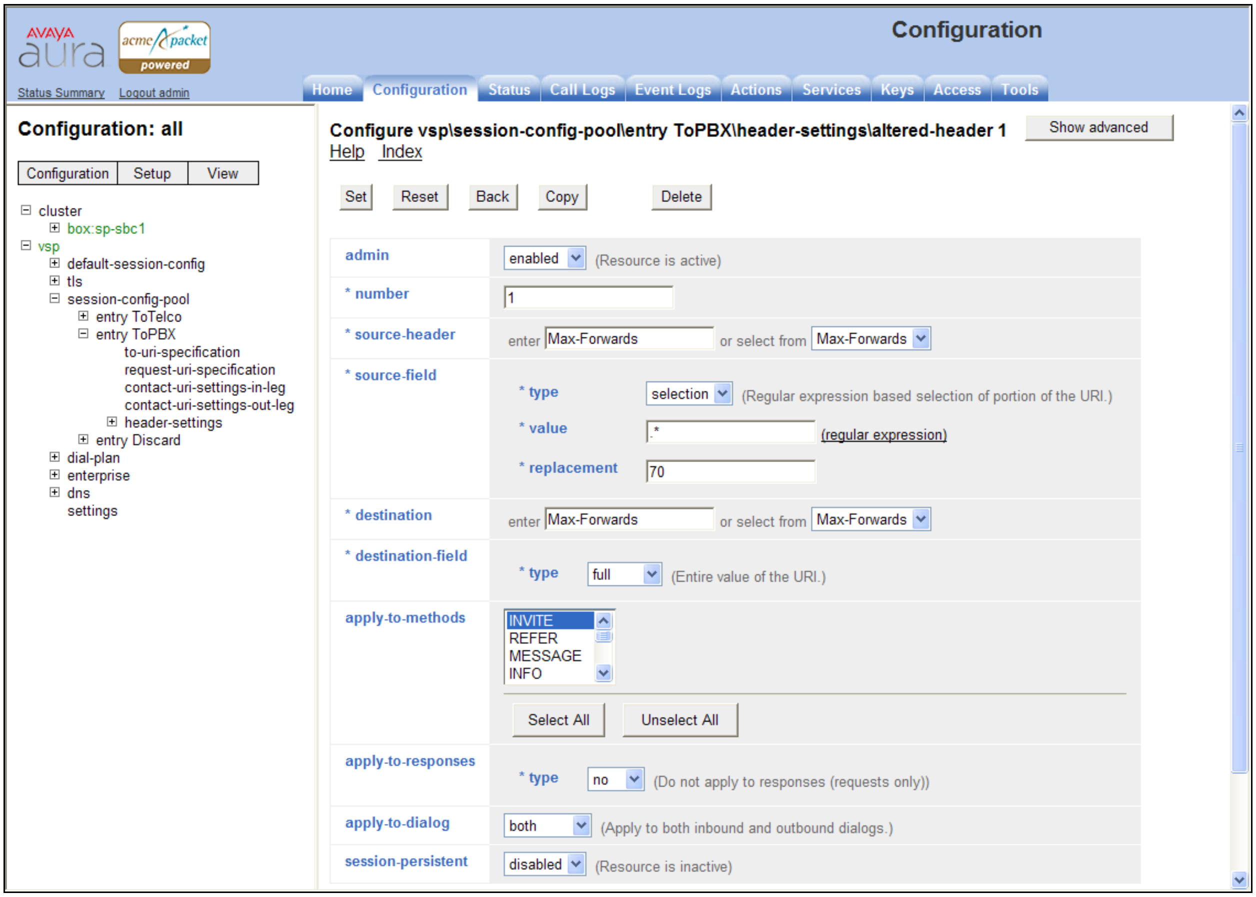
In the right pane that appears, enter the following in the fields specified below.

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

Click the **Create** button.

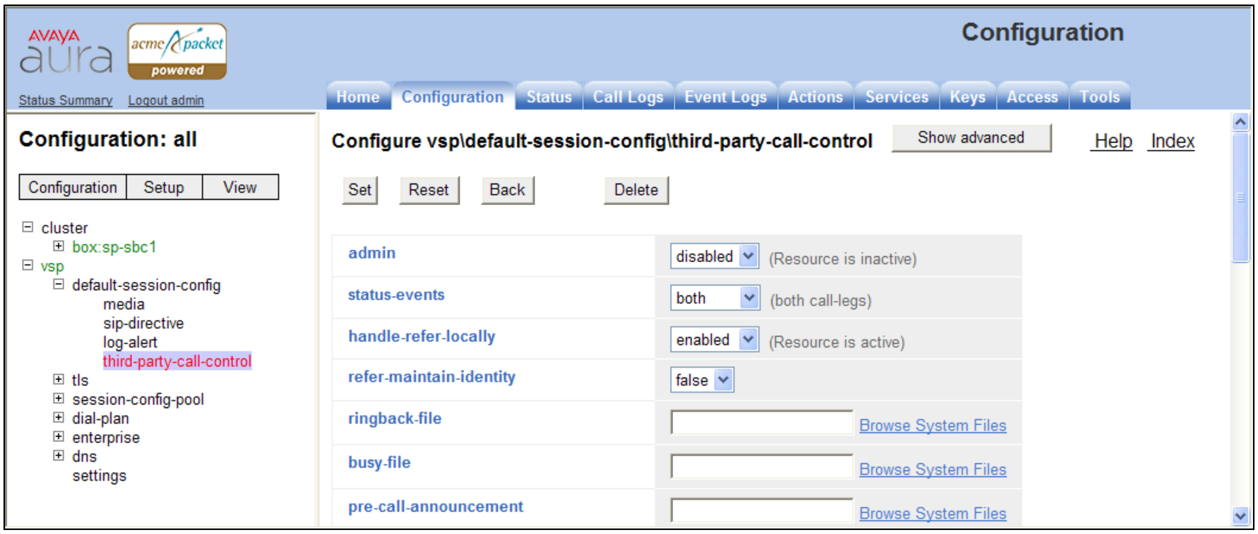


The right pane then displays the newly created altered header with default values for all other fields. Click the **Set** button on this page to complete the configuration.



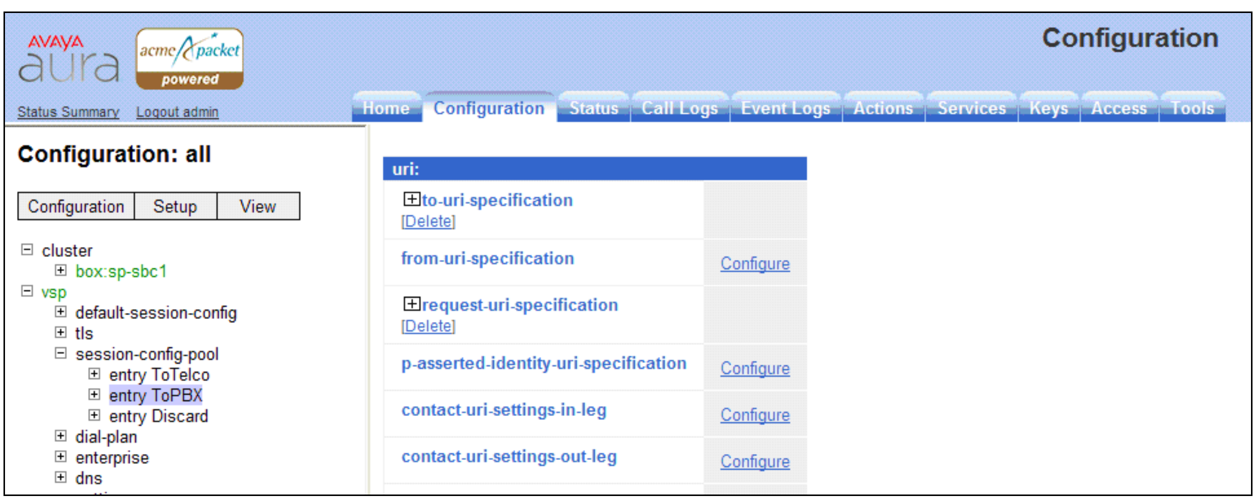
6.2.4. Third Party Call Control

Disable third party call control. Navigate to **vsp → default-session-config → third-party-call-control**. Set the **admin** field to ***disabled***. Disabling **third-party-call-control** will impact customers enabling this parameter to provide protocol conversion between the Microsoft usCSTA interface and the Broadworks Open Client Interface.

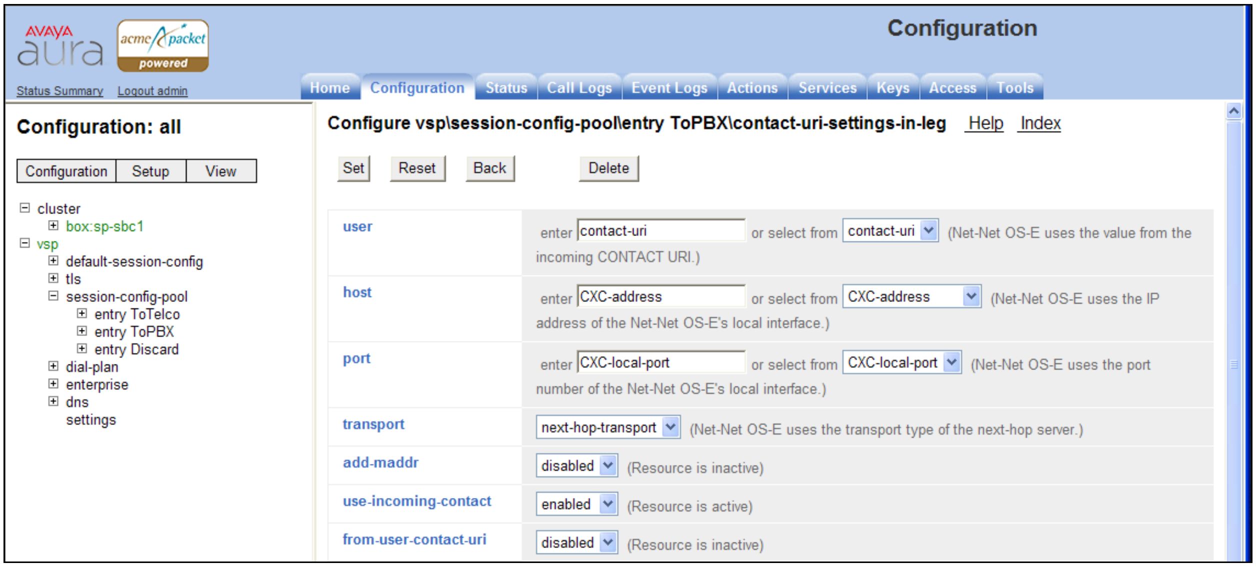


6.2.5. Contact Header

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



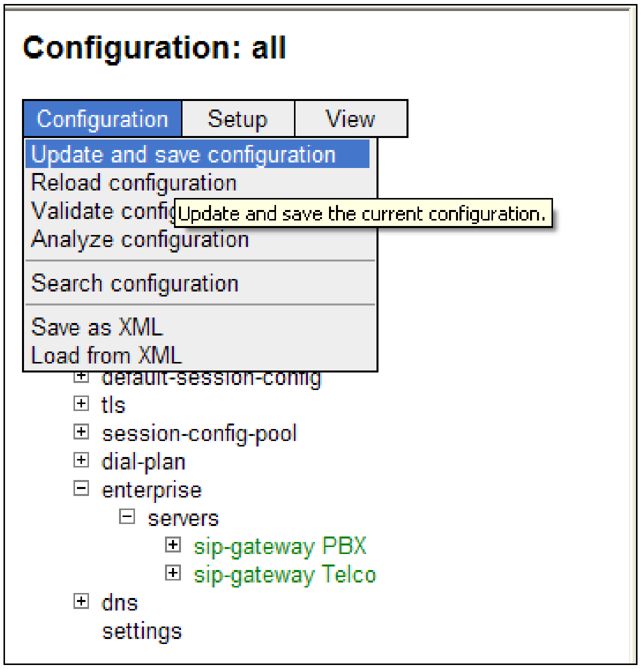
In the right pane that appears, set the **add-maddr** field to ***disabled*** and the **use-incoming-contact** field to ***enabled***.



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

6.2.6. 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**.



7. XO SIP Trunking Configuration

To use XO SIP Trunking, a customer must request the service from XO using their sales processes. The process can be started by contacting XO via the corporate web site at www.xo.com and requesting information via the online sales links or telephone numbers.

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

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

8. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager, Session Manager and the SBC to connect to XO SIP Trunking. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 1.1**.

XO SIP Trunking passed compliance testing.

9. Verification and Troubleshooting

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

Verification Steps:

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

Troubleshooting:

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to XO SIP Trunking. XO SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. XO SIP Trunking 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, June 2010.
[2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
[3] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* May 2009, Document Number 555-245-205.
[5] *Installing and Upgrading Avaya Aura® System Manager 5.2 GA Version*, January 2010.
[6] *Installing Avaya Aura® Session Manager*, January 2010.
[7] *Administering Avaya Aura® Session Manager,* March 2010, Document Number 03-603324.
[8] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x,* February 2010, Document Number 16-601443.
[9] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.
[10] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.
[11] *Avaya one-X Communicator Getting Started, November 2009.*
[12] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/
[13] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/
[14] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

12. Appendix A: Avaya Aura® SBC Configuration File

```
#
#  Copyright (c) 2004-2010  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 12:16:35 Thu 2010-09-16
#
config cluster
 config box 1
  set hostname sp-sbc1
  set timezone America/New_York
  set name sp-sbc1
  set identifier 00:ca:fe:09:42:38
  config interface eth0
   config ip inside
    set ip-address static 10.32.128.12/24
    config ssh
    return
    config snmp
     set trap-target 10.32.128.11 162
     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 "" "" any 0
    return
    config icmp
    return
    config media-ports
    return
    config routing
     config route Default
      set gateway 10.32.128.254
     return
     config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.32.128.10
     return
     config route Static1
      set admin disabled
     return
     config route Static2
      set admin disabled
```

```
     return
     config route Static3
      set admin disabled
     return
     config route Static4
      set admin disabled
     return
     config route Static5
      set admin disabled
     return
     config route Static6
      set admin disabled
     return
     config route Static7
      set admin disabled
     return
     config route internal-sip-media
      set destination host 10.32.24.235
      set gateway 10.32.128.254
     return
    return
   return
  return
  config interface eth2
   config ip outside
    set ip-address static 10.5.5.191/24
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" any 0
    return
    config media-ports
    return
    config routing
     config route Default
      set admin disabled
     return
     config route external-sip-media
      set destination network 10.2.2.0/24
      set gateway 10.5.5.254
     return
    return
   return
  return
  config cli
   set prompt sp-sbc1
  return
  config os
  return
 return
return

config services
 config event-log
  config file access
   set filter access info
```

```
    return
    config file system
     set filter general info
     set filter system info
    return
    config file errorlog
     set filter all error
    return
    config file db
     set filter db debug
     set filter dosDatabase info
    return
    config file management
     set filter management info
    return
    config file peer
     set filter sipSvr info
    return
    config file cac
     set filter sipCAC warning
    return
    config file dos
     set filter dos alert
     set filter dosSip alert
     set filter dosTransport alert
     set filter dosUrl alert
    return
    config file krnlsys
     set filter krnlsys debug
    return
    config file acct
     set filter acct debug
    return
  return
return

config master-services
 config accounting
 return
 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
  return
  config third-party-call-control
  return
 return
 config tls
  config certificate ws-cert
   set certificate-file /cxc/certs/ws.cert
  return
 return
 config session-config-pool
  config entry ToTelco
   config sip-settings
   return
   config to-uri-specification
    set host next-hop
   return
   config from-uri-specification
    set host local-ip
   return
   config request-uri-specification
    set host next-hop
   return
   config p-asserted-identity-uri-specification
    set host local-ip
   return
   config contact-uri-settings-in-leg
    set add-maddr disabled
    set use-incoming-contact enabled
   return
   config contact-uri-settings-out-leg
    set add-maddr disabled
    set use-incoming-contact enabled
   return
   config header-settings
    set blocked-header P-Site
   return
  return
  config entry ToPBX
   config to-uri-specification
    set host next-hop-domain
   return
   config request-uri-specification
    set host next-hop-domain
   return
   config contact-uri-settings-in-leg
    set add-maddr disabled
    set use-incoming-contact enabled
   return
   config contact-uri-settings-out-leg
    set add-maddr disabled
    set use-incoming-contact enabled
   return
   config header-settings
    set blocked-header P-Site
```

```
    config altered-header 1
     set source-header Max-Forwards
     set source-field selection .* 70
     set destination Max-Forwards
     set destination-field full
    return
    config reg-ex-header 1
     set destination Refer-To
     set create Refer-To "<sip:(.*)@avaya\.com(.*)>" "<sip:\1@\r\2>"
     set apply-to-methods REFER
    return
   return
  return
  config entry Discard
   config sip-directive
   return
  return
 return
 config dial-plan
  config route Default
   set priority 500
   set location-match-preferred exclusive
   set session-config vsp\session-config-pool\entry Discard
  return
  config source-route FromTelco
   set peer server "vsp\enterprise\servers\sip-gateway PBX"
   set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
   set peer server "vsp\enterprise\servers\sip-gateway Telco"
   set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
 return
 config enterprise
  config servers
   config sip-gateway PBX
    set domain avaya.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 10.32.24.235
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set failover-detection ping
    set ping-interval 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
     config server Telco1
      set host 10.2.2.138
     return
```

```
    return
   return
  return
 return
 config dns
  config resolver
   config server 10.32.24.150
   return
  return
 return
 config settings
  set stack-socket-threads-max 2
 return
return

config external-services
return

config preferences
 config gui-preferences
  set enum-strings SIPSourceHeader Refer-To
  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 0x002bdd5d9fea2fefeb97b0115854a47db2c8b27a2fe0187e0274977f4b
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x004803cd9fae4ee1b2462598359d6c5e179008f9083caa7b30b9b19b43
   set permissions access\permissions read-only
  return
 return
return

config features
return
```

13. Appendix B: Workaround for Double DTMF Digit Detection

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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Enable Session for TN2602
In order to log into the TN2602 Circuit Pack, first enable this capability by using the enable session command on the Avaya Communication Manager SAT interface. Set the parameters as described below.

Login: Create a login name for use when logging into the circuit pack.
Password: Create a password for this login name.
Reenter Password: Enter the password again.
Secure?: Select n for Telnet or y for SSH.
Time to login: Enter the number of minutes this login will be valid. The maximum value is 255.
Board address: Enter the cabinet/carrier/slot location for the circuit pack that will be accessed. This value can be found from the list configuration all command.

<pre>
enable session   Page   1 of 1

                                 ENABLE SESSION

                 Login: user
              Password:
      Reenter Password:
               Secure? n
         Time to login: 200
         Board address: 1a03
</pre></td></tr>
</table>

Step	Description

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

Step	Description

3.	**G450/430 Gateway**
	If a G450/G430 is used in the configuration, then log in to the gateway using proper credentials and issue the following command shown in bold below.
	
	▪ **voip-parameters** – Enter the VoIP parameters configuration mode.
	▪ **set id 60 value 1** - Sets up a temporary buffer with VOIP parameter 60 set to value 1. This parameter enables the firmware workaround.
	▪ **dsp-downlink** - Sends any VOIP parameters to the DSPs.
	▪ **Exit** – Exit the VoIP parameter mode.
	▪ **copy run start** - Save parameters to flash memory so the configuration will survive a reset.
	
	`sp3-g450-001(super)# voip-parameters`
	`Warning:`
	`The values chosen for non-default voip parameters can significantly affect the quality of service that users experience.  Avaya recommends seeking technical assistance from Avaya before making any modifications to the voip parameter defaults.`
	`sp3-g450-001(super-voip-parameters)# set id 60 value 1`
	`Done!`
	`sp3-g450-001(super-voip-parameters)# dsp-downlink`
	`Done!`
	`sp3-g450-001(super-voip-parameters)# exit`
	`sp3-g450-001(super)# copy run start`
	`Warning! It is a recommended policy to override default configuration master key with user defined secret - for details see user reference.`
	`Otherwise device saves configuration secrets using Avaya default secret.`
	`Beginning copy operation .................. Done!`
	`sp3-g450-001(super)#`

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.